GRA

GIBRALTAR REGULATORY AUTHORITY

Network and Information Systems General Guidance for Operators of Essential Services

Date 6th May 2022

CS 02/22

FOREWORD

This guidance is for Operators of Essential Services ("OESs"), as designated by the Gibraltar Regulatory Authority ("GRA") under section 35(2) of the Civil Contingencies Act 2007 (the "Act"), and for Digital Service Providers ("DSPs") under section 43 of the Act.

This guidance sets out an overview of the requirements OESs and DSPs need to consider to comply with their obligations under sections 41, 42 and 43 of the Act respectively.

This guidance is issued in accordance with the duties of the GRA in its role as the Competent Authority, as provided in section 54 of the Act.

CONTENTS

Executive Summary

The European Union ("EU") 2016/1148 Directive on Security of Network and Information Systems (the "NIS Directive"), provides legal measures to protect essential services and infrastructure by improving the security of their network and information systems ("NIS") used by those administering these.

The main objective of the NIS Directive, formally transposed into Gibraltar legislation on 10th May 2018 and found in Part 7 of the Civil Contingencies Act 2007 (the "Act"), is to ensure that there is a common high-level security of network and information systems across Member States and as such, it requires Member States to take a number of significant measures with regard to cyber security.

Although Gibraltar is no longer in the EU, the requirements contained in the Act still play a key part in ensuring that Gibraltar has in place, an effective cyber security framework to protect Gibraltar's critical national infrastructure.

The measures required include the application of a set of binding network and information system security and incident reporting obligations to a wide range of critical infrastructure operators, termed 'Operators of Essential Services' ("OESs") including energy, health, transport, drinking water supply and distribution, banking, financial market infrastructure and digital infrastructure. The measures are also applicable to providers of digital services, termed Digital Service Providers ("DSPs"), who provide an online marketplace, online search engine and cloud computing services.

Section 54 of the Act allows the Gibraltar Regulatory Authority (the "GRA") to issue guidance for the purpose of providing information and advice as regards compliance by OESs and relevant DSPs with their obligations under the Act ("Guidance Notes"). This document establishes a set of cyber security principles ("Principles") designed to assist OESs and DSPs in meeting their network and information system ("NIS") security and incident reporting requirements under section 41,42 and 43 of the Act.

The Principles are both technology neutral and non-sector specific to allow OESs in different sectors to adapt these to meet their needs, and to evolve their sector specific response along with technological advances and business requirements.

While these Principles were developed to improve cyber security risk management and incident response in OESs in accordance with their obligations under the Act, the Principles enable organisations, regardless of size, degree of cyber security risk, or cyber security sophistication, to apply these and best practices to improve security and resilience.

The Principles are not a universal approach to managing cyber security risk for critical infrastructure. Many sectors will have unique risks, threats and vulnerabilities which require a sector specific approach. The fundamental aim of the Principles is to establish cross-sectoral measures to create a high common level of security of NIS in Gibraltar.

Introduction

1.1 Competent Authority

Section 38 of the Act designates the GRA as the Competent Authority for the security of NIS in respect of designated OESs.

Additionally, the Act also designates the GRA as the single point of contact for the security of NIS for Gibraltar with the main role of facilitating cross-border cooperation and communication.

1.2 Identification and designation of Operators of Essential Services

Section 35 allows the GRA to designate a person as an operator of essential services ("OES") where it is satisfied that:

(a) the person provides a service which is essential for the maintenance of critical societal or economic activities (an "essential service");

(b) the provision of that essential service by that person relies on NIS; and

(c) if in the GRA's view, an incident affecting the provision of that essential service by that person is likely to have significant disruptive effects on the provision of that essential service.

Before designating a person as an OES, the GRA must have regard to the following factors:

i. the number of users relying on the service provided by the person;

ii. the degree of dependency of the other relevant sectors on the service provided by that person;

iii. the likely impact of incidents on the essential service provided by that person, in terms of its degree and duration, on economic and societal activities or public safety;

iv. the market share of the essential service provided by that person;

v. the geographical area that may be affected if an incident impacts on the service provided by that person;

vi. the importance of the provision of the service by that person for maintaining a sufficient level of that service, taking into account the availability of alternative means of essential service provision; and

vii. any other factor the GRA considers appropriate to have regard to.

