MALTA COMMUNICATIONS AUTHORITY

CONSULTATION DOCUMENT

Measures towards enhancing further the security and integrity of Electronic Communications Networks and Services

Initiative #1 – Implementing a Minimum Set of Security Measures

MCA Reference: MCA/C/23-4803

Publication Date: 6th January 2023

☎ (+356) 2133 6840 @ info@mca.org.mt 🌐 www.mca.org.mt/

🏠 Valletta Waterfront, Pinto Wharf, Floriana FRN1913, Malta

TABLE OF CONTENTS

1 Introduction

In 2017, the Malta Communications Authority (hereafter the ‘MCA’ or ‘Authority’) organised a self-assessment survey amongst the top three ECS and ECN providers requesting details about their approach to network security and integrity. The Authority carried out this assessment in two stages. The first stage consisted of a questionnaire assessing the various security policies and procedures as adopted by the providers and compare them against a homogenous map indicated in ENISA's publication "Technical Guideline on Security Measures[1]". The questionnaire itself was organised in seven main domains and touched upon the measures related to all security objectives as indicated in the same guidelines.

The second stage consisted of collecting and evaluating the respective documentation substantiating the ECNS providers' claims made earlier in the first stage of the survey.

Through this exercise, the Authority concluded that while each ECNS provider adopted its methods and procedures to address various security objectives, it was also evident that not all ECNS providers were addressing the whole breadth of the security objectives as identified by ENISA. Also, at that time, the Authority noted that some providers might have some open issues concerning security documentation.

In 2022, the Authority conducted a similar self-assessment exercise where amongst other questions, the Authority asked providers of electronic communication networks and services for a rating on the security measures as listed in Appendix 1 of this document. While the exercise remains a self-assessment one, the high-level conclusions drawn show a general positive trend whereby providers adopted a more tight approach towards network and service security. Furthermore, during the last five years, two of the ECS and ECN providers surveyed have either been awarded the ISO27001 certification or extended their existing certification to cover a wider scope of the operation.

This indicates that the sector is recognising the need to bolster its security positioning of the networks and services on the market. However, the same findings indicate that such positioning is not homogenous across the market.

The Authority notes that until the Decision following this consultation process is concluded, there is only a general obligation to maintain the security of the networks and services;

[1] ENISA is the European Union Agency for Cybersecurity (https://www.enisa.europa.eu/)

however, with the exception of holders of the rights of use of 5G spectrum[2], no specific measures are established and applicable across the sector.

Throughout this consultation the Authority will be presenting a set of proposals which are intended to ensure that all providers engage in a framework where security risks are assessed and mitigated for. The proposals on the implementation of Minimum Security Measures are aimed at ensuring that a minimum security level adequate for present networks and services will be in place across the whole sector in Malta. Such a measure, amongst the underlying added benefits, shall facilitate the forecasting of the security budget in terms of capital and operation expenditure for the respective stakeholders' business plans.

The Authority is proposing a security framework that adopts on a national basis the security measures published by ENISA as published in the "Guideline on Security Measures under the EECC"[3] The document organises the security objectives under eight themes or security domains. For each objective, a set of actions are listed, which are grouped into three levels of sophistication levels termed the Basic Level, the Industry Standard, and the State-of-the-art Levels. Further to adopting these guidelines, the Authority includes requirements for providers of ECNS to carry out a risk assessment and an audit which should be repeated periodically.

The list below summarises the key proposals related to the minimum security measures:

Proposal 1 presents the obligation of Electronic Communications Networks and Services providers to carry out a periodic risk assessment at least every three years. Providers are also expected to update the same risk assessment to reflect the ongoing changes in the organisation, the services offered, and the risk presented. The Authority will request evidence of the process while reserving the right to analyse the risk assessment as needed from time to time.

Proposal 2 presents the security measures to be taken by providers of Electronic Communication Networks and Services to address the security risks of the networks and services.

[2] Holders of 5G spectrum licences are obliged to follow security guidelines published by the MCA, or other competent bodies such as ENISA

[3] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/@@download/fullReport

Proposal 3 presents the three sophistication levels in which the measures related to the various security objective shall be grouped. This tiered approach facilitates the application of proportionality between the level of risk and the mitigation measures

Proposal 4 presents the minimum set of measures that the Authority considers necessary to be implemented by Electronic Communication Networks and Services providers to consider them as having taken the appropriate measures to address their risks.

Proposal 5 presents the obligation to carry out a security audit periodically

Proposal 6 presents the technical requirements for an audit process to be recognised at law

Proposal 7 presents the requirement on providers of electronic communications networks and services to establish a contact point suitable to deal with security incidents of a significant scale

Proposal 8 puts forward the timelines for the implementation of this framework

As an appendix to this Consultation, the Authority presents its views on the extension of obligations to the providers of Electronic Communications Networks and Services to build their own CSIRT functionality to improve the security response of the entire sector in Malta.

2 Risk Management Process and the related Proposals

Figure 1 below shows the foundations of a risk management process, which also forms the basis for the proposals put forward in this consultation paper.

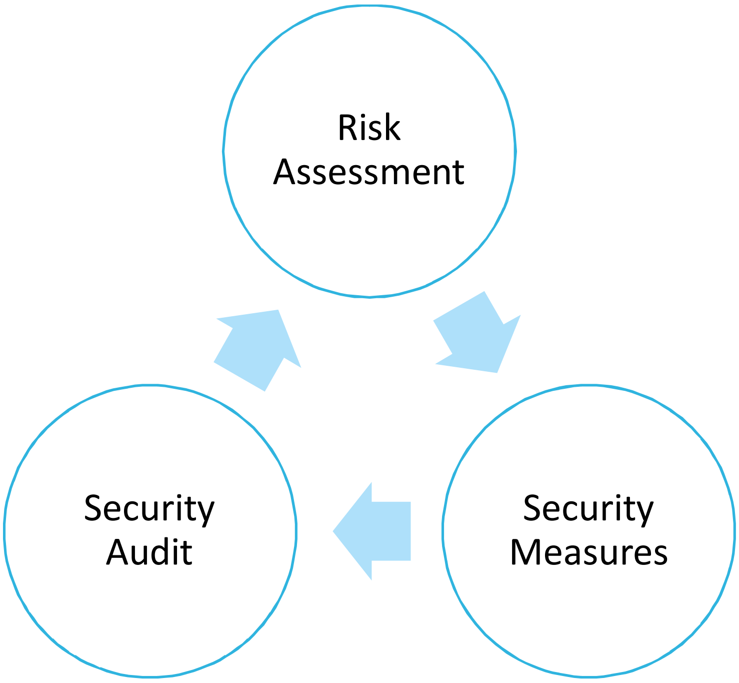

Figure 1 Risk Management Process

2.1 Risk Assessment

A provider of publicly available ECNS is required to take the necessary steps to appropriately manage the risks posed to the security of networks and services. The term 'security' refers to the ability of the networks and services to withstand, within the limits of proportionality, those attacks that may impact the availability, authenticity, integrity or confidentiality of the networks and services. 'Security' also extends towards any data stored, processed or transmitted over the networks. A risk assessment is the first step in the risk management process, where risks are identified and addressed. The provider shall identify both the assets, including any underlying supporting systems and the relevant processes directly associated with the delivery of the electronic communications networks and services. For each asset and process identified in the risk assessment, the ECNS provider shall examine the related risks in terms of the actual probability of materialisation of the risk and the damage caused to the subscribers and their data when the risk materialises. Assets and processes are further classified according to their level of criticality in contributing to the security of networks and services using the classification system identified in the introductory paper of this Consultation[4].

