GRA

GIBRALTAR REGULATORY AUTHORITY

Guidance for Operators of Essential Services on the implementation of Part 7 on the Security of Network and Information Systems of the Civil Contingencies Act 2007

Date 6th May 2022

CS 03/22

FOREWORD

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

The GRA may have regard to this guidance when interpreting the requirements of Part 7 of the Act.

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

CONTENTS

Introduction

1. Executive Summary

This guidance has been issued to support Operators of Essential Services ("OESs") as regards compliance with the requirements of Part 7 of the Civil Contingencies Act 2007 (the "Act") on the Security of Networks and Information Systems ("NIS").

The purpose of these requirements is to increase the overall cyber security and cyber resilience of OESs, in relation to the network and information systems that support the delivery of essential services. OESs **must** take appropriate and proportionate technical and organisational cyber security countermeasures to manage risks posed to the security of the network and information on which their essential service relies, and to prevent and minimise the impact of incidents on the essential service.

This will be achieved through partnership and collaboration between OESs and the Gibraltar Regulatory Authority (the "GRA"). This guidance supports OESs in complying with the requirements of the Act and sets a process to help OESs demonstrate they are managing cyber security risks in relation to essential services. This guidance should be used in accordance with the **14 Principles of the Cyber Assessment Framework ("CAF")**.

Additionally, this guidance sets out a series of activities that OESs are expected to complete. These include:

- Preliminary self-assessment;
- Scoping;
- CAF self-assessment; and
- Identifying and implementing improvement plans.

OESs are required to perform yearly self-assessments against the CAF, are expected to engage directly with the GRA and raise any queries at the earliest possible opportunity on how to apply the self-assessment. Upon completion of the self-assessment, the GRA may, where appropriate, review the self-assessment and any proposals about what cyber security countermeasures OESs consider appropriate to manage the risks. The GRA may provide advice on whether further cyber security countermeasures are required. Where appropriate, audits and inspections may also be scheduled by the GRA to determine an Operator of Essential Services ("OES") compliance with the requirements of the Act and/or in respect of matters related to the self-assessment and improvement plans they submit.

OESs also have a duty to report to the GRA incidents that meet the agreed sector specific thresholds which have an adverse effect on security of network and information systems, used in the provision of the essential service. The GRA may also liaise with the respective entities and conduct post-incident inspections.

2. Limitations

This guidance represents the GRA's interpretation of current and developing standards for cyber security, predominantly on operational technology ("OT"). It does not cover protection of personal data or intellectual property considerations for OESs.

This guidance may be updated and expanded in the future as required, based on the continued partnership and collaboration with OESs.

This document does not provide guidance around the project engineering lifecycle, from design, development, factory or site acceptance testing, commissioning, decommissioning and disposal. Security requirements should be considered from the start of the design process. OESs should also ensure that appropriate and proportionate cyber security compliance requirements are used in the procurement process and for product specifications, with appropriate security standards.

3. Status of this guidance

Responsibility for compliance with the Act lies with the OESs. While this guidance may help OESs in achieving and maintaining compliance, OESs should not rely solely on the GRA and/or this guidance for this purpose.

The GRA relies on the information and data submitted by OESs as being accurate and reliable. Any information or data provided to the GRA (in whatever form), may be used for the purposes of enforcement action in accordance with the GRA's statutory duties.