When designating an OES, the GRA must serve a notice on the person who is to be designated and provide reasons for the designation in the notice. Before the GRA designates a person as an OES, the GRA may request information from that person under section 48(1) of the Act and invite the person to submit any written representations about the proposed decision to designate it as an OES.

1.3 Information notices

Section 48 of the Act provides the GRA with powers to serve an information notice to OESs to assess the security of their NIS, including its documented security policies, the OES' compliance with section 41 of the Act, and the implementation of its security policies, including information about inspections conducted under section 49 of the Act, and any underlying evidence in relation to such an inspection.

1.4 Power of inspection

The powers granted to the GRA under section 49 of the Act allows for inspections of OESs. The GRA can also appoint an inspector to conduct the inspection on the GRA's behalf, as well as directing an OES to appoint an inspector approved by the GRA.

Section 49 mandates that OESs pay the reasonable costs of the inspection and that it co-operates with the person conducting the inspection, as well as allowing reasonable access to their premises. An OES must also allow the inspector to carry out its duties relevant to the inspection by allowing the copying or removing of documents, including information held electronically. Furthermore, an OES must allow the inspector access to any person should the inspector seek any information relevant to the inspection.

Operators of Essential Services

2.1 Security Requirements

Section 41 of the Act sets out the NIS obligations for OESs.

OESs must:

- take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of NIS which it uses in its operations; and

- take appropriate measures to prevent and minimise the impact of incidents affecting the security of NIS used by it for the provision of the essential services in respect of which it is designated as an OES, with a view to ensuring the continuity of the provision by it of those services.

Section 41(3) provides that the measures taken shall ensure a level of security of NIS appropriate to the risks posed. It will be the responsibility of the OES to demonstrate that they are complying with the security and incident notification obligations under the Act.

This Guidance Note offers a sample general approach for OESs and DSPs with regard to compliance with their obligations, identifying a best practice framework which if adopted, would be likely to achieve the outcomes set out in Section 41(1) and (2) of the Act. In doing so, the OES would be taking appropriate technical and organisational measures to manage risks posed to the security of NIS used in its operations and minimising the impact of incidents on those systems, with a view to ensuring the continuity of the essential services.

2.2 Considerations

It is recognised that it is not possible to fully protect information systems from all potential security incidents. Consequently, the security requirements in the Act are aimed at reducing risk throughout the incident response lifecycle and should not be considered to render systems or entities invulnerable. Furthermore, the enforcement provisions in the Act will apply where an OES has failed to introduce or properly apply appropriate NIS security measures, either in the normal course of events, or in the aftermath of an incident.

However, the fact that an OES may have experienced an incident does not automatically mean that further enforcement action will follow. Rather, the role of the GRA in these circumstances would be to consider whether an affected OES had properly assessed the risks to their service, was managing the assessed risks appropriately and appropriate security measures were in place.

Lastly, when OESs are formally designated as such, it will be with reference to the essential service or services that they provide. The security measures that the OES chooses to apply should specifically identify those NIS used for the provision or support of those essential services.

General Measures for Network and Information Systems Security

3.1 Measures

OESs should take the following into account when applying security measures and must ensure they are:

- **Effective -** in increasing the cybersecurity posture of an OES in relation to the threat landscape now and into the foreseeable future.
- **Tailored -** to ensure effort is applied to measures which will have the most impact in relation to enhancing the security of an OES.
- **Compatible -** to address cross-sectoral vulnerabilities, and complemented with sector specific security measures.
- **Proportionate -** to the risks, with an emphasis on protecting systems underpinning essential services.
- **Concrete -** and easy to understand, to ensure the measures are actually implemented in full and actively enhance the cybersecurity posture.
- **Verifiable -** to ensure it can provide the GRA with evidence of the effective implementation of security measures.
- **Inclusive** - to ensure measures are applied to cover all 4 objectives listed in paragraphs 4.1 below.