Three main influencing factors which are considered significant when compiling the risk assessment, are:-

a. All assets (including operating software running on the respective assets) involved in the setup of the electronic communications network and delivery of the associated services,
b. Organisational setup and processes necessary to operate and maintain the electronic communications network and delivery of the associated services
c. External factors intrinsically beyond the control of the ECNS provider which have an impact on the security and integrity of the electronic communications network and/or the delivery of the associated services,

2.2 Proposal 1 – The compilation of periodic risk assessments

The Authority proposes that providers of ECNS shall carry out a risk assessment of their networks and services to assess the risk of breaching security and integrity which may result in significant disruption to the operation of the network and service delivery. For this exercise, as a minimum, the risk assessment should address scenarios that may result in security incidents of such scale that, upon considering the incident scale presented in Table 1 of the accompanying document that treats the revision of the incident reporting mechanism[5], would then be classified as Level 3 – Severe Impact Incidents

To complete the risk assessment, ECNS providers shall be required to:

a) Identify all the assets used to set up the electronic communications networks and deliver the relevant electronic communications services;
b) Classify the assets in line with their criticality;
c) Identify the organisational structure and processes required to manage the assets.
d) Identify those risks which may expose the networks and services to significant disruption;
e) Identify those measures which are necessary and feasible to address and mitigate identified risk; and

[4] Effecting Measures towards enhancing further the security and integrity of Electronic Communications Networks and Services - Outline Document

[5] Effecting Measures towards enhancing further the security and integrity of Electronic Communications Networks and Services - Initiative #2 Revision of the Incident Reporting Mechanism"

f) Identify any residual risks that may remain unmitigated.

ECNS providers shall be required to carry out a fully comprehensive risk assessment at least once every three years. Moreover, at least once a year, during the interim years, providers should reassess and update their risk assessment in those areas which were significantly impacted by changes to any of the following elements

a) the assets, including the software and configuration; and
b) changes of organisational nature, including procedures.

It is proposed that providers of ECNS present the Authority with the documentation confirming the completion of the process, including interim updates. The Authority reserves the right to request a copy of the risk assessment report or parts thereof.

Consultation Questions11	
SM 1	What are your views on the proposed requirement for providers to carry out security and integrity risk assessments every three years, with intermediate revisions every year?
SM 2	What are your views on the elements that need to be captured in a risk assessment report?
SM 3	What are your views about the identified criteria which would influence the validity of a risk assessment? Do you suggest the inclusion or ommission of additional elements in this list? Please provide a detailed justification
SM 4	What are your views on the reporting requirements proposed?
SM 5	If you are an ECS and/or ECN provider, how do the proposed requirements of a risk assessment differ from those of your organisation? Conversely, how similar are they?

3 Proposal 2 - Security Measures

The balance between the technology adopted by the provider, the risk to be addressed and the cost to address the risk is to be sought. This balance forms the basis of the proportionality criteria on which the proposed security measures rest. In its proposals, the Authority puts forward a matrix that pairs the mitigation measures with the security objectives a provider is to reach. All mitigation measures are graded in terms of sophistication levels that are adequate to address different risk levels.

In December 2020, ENISA published its guidelines on the security measures that form the basis for the security measures put forward. This section represents the main eight (8) domains under which the objectives are grouped:

1. **Governance and risk management:** An organisation has appropriate management policies and processes to govern its approach to the security of its networks and services.
2. **Human resources security**: Human resources are a central element towards any organisation, not least in implementing its security policies and procedures. An organisation's policy that looks into the recruitment requirements of personnel and relevant security training is covered within this domain.
3. **Security of systems and facilities**: This domain covers the physical and logical security of network and information systems and facilities
4. **Operations management**: This domain covers operational procedures, change management and asset management
5. **Incident management**: Incidents that disrupt networks and services are bound to happen. This domain addresses the need for policies that detect, manage and escalate incidents as necessary
6. **Business continuity management**: Service disruptions will invariably happen. However, organisations shall have tried and tested processes intended to contain or limit the impact of compromise arising from the incident.
7. **Monitoring, auditing and testing**: Security policies should be continuously tested to ensure their adequacy when considering the evolution of the technology providing the network and services offered and associated security risks.
8. **Threat Awareness:** Providers should be aware of current threats and where necessary, share information about major threats with their end-users.

Appendix 1 of this document provides the complete list of measures applicable in each domain that form part of this proposal.

3.1 Proposal 3 – Different Sophistication Levels in mitigating risk

The Authority understands that there is no one-size-fits-all measure that is suitable across the sector, since each provider is unique in its setup, the type of services offered, and the customers catered for are amongst the many variances that differentiate providers. These variances give rise to different security risks that the networks and services may be exposed to and the different tolerance to security and integrity failures each network may accept. Providers may need to adopt different measures at least in terms of scale. In its guidelines, ENISA suggests that all measures listed under a given security objective are subdivided into three sophistication levels labelled from Level 1, which is termed the basic level, up to Level 3, which is the state-of-the-art measure. This also provides for a structured approach when addressing security risks and mitigation. The different sophistication levels are presented below:

1. Sophistication Level 1 (Basic Sophistication Level) – in which the minimum measures are employed to address a specific objective
2. Sophistication Level 2 (Industry Standard) – refers to the method commonly applied within the industry to address a specific objective
3. Sophistication Level 3 (State of the Art) – which refers to advanced security measures coupled with continuous monitoring of implementation, structural review of the implementation of measures taking into account ongoing changes and informed with data gathered from incidents and exercises with the aim of preempting any security threats.

The measures necessary to reach a specified sophistication level are all cumulative. Therefore, in reaching a specific sophistication level for a given security objective, all the measures listed under that specific level must be addressed along with those listed under all lower sophistication levels.

The detailed security measures listed in Appendix 1 are presented using the sophistication levels as follows:

1. Each table consists of three columns and three rows.
2. The first column details the sophistication level associated with the measures within that row.
3. The second column lists those measures related to each sophistication level. Reaching the objectives of a sophistication level is a cumulative process. Therefore, to reach Sophistication Level 3, all the security measures of the other two sophistication levels are to be reached. Similarly, reaching Sophistication Level 2 automatically implies that Sophistication Level 1 is also reached.
4. The third column lists the type of evidence expected to indicate which security measures were implemented. In the eventuality of an audit, either the evidence listed

in this section will be sought, or else alternative but equivalent evidence may be presented by the provider. When alternative evidence is presented, it shall be the task of the provider to appropriately map the presented evidence with the list of evidence listed in this section. .