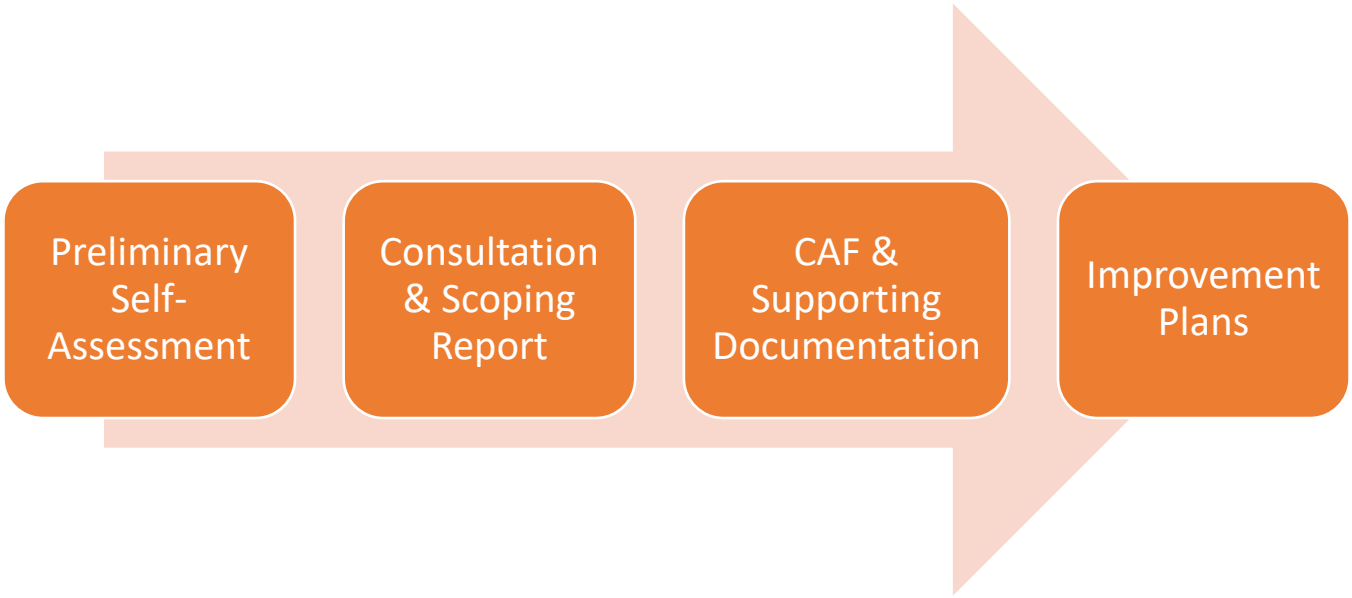
The receipt of any information or data from an OES or other party (howsoever provided and including, without limitation, in an OES self-assessment report, completed CAF spreadsheet, improvement plan, audit or inspection report), should not be taken as tacit approval or endorsement of any conduct described therein. In addition, any reviews or associated commentary the GRA may provide in relation to the same are purely advisory and do not represent the GRA's approval or endorsement of an OES's conduct, unless expressly stated in writing. Any such reviews or associated commentary are issued without prejudice to the GRA's right to take enforcement action should this be considered appropriate.

The guidance is not intended to provide a comprehensive guide to compliance with the requirements of Part 7 of the Act. The guidance sets out the GRA's interpretation of certain relevant obligations under the Act and the GRA's expectations associated with the same. It is not a substitute for independent legal advice and each OES is responsible for seeking such legal (or other professional) advice, as it considers appropriate to ensure compliance with its obligations.

Section A – Assessment Stages

1. Introduction

The diagram below sets out the initial stages planned for the scoping and self-assessment leading to the further development of the CAF. It is expected that these stages and an appropriate timeline will be agreed with OESs.



1. Preliminary CAF Self-Assessment - OESs are expected to submit a general self-assessment for the essential services that they provide. The GRA may, where appropriate, review the self-assessment and seek further information or clarification from the OES on their contents.

2. Consultation & Scoping – The GRA will engage in discussions with OESs to determine whether the overall CAF is appropriate or specific sections of the CAF are not applicable, and to determine the scope of each assessment in relation to the essential service. If the GRA determines that the CAF self-assessment is not appropriate for a specific industry or sector, then other documentation or forms of proof of compliance may be required.

3. CAF & Supporting Documentation - OESs are expected in most cases to submit CAF self-assessments for each of the essential services that they provide with supporting documentation.

4. Improvement Plans - Once the self-assessment and supporting documentation has been reviewed, OESs may need to develop improvement plans to mitigate risks that require treatment. The GRA may, where appropriate, review the improvement plan and seek further information or clarification from the OES on its contents.

2. Scoping

The network and information systems which are within the scope of the Act are only those that are relevant to the delivery of the essential services that the OES provides, with particular reference to areas where compromise of that system could impact the continuity of the essential service.

The output of scoping is for OESs to identify critical systems and networks, in order to develop an understanding for the self-assessment. The scoping document should set out clear lines of responsibility and accountability, statement of assumptions made, identification of reliance scope, list of systems and networks, grouping of assets, and where applicable, listing of all relevant sites or aggregated numbers of related sites.

2.1 Structure of scoping report

The format of the scoping report can be tailored for OES's needs. The typical format is one which has all of the following:

1. High level description of the critical systems and networks.
2. High level diagram of environment mapped to Purdue architecture model (See Annex 1).
3. List of assumptions made and list of systems and networks that may be related and deemed explicitly as out of scope, including justification as to why they are deemed as out of scope. Boundary diagrams may be a useful aid to illustrate this for cases of interfaces or common interfaces.