Overview of the Network and Information Systems Cyber Security Principles in respect of Operators of Essential Services security requirements

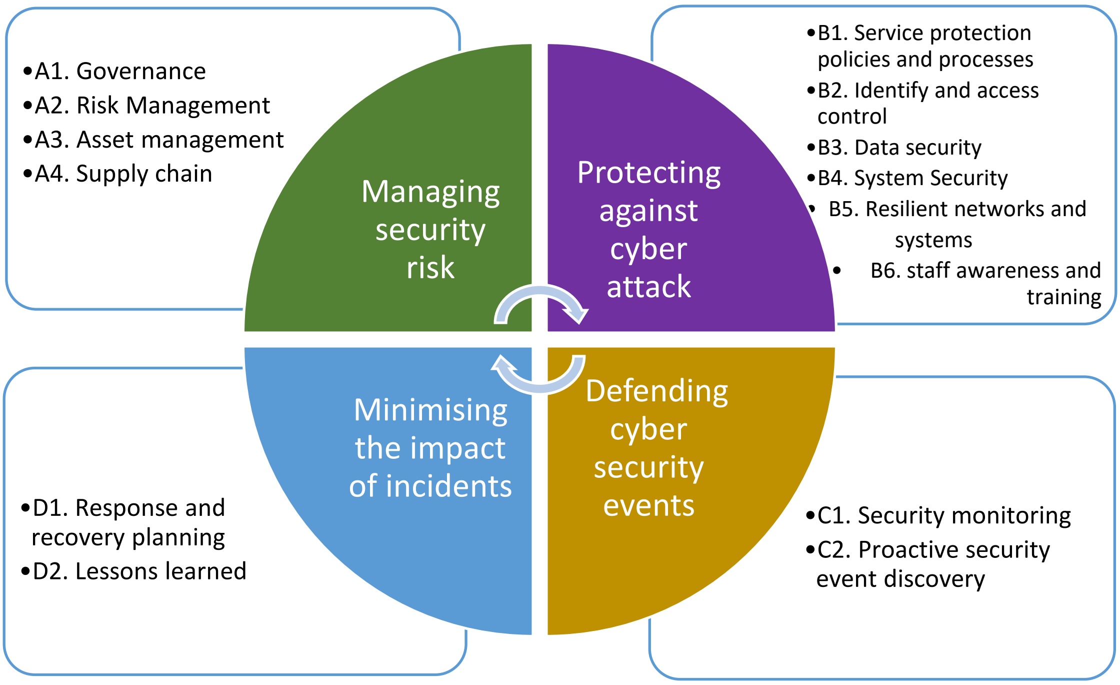
4.1 Cyber Assessment Framework

The technical and organisational measures which are identified in the 14 Principles outlined below offer a best practice framework for ensuring the protection of NIS. The Principles represent an approach that could be adopted by OESs to manage the risks posed to the security of NIS used in their operations and to minimise the impact of incidents affecting those systems.

The security Principles consist of 4 objectives which provide a high-level view of an organisation's management of cyber security risk. Each objective is accomplished by applying the relevant Principles related to it. These 4 objectives are:

- **Managing security risk;**
- **Protecting against cyber attack;**
- **Defending cyber security events; and**
- **Minimising the impact of incidents**.

Each objective has the following Principles associated to it:



Managing security risk

- A1. Governance
- A2. Risk Management
- A3. Asset management
- A4. Supply chain

Protecting against cyber attack

- B1. Service protection policies and processes
- B2. Identify and access control
- B3. Data security
- B4. System Security
- B5. Resilient networks and systems
- B6. staff awareness and training

Defending cyber security events

- C1. Security monitoring
- C2. Proactive security event discovery

Minimising the impact of incidents

- D1. Response and recovery planning
- D2. Lessons learned

This framework is designed to:

i. enable OESs to describe their current cyber security status;

ii. provide an outcome-focused approach of the security principles for NIS;

iii. be compatible with and complement existing risk management, standards and cyber security programs in use by OESs;

iv. enable the identification of effective cyber security improvement activities;

v. be as straightforward to apply as possible; and

vi. assist the GRA in carrying out effective security assessments (by means of inspection or otherwise) of the compliance by an OES with its obligations under Section 41 of the Act.