3.2 Proposal 4 - Minimum Security Measures

In highlighting how the EECC directive expects providers of ECNS to fulfil their obligation of taking the necessary measures to safeguard the security of their networks and services, Recital (94) of the same directive, identifies four major areas, each with their relevant sub-areas, which merit to be relisted here:

a) Security of networks and facilities:
   a) Physical and environmental security,
   b) Security of supply,
   c) Access control to networks, and
   d) Integrity of networks
b) Handling of security incidents
   a) Handling procedures
   b) Security incident detection capability
   c) Security incident reporting and communication
c) Business continuity management
   a) Service continuity strategy and contingency plans
   b) Disaster recovery capabilities
d) Monitoring, auditing and logging policies
   a) Exercise contingency plans
   b) Network and service testing
   c) Security assessments and compliance monitoring
   d) Compliance with international standards

In December 2020, ENISA published its "Guideline on Security Measures under the EECC[6]" which proposes a number of security measures to be considered by providers of ECSN to secure their networks and services. These guidelines present a list of twenty-nine (29) security objectives which are grouped into eight security domains. Although the organisation of the objectives presented by ENISA's guidelines is slightly different from that identified in Recital 94 of the EECC directive, the areas of interest are the same. Given that the literature provided

[6]https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/at_download/fullReport

by ENISA is more detailed and given further that ENISA's guidelines readily present the objectives in three sophistication levels, the security objectives in this paper will also be presented in line with ENISA's document.

The Authority proposes that by default, all providers of Electronic Communication Networks and Services operating both Category A and Category B assets shall implement those security measures required to address the risks highlighted in their respective risk assessments aiming to avoid security and integrity incidents at Level 3 of the incident reporting scale.

The Authority further proposes that by default, providers of Electronic Communication Networks and Services that operate Category A assets shall be required to implement all those measures listed in Appendix 1 such that they reach the Basic Sophistication Level as a minimum.

The Authority considers this position proportionate given that failures of integrity and security impacting providers that operate Category A assets bear a more significant impact on a national scale than those that only operate up to Category B assets. Moreover, a recent survey carried out by the Authority in 2022 shows that two of the three operators that the Authority perceives as operating Category A assets reported that they reached the Industry Standard level of implementation for most security objectives. This is a whole tier above the sophistication level that is proposed as a minimum.

Therefore for a provider of electronic communication networks and services to be considered compliant with the requirements of regulations 27 and 28 of S.L 399.48, it must carry out a risk assessment in accordance with Proposal 1 of this document and implement those measures that are required to address the security threats highlighted. In addition, operators of Category A assets must ensure that the minimum security measures implemented are sufficient to reach the Basic Sophistication Level for all security objectives listed in Appendix 1 of this document.

The Authority is open to discuss with the respective providers any exceptions that could be justified on a case-by-case approach after analysing the relevant risk assessment that justifies specific scenarios, provided that the risk assessment is deemed comprehensive. The Authority reserves the right to request the provider to undergo further evaluations of its risk assessments when necessary.

The Authority, reserves the right to inspect risk assessments, especially in those cases whenever the Authority deems it necessary to ensure that measures implemented reflect the risk posed.

Upon its objective assessment, the Authority reserves the right to conclude that the security measures adopted are not sufficient to address the risk presented and shall take the necessary regulatory measures to ensure that the providers revise the security measures adopted to reflect the risk presented.

Consultation Questions	
SM 6	What are your views on the security objectives presented?
SM 7	What are your views on the necessary documentation to be maintained by the providers?
SM 8	What are your views on the proposal requiring providers to implement the Basic Sophistication Level as a minimum for all the security objectives?
SM 9	What are your views on the tiered approach towards the minimum security mitigation to be implemented by providerse operating Category A and Category B assets.
SM 10	If you are an ECS and/or ECN provider, how does the documentation required differ from that held within your organisation?

4 Security Audits

Auditing is an essential tool to ensure that mitigation measures are effective and appropriately implemented. Providers of electronic communication networks and services, particularly those that operate critical assets, are expected to carry out their own audits on a periodic basis.

4.1 Proposal 5 – Obligation to carry out a security audit every two years

It is proposed that providers operating Category A assets should carry out periodic audits at least once every two years. In accordance with the law, such audits shall establish compliance with the implementation of the security guidelines as proposed in this paper and future guidelines the Authority may lay down from time to time.

In addition, the Authority may, request providers to carry out additional audits in order to assess the level of security, integrity and resiliency of either the entire network and its organisational operation or part thereof. Such request from the Authority shall be justified on the basis of an assessment of specific issues related to ongoing investigations the Authority may be running from time to time. Such requests shall be focused and only intended to address areas of concern. The Authority shall give the provider notice of six months before proceeding with such audits.

In line with the provisions of the law, the providers of electronic communication networks and services shall finance such audits.

4.2 Proposal 6 – Technical requirements of the Audit process

It is proposed that for an audit to be deemed admissible under the terms of the law, a number of criteria need to be met as part of the process:

(a) Auditors should be independent of the providers engaging them for the audit. Independence of the auditors is assured if the auditors are not suppliers of the same provider, except for those cases where the auditors are carrying out external audits.

(b) Competence of the auditors in terms of technical knowledge about applicable industry standards, specifications, and known industry best practices, particularly in the field of electronic communications, is to be demonstrated.

(c) Providers of electronic communication networks and services are to provide the auditor with adequate access to relevant documentation and sites so as not to hinder the audit process.

(d) Detailed documentation is to be made available to the Authority before the commencement of the audit and after the conclusion of the audit process.

(i) At least three months before the commencement of the Audit, the provider is to send the Authority documentation listing the following:

1. The identification of the auditor and the necessary declaration of independence of the auditor,
2. An audit plan detailing the objectives of the audit; and
3. A high-level audit plan

(ii) Prior to the commencement of the Audit, the Authority shall approve the audit plan presented by the electronic communication network and service provider. In some cases, the Authority might need to seek clarification either from the electronic communication network and service provider or the auditor itself. In the case of the latter, the provider must provide free access to the auditor. The Authority reserves the right to suggest modifications to the plan, to which the provider is to take due account of.

(iii) By not later than one month after the conclusion of the Audit, providers of electronic communication and services shall be required to submit the final audit report to the Authority.

1. The Authority shall reserve the right to hold discussions both with the ECSN provider and the auditor, either jointly or separately.
2. In those cases where the auditor's report indicates elements of non-compliance, the provider should provide plans on how to remedy the non-conformance.

Consultation Questions	
SM 11	What are your views in relation to the auditing of the implementation of security measures every two years?
SM 12	What are your views on the proposed process related to security audits?

5 Proposal 7 - Establishing contacts in case of security incidents

Collaboration with the stakeholders in the electronic communications sector is key to confront the ever-increasing risk to security. While the Authority is considering the future possibility of requesting all providers of ECNS to set up, in some form or another, their own CSIRT[7] functionality, the Authority is proposing that as an initial and interim measure, providers of ECNS that operate Category A Assets should ensure that the Chief Information Security Officer (CISO) or a delegate is continuously accessible on a 24/7 basis for both the locally based ECNS providers, the national authorities including the Authority. Such contact is necessary to ensure timely collaboration between ECNS providers and other interested entities to prevent significant scale incidents or mitigate the impact of an ongoing security incident. While the role of this communication channel is to facilitate the exchange of information in a timely manner, the responsibility to act on the networks rests solely with the network providers.

[7] Refer to Appendix 2 for further detail

6 Proposal 8 - Implementation Timelines

Upon taking into account the state of play of providers and the time and effort required to implement the security framework proposed, organise and maintain the relevant documentation, the Authority is proposing to split the implementation of these measures into three milestones as below.

All references to time associated with each milestone is measured from the date of publication of the final decision paper.

Milestone 1: Reachable after 12 months with an interim milestone reachable after 3 months

Milestone 1a Reachable after 3 months: The operator of ECNS should identify the assets utilised to deliver its electronic communication networks and services and classify them as either within Category A or Category B in line with the definitions proposed. Based on this classification, the provider should:

a) Carry out a risk assessment to establish the risks and vulnerabilities associated with its assets, as well as establish the appropriate response for these risks.
b) Having referred to the risk assessment and the security objectives, both outlined in this document, together with the state of implementation of the security measures already in place, the provider should establish a plan, which, within a period not longer than two years, leads the provider to reach the Basic Sophistication Level for all the eight domains. The provider should provide its plan to the Authority by the end of this 3-month period.

Milestone 1: Reachable after 12 Months: Provider shall submit an interim report to the Authority indicating the state of implementation of the security measures.

Milestone 2: Reachable after two years: Provider shall reach a state of having completed the implementation of all the security measures at the Basic Sophistication Level (Level 1). Upon reaching this stage, the operator is still expected to update and maintain its security measures in order to reflect those actions required to address any emerging threats thus preventing the likelihood of occurrence of such incidents. As part of the implementation process, providers are required to prepare a report for the Authority providing evidence of the measures implemented.

Milestone 3: Reachable after three years: Providers shall carry out an audit in line with the requirements proposed under Proposals 5 and 6. The purpose of this audit is to obtain an independent assessment of the security measures taken by the provider.

Upon reaching Milestone 3, providers are expected to, on the basis as proposed under Proposal 1, carry out regular risk assessments, or update their existing risk assessments as the case may be, and provide the relevant documentation to the Authority.

6.1 New Market Entrants

It is proposed that for providers of electronic communication networks and service providers established after the publication of the final decision notice is published shall be subject to the terms of the published Decision.

On considering the natural growth of a provider in terms of the development of the network and its growth of marketshare it would gradually transition to operate assets which are not critical up to assets which are classified as Category A. During this process, the requirements presented in this framework will also increase gradually for new market entrants.

Consultation Questions	
SM 13	What are your views on the proposed implementation timelines?

7 Invitation to Comments

In accordance with article 4A of the Malta Communications Authority Act [Cap. 418 of the Laws of Malta], the Authority invites written comments and representations from interested parties and stakeholders during the national consultation period, which shall run from the 6th January 2023 till the 3rd March 2023.

The Authority appreciates that respondents may provide confidential information in their feedback to this Consultation document. This information is to be included in a separate Annex and should be clearly marked as **confidential**. Respondents are also requested to state the reasons why the information should be treated as confidential.

For the sake of transparency, the Authority may publish a list of all respondents to this Consultation on its website, within three days following the deadline for responses. The Authority will take the necessary steps to protect the confidentiality of all such material as soon as it is received, in accordance with the Authority's confidentiality guidelines and procedures[8]. Respondents are, however, encouraged to avoid confidential markings wherever possible.

All responses should be submitted electronically to the Authority on consultations@mca.org.mt and addressed to the Chief Executive Officer.

Extensions to the consultation deadline will only be permitted in exceptional circumstances and only where the Authority deems fit. The MCA reserves the right to grant or refuse any such request at its discretion. Requests for extensions are to be made in writing within the first ten (10) working days of the consultation period.

[8] http://www.mca.org.mt/sites/default/files/articles/confidentialityguidelinesFINAL_0.pdf

Appendix – 1 Detailed Security Measures

Domain 1 – Governance and Risk Management

Electronic communication networks and service providers are required to have documented policies and processes identifying the key assets to deliver the network and/or service, the associated risks and mitigation measures. These assessments should extend towards risks which could be inherent in the supply chain of the provider.

Security Objective 1: Information security policy

	Security measures	Evidence
1	a) Set a high-level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. ii. Key personnel are aware of the security policy and its objectives (interview).
2	c) Set detailed information security policies for critical assets and business processes. d) Make all personnel aware of the security policy and what it implies for their work. e) Review the security policy following incidents.	iii. Documented information security policies, approved by management, including applicable law and regulations, accessible to personnel. iv. Personnel are aware of the information security policy and what it implies for their work (interview). v. Review comments or change logs for the policy.
3	f) Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	vi. Information security policies are up to date and approved by senior management. vii. Logs of policy exceptions, approved by the relevant roles. viii. Documentation of review process, taking into account changes and past incidents.

Security objective 2: Governance and risk management

	Security measures	Evidence
1	a) Set a high level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security of networks and services ii. Key personnel know the main risks (interview).
2	c) Set detailed information security policies for critical assets and business processes d) Set up a risk management methodology and/or tools based on industry standards. e) Ensure that key personnel use the risk management methodology and tools. f) Review the risk assessments following changes or incidents. g) Ensure residual risks are accepted by management.	iii. Documented risk management methodology and/or tools. iv. Guidance for personnel on assessing risks. v. List of risks and evidence of updates/reviews. vi. Review comments or change logs for risk assessments. vii. Management approval of residual risks.
3	h) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	viii. Information security policies are up to date and approved by senior management. ix. Logs of policy exceptions, approved by the relevant roles. x. Documentation of review process, taking into account changes and past incidents.

Security objective 3: Security roles and responsibilities

	Security measures	Evidence
1	a) Assign security roles and responsibilities to personnel. b) Make sure the security roles are reachable in case of security incidents.	i. List of security roles (CISO, DPO, business continuity manager, etc.), who occupies them and contact information.
2	c) Personnel is formally appointed in security roles. d) Make personnel aware of the security roles in your organisation	ii. List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles (CISO, DPO, etc.).

	and when they should be contacted.	iii. Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
3	e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	iv. Up-to-date documentation of the structure of security role assignments and responsibilities v. Documentation of review process, taking into account changes and past incidents.