4.2 Non applicability

As the Principles are designed for use across multiple sectors and subsectors, the outcomes described may not be relevant in all situations. As a result, it will be the responsibility of individual OESs to determine how best to satisfy the security requirements under Section 41 of the Act.

4.3 Standardisation

The use of internationally accepted standards and specifications relevant to the security of NIS is encouraged in order to promote convergent implementations of the requirements in section 41 of the Act.

Managing Security Risk

OESs should develop the organisational understanding, structures, polices and processes to manage cyber security risk to the NIS of the organisation’s essential services, assets, data, and capabilities, as follows:

A1. Governance

The policies, procedures, and processes to manage and monitor the organisation’s regulatory, legal, risk, environmental, and operational requirements are identified, understood and documented, and inform the management of cyber security risk.

A2. Risk Management

Priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

A3. Asset Management

All systems and/or services that are required to deliver or support essential services should be identified, understood and documented. This includes data, personnel, devices, systems and facilities.

A4. Supply Chain Risk Management

Weaknesses in supplier security can be used to circumvent an organisation's internal controls. Processes are established and implemented to identify, assess and manage supply chain risks.

Defending Against Cyber Attack

B1. Service Protection Policies and Processes

Define, communicate and document appropriate policies, processes and procedures that direct the overall organisational approach to securing systems and data that support delivery of essential services.

B2. Identity and Access Control

Access to assets and associated facilities is limited to authorised users, processes, and devices, consistent with the principle of least privilege and is managed consistent with the assessed risk.

B3. Data Security

Information and records (data) are managed consistent with the risk strategy to protect the confidentiality, integrity, and availability of information and systems.

B4. System Security

All systems critical for the delivery of the essential services are protected from cyber attack. Robust and reliable protective security measures to effectively limit opportunities for attackers must be in place, proportionate to the cyber security risk.

B5. Resilient networks and systems

Resilience against cyber attacks and system failures are built into the design, operations and management of systems that support delivery of essential services.

B6. Staff Awareness and Training

Personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related documented policies, procedures, and agreements.

Defending Cyber Security Events

C1. Security Monitoring

The information system and assets are monitored in order to identify potential cyber security events and verify the effectiveness of protective measures. All aspects of the security continuous monitoring process are documented.

C2. Proactive security event discovery

Anomalous activity is detected in a timely manner and the potential impact of events is understood. The event detection processes and procedures are documented, maintained and tested to verify effectiveness and ensure continuous improvement.

Minimising the Impact of Incidents

D1. Response and recovery planning

Response and recovery processes and procedures are executed, maintained and documented, to ensure timely response to cyber security events and to ensure timely restoration of systems or assets affected by cyber security incidents.

D2. Lessons learned

Recovery planning and processes are improved and documented by incorporating lessons learned into future activities.

Incident Notification by Operators of Essential Services

OESs must notify the GRA about any incident which has a significant impact on the continuity of the essential service which the specific OES provides ("NIS incident"), as per the requirements of section 42(1) of the Act. A NIS incident is an incident, which has an actual adverse effect on the security of NIS used in the provision of essential services with reference to the agreed sector specific thresholds.

When an OES becomes aware that an incident has reached the threshold for reporting, they must report it to the GRA within 72 hours by submitting an Incident Notification Form available on the GRA's website.

For further information on the Incident Notification Form, please refer to our **'Guidance to understanding the NIS Incident Report Notifications'** document on the following webpage:

https://www.gra.gi/cyber-security-compliance/documents/guidance

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

☎ (+350) 20074636
✉ csc@gra.gi
🌐 www.gra.gi