Security objective 4: Security of third party assets

Security measures		Evidence
1	a) Include security requirements in contracts with third-parties.	i. Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centres, interconnections, shared facilities, etc.
2	b) Set a security policy for contracts with third-parties. c) Ensure that all procurement of services/products from third-parties follows the policy. d) Review security policy for third parties, following incidents or changes. e) Demand specific security standards in third-party supplier's processes during procurement. f) Mitigate residual risks that are not addressed by the third party.	ii. Documented security policy for contracts with third parties. iii. List of contracts with third-parties. iv. Contracts for third party services contain security requirements, in line with the security policy for procurement. v. Review comments or change logs of the policy. vi. Contracts with equipment suppliers contain requirements for adhering to security best practices and industry standards[9]. vii. Residual risks resulting from dependencies on third parties are listed and mitigated.

[9] This should include demonstrating quality levels of information security processes, security maintenance of products and equipment throughout its lifetime and built-in of security in the product development processes.

3	g) Keep track of security incidents related to or caused by third-parties. h) Periodically review and update security policy for third parties at regular intervals, taking into account past incidents, changes, etc.	viii. List of security incidents related to or caused by engagement with third-parties. ix. Documentation of review process of the policy.

Domain 2 – Human Resources Security

Providers of electronic communications networks and services depend on the human beings who effectively implement and operate the security manual of the organisation. Therefore, an electronic network and services provider exercises diligence in selecting its staff, provide them with adequate awareness and training about the security policies in place. Since things could one day go wrong, adequate procedures are necessary to cater for such eventuality.

Security objective 5: Background checks

	Security measures	Evidence
1	a) Check professional references of key personnel (system administrators, security officers, guards, etc.).	i. Documentation of checks of professional references for key personnel.
2	b) Perform background checks/screening for key personnel, when needed and legally permitted. c) Set up a policy and procedure for background checks.	ii. Policy and procedure for background checks/screenings. iii. Guidance for personnel about when/how to perform background checks/screenings.
3	d) Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	iv. Review comments or change logs of the policy/procedures.

Security Objective 6: Security knowledge and training

	Security measures	Evidence
1	a) Provide key personnel with relevant training and material on security issues.	i. Key personnel have followed security trainings and have sufficient security knowledge (interview).
2	b) Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. c) Organise trainings and awareness sessions for personnel on security	ii. Personnel have participated in awareness sessions on security topics. iii. Documented program for training on security skills, including, objectives for different roles and how to reach it (by e.g.

	topics important for your organisation.	training, awareness raising, etc.).
3	d) Review and update the training program periodically, taking into account changes and past incidents. e) Test the security knowledge of personnel.	iv. Updated security awareness and training program v. Results of tests of the security knowledge of personnel. vi. Review comments or change logs for the program.

Security Objective 7: Personnel changes

Security measures		Evidence
1	a) Following changes in personnel revoke access rights, badges, equipment, etc., if no longer necessary or permitted. b) Brief and educate new personnel on the policies and procedures in place.	i. Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, etc. ii. Evidence that new personnel has been briefed and educated about policies and procedures in place.
2	c) Implement policy/procedures for personnel changes, taking into account timely revocation of access rights, badges and equipment. d) Implement policy/procedures for education and training for personnel in new roles.	iii. Documentation of process for personnel changes, including, responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles. iv. Evidence that personnel changes have been carried out according to the process and that access rights have been updated timely (e.g. checklists).
3	e) Periodically check that the policy/procedures are effective. f) Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents.	v. Evidence of checks of access rights etc. vi. Up to date policy/procedures for managing personnel changes. vii. Review comments or change logs.

Security Objective 8: Handling violations

	Security measures	Evidence
1	a) Hold personnel accountable for security incidents caused by violations of policies, for example via the employment contract.	i. Rules for personnel, including responsibilities, code of conduct, violations of policies, etc., possibly as part of employment contracts.
2	b) Set up procedures for violations of policies by personnel.	ii. Documentation of procedures, including types of violations which may be subject to disciplinary actions, and which disciplinary actions may be taken.
3	c) Periodically review and update the disciplinary process, based on changes and past incidents.	iii. Review comments or change logs

Domain 3 – Security of Systems and Facilities

Security Objective 9: Physical and environmental security

	Security measures	Evidence
1	a) Prevent unauthorised physical access to facilities and infrastructure and set up adequate environmental controls, to protect provider assets[10] against unauthorised access, burglary, fire, flooding, etc.[11]	i. Basic implementation of physical security measures and environmental controls , such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, etc.
2	b) Implement a policy for physical security measures and environmental controls. c) Industry standard implementation of physical and environmental controls. d) Apply reinforced controls for physical access to critical assets[12].	ii. Documented policy for physical security measures and environmental controls, including description of facilities and systems in scope. iii. Physical and environmental controls, like electronic control of entrance and audit trail, segmentation of spaces according to authorisation levels, automated fire extinguishers with halocarbon gases, etc. iv. The policy includes lists of critical assets and reinforced physical controls for accessing these assets.
3	e) Evaluate the effectiveness of physical and environmental controls periodically. f) Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents.	v. Up to date policy for physical security measures and environmental controls vi. Documentation about evaluation of environmental control, review comments or change logs.

[10] Including third party assets, where applicable.

[11] Security controls should be selected based on the risk assessment, which should also take in consideration current and forecasted environmental security risks – e.g. related to climate change.

[12] For example, physical access to such assets should only be granted to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored.

Security Objective 10: Security of supplies

Security measures			Evidence	
1	a)	Ensure security of critical supplies.	i.	Security of critical supplies is protected in a basic way, for example, backup power and/or backup fuel is available.
2	b) c)	Implement a policy for security of critical supplies. Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.).	ii. iii.	Documented policy to protect critical supplies such as electrical power, fuel, etc., describing different types of supplies, and the security measures protecting the supplies. Evidence of industry standard measures to protect the security of critical supplies
3	d) e)	Implement state of the art security measures to protect critical supplies (such as active cooling, UP, hot standby power generators, SLAs with fuel delivery companies, redundant cooling and power backup systems). Review and update policy and procedures to secure critical supplies regularly, taking into account changes and past incidents.	iv. v.	Evidence of state of the art measures to protect security of critical supplies. Updated policy for securing critical supplies and supporting facilities, review comments and/or change logs.

Security Objective 11; Access control to network and information systems

Security measures			Evidence	
1	a) b)	Users and systems have unique ID's and are authenticated before accessing services or systems. b) Implement logical access control mechanism for network and information systems to allow only authorised use.	i. ii.	Access logs show unique identifiers for users and systems when granted or denied access. Overview of authentication and access control methods for systems and users.
2	c)	Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and	iii.	Access control policy including description of roles, groups,

	procedures for assigning and revoking access rights. d) Choose appropriate authentication mechanisms, depending on the type of access. e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations. f) Reinforce controls for remote access to critical assets of network and information systems by third parties.	access rights, procedures for granting and revoking access. iv. Different types of authentication mechanisms for different types of access. v. Log of access control policy violations and exceptions, approved by the security officer. vi. Principles of least privilege and segregation of duties are documented and applied where appropriate. vii. Remote access to critical assets by third-parties is minimised and subjected to strict access controls, including state of the art authentication, authorisation and auditing controls, especially for privileged accounts.
3	g) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. h) Access control policy and access control mechanisms are reviewed and when needed revised.	viii. Reports of (security) tests of access control mechanisms. ix. Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). x. Logs of intrusion detection and anomaly detection systems. xi. Updates of access control policy, review comments or change logs. xii. Documented risk analysis for the application of logging and retention xiii. Procedures to ensure that access controls are in effect all the time and that they evolve with the network.

Security Objective 12: Integrity of network and information systems

	Security measures	Evidence
1	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls. b) Check for malware on (internal) network and information systems.	i. Software and data in network and information systems is protected using input controls, firewalls, encryption and signing. ii. Malware detection systems are present, and up to date.

2	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems. d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks.	iii. Documentation about how the protection of software and data in network and information system is implemented. iv. Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). v. Logs of intrusion detection and anomaly detection systems. vi. Adequate tools and processes to ensure software integrity[13] when performing software updates and applying security patches to critical assets in virtualised networks.
3	e) Set up state of the art controls to protect integrity of systems. f) Evaluate and review the effectiveness of measures to protect integrity of systems.	vii. State of the art controls to protect integrity of systems, such as code signing, tripwire, etc. viii. Documentation of process for checking logs of anomaly and intrusion detection systems.

Security Objective 13 – User of Encryption

	Security measures	Evidence
1	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data[14] during its storage in and/or transmission via networks.	i. Description of main data flows, and the encryption protocols and algorithms used for each flow. ii. Description of justified exclusions and limitations[15] in implementing encryption.
2	b) Implement encryption policy. c) Use industry standard encryption algorithms and the corresponding	iii. Documented encryption policy including details about the cryptographic algorithms and corresponding cryptographic keys,

[13] Including reliable identification, monitoring and tracking of changes and the status of patches.

[14] The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents.

[15] Ability to implement encryption may also be influenced by technological limitations, like in the case of legacy networks or when old equipment and network protocols are used.

	recommended lengths of encryption keys.	according to international best practices and standards. iv. Documented justified exclusions that provide rationale for when data is not encrypted, including the related impact assessment.
3	d) Review and update of encryption policy. e) Use state of the art encryption algorithms.	v. Updated encryption policy, review comments and/or change logs. vi. Encryption policy includes details about the state of the art cryptographic protocols used.

Security Objective 14: Protection of security of critical data

	Security measures	Evidence
1	a) Make sure that cryptographic key material, shared secrets and passwords and similar security-critical data is not disclosed or tampered with. b) Access to private keys is strictly controlled and monitored.	i. Security critical data is protected using security best practices and standards for protection mechanisms (like split knowledge and dual control, encryption, hashing, secure hardware etc.). ii. Description of mechanisms for controlling and monitoring access to private keys.
2	c) Implement policy for management of cryptographic keys. d) Implement policy for management of user passwords.	iii. Key management policy including roles, responsibilities and controls for the use, protection and lifetime of cryptographic keys throughout their life cycle including controls for access to and backup and recovery of private keys. iv. User password management policy including processes, methods and techniques for secure storing of user passwords using industry best practices[16].
3	e) Review and update of key management policy. f) Review and update of user password management policy.	v. Updated key management policy, review comments and/or change logs. vi. Updated user password management policy, review comments and/or change logs.

[16] E.g. hashing using appropriate hashing algorithms, salting etc.

Domain 4 – Operations management

Security Objective 15: Operational procedures

	Security measures	Evidence
1	a) Set up operational procedures and assign responsibilities for operation of critical systems.	i. Documentation of operational procedures and responsibilities for key network and information systems.
2	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures.	ii. Documented policy for operation of critical systems, including an overview of network and information systems in scope.
3	c) Review and update the policy/procedures for operation of critical systems, taking into account incidents and/or changes.	iii. Updated policy/procedures for critical systems, review comments and/or change logs.

Security Objective 16: Change management

	Security measures	Evidence
1	a) Follow predefined methods or procedures when making changes to critical systems	i. Documentation describing predefined methods or procedures followed when making changes to critical systems.
2	b) Implement policy/procedures for change management, to make sure that changes of critical systems are always done following a predefined way. c) Document change management procedures, and record for each change the steps of the followed procedure.	ii. Documentation of change management policy/procedures including, systems subject to the policy, objectives, roll back procedures, etc. iii. For each change, a report is available describing the steps and the result of the change.
3	d) Review and update change management procedures regularly, taking into account changes and past incidents.	iv. Up to date change management procedures, review comments and/or change logs.

Security Objective 17: Asset management

	Security measures	Evidence
1	a) Identify critical assets and configurations of critical systems.	i. List of critical assets and critical systems. The list should include all critical assets and critical systems for network or service, operational and security, including relevant third party assets.
2	b) Implement policy/procedures for asset management and configuration control.	ii. Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, the objectives of asset management. iii. An asset inventory or inventories, containing critical assets and the dependency between assets. iv. A configuration control inventory or inventories, containing configurations of critical systems.
3	c) Review and update the asset management policy regularly, based on changes and past incidents.	v. Up to date asset management policy/procedures, review comments and/or change logs.

Domain 5 – Incident management

Providers of electronic communication networks and services should ensure effective and tested processes which address and minimise potential disruption to networks and services in case of an incident.

Security Objective 18: Incident management procedures

	Security measures	Evidence
1	a) Make sure personnel is available and prepared to manage and handle incidents. b) Keep a record of all major incidents.	i. Personnel is aware of how to deal with incidents and when to escalate. ii. Inventory of major incidents and per incident, impact, cause, actions taken and lessons learnt.
2	c) Implement policy/procedures for managing incidents.	iii. Policy/procedures for incident management, including, types of incidents that could occur, objectives, roles and responsibilities, detailed description, per incident type, how to manage the incident, when to escalate to senior management (e.g. CISO) etc.
3	d) Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident. e) Evaluate incident management policy/procedures based on past incidents.	iv. Individual reports of the handling of major incidents. v. Up to date incident management policy/procedures, review comments and/or change logs.

Security Objective 19: Incident detection capability

	Security measures	Evidence
1	a) Set up processes or systems for incident detection.	i. Documented examples of past incidents that were detected and timely forwarded to the appropriate people.
2	b) Implement industry standard systems and procedures for incident detection. c) Implement systems and procedures for registering and forwarding	ii. Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, security helpdesk for personnel, reports and advisories from Computer Emergency

	incidents timely to the appropriate people.	Response Teams (CERTs), tools to spot anomalies, etc. iii. Network Operation Centres (NOC) and/or Security Operation Centres (SOC)[17] for ensuring visibility and effective network monitoring and to detect anomalies and to identify and avoid threats.
3	d) Review systems and processes for incident detection regularly and update them taking into account changes and past incidents. e) Implement state of the art systems and procedures for incident detection.	iv. Up to date documentation of incident detection systems and processes. v. Documentation of review of the incident detection process, review comments, and/or change logs. vi. NOC/SOC solutions with state of the art capabilities are used - e.g. SOAR (Security Orchestration, Automation and Response), ensuring integration with threat and vulnerability management and incident response function, security operations automation etc.

Security Objective 20: Incident reporting and communication

Security measures		Evidence
1	a) Communicate and report about ongoing or past incidents to third parties, customers, and/or government authorities, when necessary.	i. Evidence of past communications and incident reporting.
2	b) Implement policy and procedures for communicating and reporting about incidents.	ii. Documented policy and procedures for communicating and reporting about incidents, describing reasons/motivations for communicating or reporting (business reasons, legal reasons etc.), the type of incidents in scope, the required content of communications, notifications or reports, the channels to be used, and the roles responsible for

[17] Where justified on the basis of the actual assessment of the security risks involved, operators should run their NOC and/or SOC on premise, inside the country and/or inside the EU.

		communicating, notifying and reporting. iii. Templates for incident reporting and communication.
3	c) Evaluate past communications and reporting about incidents. d) Review and update the reporting and communication plans, based on changes or past incidents.	iv. List of incident reports and past communications about incidents. v. Up to date incident response and communication policy, review comments, and/or change logs.

Domain 6 – Business continuity management

Providers of electronic communication networks and services should ensure effective and tested processes which address and minimise potential disruption to networks and services in case of an incident.

Security Objective 21: Service continuity strategy and contingency plans

	Security measures	Evidence
1	a) Implement a service continuity strategy for the communications networks and/or services provided.	i. Documented service continuity strategy, including recovery time objectives for key services and processes
2	b) Implement contingency plans for critical systems. c) Monitor activation and execution of contingency plans, registering successful and failed recovery times. d) Implement contingency plans for dependent and inter-dependent critical sectors and services[18].	ii. Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives. iii. Decision process for activating contingency plans. iv. Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time. v. Map of critical sectors and services essential for and/or dependent on the continuity of the network and service operation and contingency plans for mitigating the impact related to dependent and interdependent sectors and services.
3	e) Review and revise service continuity strategy periodically.	vi. Up to date continuity strategy and contingency plans, review comments, and/or change logs.

[18] When determining dependent critical sectors and services, providers may take into account those services that are dependent on the continuity of the network and service operation which are essential for the maintenance of critical societal and/or economic activities and for which an incident would have significant disruptive effects on the provision of that service. One possible way for identifying such dependent services may be to pass the obligation to service consumers to inform the providers if their service is considered critical.

	f) Review and revise contingency plans, based on past incidents and changes.	

Security Objective 22: Disaster recovery capabilities

	Security measures	Evidence
1	a) Prepare for recovery and restoration of services following disasters.	i. Measures are in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, etc.[19]
2	b) Implement policy/procedures for deploying disaster recovery capabilities. c) Implement industry standard disaster recovery capabilities. or be assured they are available from third parties (such as national emergency networks).	ii. Documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third parties). iii. Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, etc.
3	d) Set up state of the art disaster recovery capabilities to mitigate natural and/major disasters. e) Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	iv. State of the art disaster recovery capabilities, such as full redundancy and failover mechanisms to handle natural and/or major disasters. v. Updated documentation of disaster recovery capabilities in place, review comments and/or change logs

[19] Not all of the listed evidence may be applicable in scenarios with large geographically extended national Telco networks, for assets offering direct connectivity to end users

Domain 7 – Monitoring, auditing and testing

Providers of electronic communication networks and services are expected to have in place processes which continuously assess the adequacy of the measures taken in view of organisational evolution, network improvement and changes in threats

Security Objective 23: Monitoring and logging policies

	Security measures	Evidence
1	a) Implement monitoring and logging of critical systems.	i. Logs and monitoring reports of critical network and information systems.
2	b) Implement policy for logging and monitoring of critical systems. c) Set up tools for monitoring critical systems d) Set up tools to collect and store logs of critical systems.	ii. Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs. iii. Tools for monitoring systems and collecting logs. iv. List of monitoring data and log files, in line with the policy.
3	e) Set up tools for automated collection and analysis of monitoring data and logs. f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	v. Tools to facilitate structural recording and analysis of monitoring and logs. vi. Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs.

Security Objective 24: Exercise contingency plans

	Security measures	Evidence
1	a) Exercise and test backup and contingency plans to make sure systems and processes work and personnel is prepared for large failures and contingencies.	i. Reports of past exercises of backup and contingency plans.
2	b) Implement program for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over time. c) Make sure that the issues and lessons learnt from exercises are	ii. Exercise program for backup and contingency plans, including types of contingencies, frequency, roles and responsibilities, templates and procedures for conducting exercises, templates for exercise reports.

	addressed by the responsible people and that the relevant processes and systems are updated accordingly.	iii. Reports about exercises and drills showing the execution of contingency plans, including lessons learnt from the exercises. iv. Issues and lessons learnt from past exercises have been addressed by the responsible people
3	d) Review and update the exercise plans, taking into account changes and past incidents and contingencies which were not covered by the exercise program. e) Involve suppliers, and other 3rd parties, like business partners or customers in exercises.	v. Updated exercises plans, review comments, and/or change logs. vi. Input from suppliers and other 3rd parties involved about how to improve exercise scenarios.

Security Objective 25: Network and information systems testing

	Security measures	Evidence
1	a) Test networks and information systems before using them or connecting them to existing systems.	i. Test reports of the network and information systems, including tests after big changes or the introduction of new systems. Ii
2	b) Implement policy/procedures for testing network and information systems, c) Implement tools for automated testing	ii Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test report templates
3	d) Review and update the policy/procedures for testing, taking into account changes and past incidents.	iii. List of test reports. iv. Updated policy/procedures for testing networks and information systems, review comments, and/or change log.

Security Objective 26: Security assessments

Security measures		Evidence
1	a) Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes. .	i. Reports from past security scans and security tests.
2	b) Implement policy/procedures for security assessments and security testing.	ii. Documented policy/procedures for security assessments and security testing, including, which assets, in what circumstances, the type of security assessments and tests, frequency, approved parties (internal or external), confidentiality levels for assessment and test results and the objectives security assessments and tests.
3	c) Evaluate the effectiveness of policy/procedures for security assessments and security testing. d) Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents.	iii. List of reports about security assessment and security tests. iv. Reports of follow up actions on assessment and test results. v. Up to date policy/procedures for security assessments and security testing, review comments, and/or change log.

Security Objective 27: Compliance monitoring

Security measures		Evidence
1	a) Monitor compliance to standards and legal requirements.	i. Reports describing the result of compliance monitoring.
2	b) Implement policy/procedures for compliance monitoring and auditing.	ii. Documented policy/procedures for monitoring compliance and auditing, including what (assets, processes, infrastructure), frequency, guidelines who should carry out audits (in- or external), relevant security policies that are subject to compliance monitoring and auditing, the objectives and high level approach of compliance monitoring and auditing, templates for audit reports.

		iii. Detailed monitoring and audit plans, including long term high level objectives and planning
3	c) Evaluate the policy/procedures for compliance and auditing. d) Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents.	iv. List of all compliance and audit reports v. Updated policy/procedures for compliance and auditing, review comments, and/or change logs.

Domain 8 – Threat Awareness

Providers of electronic communication networks and services should perform regular threat monitoring and reach out for their subscribers and end-users to share information about major threats to the security of networks and services.

Security Objective 28: Threat intelligence

	Security measures	Evidence
1	a) Perform regular threat monitoring.	i. Regular monitoring of external threat intelligence feeds (OSINT, commercial feeds, security researches etc.[20]) with a recorded log of relevant significant threat events. ii. Informal and ad-hoc sharing of relevant threat intelligence with relevant organisations on bi-lateral basis.
2	b) Implement threat intelligence program.	iii. Documented and implemented threat intelligence program that includes roles, responsibilities, procedures and mechanisms for collecting information related to significant threats and corresponding mitigation measures. iv. The program also includes mechanisms for systematic sharing of threat intelligence with

[20] Information sources should be relevant, current and credible and may include known threat intelligence reports, such as ENISA Threat Landscape (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape) or various other threat reports by commercial entities, industry associations or academia.

		relevant organisation on bi-lateral and multi-lateral basis using a dedicated threat intelligence sharing platform (e.g. MISP). v. Appropriate information marking scheme in place for facilitation of sharing of sensitive threat information (e.g. TLP).
3	c) Review and update the threat intelligence program. d) Threat intelligence program makes use of state of the art threat intelligence systems.	vi. Updated threat intelligence program, review comments and/or change logs. vii. Threat intelligence platform (TIP) with state of the art functionality is used (e.g. consolidation of threat intelligence feeds from various sources, automation, security analytics and integration with other security tools etc.)

Security Objective 29: Informing users about threats

	Security measures	Evidence
1	a) Inform end-users of communication networks and services about particular and significant security threats to network or service that may affect the end-user.	i. Security bulletin, a dedicated threat information web page or another documented and tested mechanisms for reaching out to end-users in the case of significant threats. ii. Documented lists of best practices and security recommendations for end-users to mitigate typical risks (e.g. encryption, strong authentication, updates, backups, user awareness etc.).
2	b) Implement policy/procedures for regular update of end-users about security threats to network or service that may affect the end-user	iii. Documented and implemented end-user outreach policy with defined roles and responsibilities, mechanisms and criteria for identifying significant threats and the procedures, tools and methods for timely and appropriate informing of end-users. iv. The policy includes mechanisms for identifying and sharing the recommendations and best practices for end-users to mitigate specific threats.

3	c) Review and update the policy/procedures for regular update of end-users about security threats to network or service that may affect the end-user.	v. Updated outreach policy, review comments and/or change logs.

Appendix – 2 Further Consultation - Exploring the benefits of introducing the Corporate CSIRT function

As security threats and their sophistication increase, there is an ever-increasing need for providers of electronic communication networks and services to have structures in place such that they are capable for a rapid response in case of an incident. A CSIRT is a team of security experts with the main task being to respond to security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches. Having a dedicated security team helps an organisation to mitigate and prevent major incidents and helps to protect its valuable assets.

The second objective of a CSIRT is achieved through networking with other similar bodies, both locally and abroad, covering the sector and its supply chain. This network supplies the provider with information about vulnerabilities which are either trending or which have just been discovered. This information may provide an early warning system allowing the unaffected provider to prepare its mitigation measures, thus rendering its network more robust towards such vulnerabilities

The Authority is undergoing a process in which it is analysing the cost-benefit of requiring at least those providers which operate critical assets of Category A to formally set up a CSIRT structure to improve the positioning of their network and be in a better position to navigate their threat landscape. While the Authority may, in the future, issue a public consultation on the matter as necessary before considering formally this obligation, it is now seeking feedback on some specific aspects mainly related to the services to be provided by the CSIRT and its possible setup.

The Authority is considering the following set of services that would have to be provided by the CSIRT:

a) monitoring incidents of assets, systems, or networks;
b) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
c) responding to incidents;
d) Providing dynamic risk and incident analysis and situational awareness.

The Authority is also evaluating the following two possible ways of how this CSIRT function is to be set up namely that:

a) Each provider is to set up and finance its own CSIRT function. This would be the most straight forward operation which while being the most expensive, it also assures protection of the most private but of course the most expensive; or .

b) The providers may opt to outsource the whole function and benefit from the economies of scale that such operation normally brings about.

Consultation Questions (applicable only to providers of ECS and ECN)	
SM 14	What operational structures does your organisation have in place which resemble any or all of the above functionalities?
SM 15	What functions listed above are not relevant in the electronic communications sectors?

Appendix – 3 Consultation Questions

Consultation Questions	
SM 1	What are your views on the proposed requirement for providers to carry out security and integrity risk assessments every three years, with intermediate revisions every year?
SM 2	What are your views on the elements that need to be captured in a risk assessment report?
SM 3	What are your views about the identified criteria which would influence the validity of a risk assessment? Do you suggest the inclusion or ommission of additional elements in this list? Please provide a detailed justification
SM 4	What are your views on the reporting requirements proposed?
SM 5	If you are an ECS and/or ECN provider, how do the proposed requirements of a risk assessment differ from those of your organisation? Conversely, how similar are they?
SM 6	What are your views on the security objectives presented?
SM 7	What are your views on the necessary documentation to be maintained by the providers?
SM 8	What are your views on the proposal requiring providers to implement the Basic Sophistication Level as a minimum for all the security objectives?
SM 9	What are your views on the tiered approach towards the minimum security mitigation to be implemented by providerse operating Category A and Category B assets.
SM 10	If you are an ECS and/or ECN provider, how does the documentation required differ from that held within your organisation?
SM 11	What are your views of auditing the implementation of security measures every two years?
SM 12	What are your views on the proposed process related to security audits?
SM 13	What are your views on the proposed implementation timelines?
SM 14	What operational structures does your organisation have in place which resemble any or all of the above functionalities?
SM 15	What functions listed above are not relevant in the electronic communications sectors?

MALTA COMMUNICATIONS AUTHORITY

☎ (+356) 2133 6840
@ info@mca.org.mt
www.mca.org.mt
Valletta Waterfront, Pinto Wharf,
Floriana FRN1913, Malta