2.2 Suggested principles

1. Only network and information systems that are deemed necessary to the delivery of essential services should be considered.
2. Therefore, essential services managed by manual processes, which OESs are not dependent upon the information, being provided from information systems, will automatically be de-scoped.
3. Risk analysis will include internal and external influences, and by both intentional and unintentional means.
4. Appropriate segregation of 'other' information systems will be deemed adequate to de-scope, with explanation and evidence.
5. However, risks posed to the essential services which are reliant upon network and/or information services, which have persistent or intermittent interconnections or related devices shall be in scope.
6. Transferring responsibility of systems that are critical to the provision of the essential service, are typically performed if those systems are operated by an entity which is also regulated under Part 7 of the Act and has included such systems in their scope.

7. The OES will be required to validate that the information is accurate.

8. Network and information systems deemed low risk may still be in scope due to the attack vectors posed which may affect other systems or network architecture.

9. Network and information systems will be in scope if OESs are unable to operate under normal conditions beyond the acceptable outage period, with no alternative and sustainable means of operating.

2.3 Further suggestions

- All relevant systems, networks, assets and sites under the ownership of OESs should be listed, even if they are managed and operated by another party.
- Where grouping of assets/sites are performed and not considered to be in scope for NIS, OESs should provide appropriate justification(s).

2.4 Further considerations for OES

1. Organisational – which organisations, sections and people have access to the networks and information systems that deliver the essential service.

2. Interfaces - What cyber security countermeasures are there at the boundaries of the scope? Are there sufficient cyber security countermeasures at the boundary of the scope to provide confidence that OESs are meeting the requirements of the Act?

3. Dependencies – What internal (e.g. internet gateway) and external factors (e.g. telecoms networks) do the networks and information systems rely on to provide the essential service?

4. Supply Chain – Who manages and maintains your systems and how do they do that?

5. There are often several ways to map the functional and logical view in a scope. OESs should determine the approach that helps the organisation best in order to understand the components that support the essential service and how they interact.

6. The systems in scope may change over time, due to increased knowledge of how the essential service is provided, or due to changes in the network and information systems used.

7. The OES should regularly review their systems in scope (at least every twelve months) and as part of any significant change activity.

2.5 Steps for scoping

Below are some suggested steps to take for scoping:

Step 1: Identify critical business processes and their inter-dependencies classified with high impact.

Step 2: Identify and group assets/sites according to criticality to the overall essential service.

Step 3: Map (high-level not sub-level) critical business processes reliance upon the various grouping of assets/sites.

Step 4: Identify asset/site owners and determine who manages these and where there may be shared responsibilities.

Step 5: Determine impact of loss of group of assets, to business objectives and national requirements.

Step 6: Identify supporting systems and networks.

3. Overall reporting

OESs are requested to submit the following reports to the GRA using the methods set out in this section.

3.1 Preliminary Self-Assessments

OESs will submit their preliminary self-assessments to the GRA as a high-level general overview of their current achievements in line with the best practices in the CAF.

At this preliminary stage, the GRA will review the documentation submitted to determine whether it is appropriate. If the OES submits a completed CAF, the GRA will pay particular attention to instances identified as "Not Yet Assessed" and "Not Relevant" and any comments entered under the justification section. If the comments are not substantiated, then the GRA may request additional information in specific areas if it determines that documentation submitted is not detailed enough to progress to the next stage.

It is appreciated that when completing the CAF there may be instances where an OES may be mostly 'Achieved' and only parts of the OES are 'Not Achieved' or 'Partially Achieved'. As there may have already been significant efforts or resources invested to address cyber security and resilience in these areas, the OES may discuss the CAF assessment with the GRA to agree how best to reflect this. An OES could mark 'Achieved' with exceptions listed under the justification section. Any exceptions need to be made explicit and should indicate how the exceptions have been risk assessed and managed accordingly.

3.2 Consultation & Scoping Report

Following the submission of the preliminary CAF self-assessment, the GRA will assess all submissions and will consult with OESs. The aim of this consultation is to determine whether the documentation submitted and/or the CAF are appropriate and to address any changes and any "Not Relevant" sections in order to develop an appropriate reporting mechanism or tailored CAF for each sector. As part of the consultation process, each OES must prepare and submit a scoping report. The aim of the scoping process is for OESs to identify critical systems and networks, and for these to become the focus of future self-assessments. During the consultation, where CAF outcomes have been 'Achieved', justification should be provided and additional evidence may be requested by the GRA.

3.3 CAF Self-Assessments & Supporting Documentation

OESs will submit self-assessments to the GRA, comprising of:

- **The CAF spreadsheet**

A completed CAF spreadsheet with appropriate explanatory notes. No supporting evidence is required to be submitted where CAF outcomes have been 'Achieved', as these would have been addressed and/or proof would have been provided during the consultation stage.

- **Supporting evidence**

Evidence is required for areas identified as 'Not Achieved' or 'Partially Achieved'.

Once submitted, the GRA will acknowledge receipt of the self-assessment and may then review OESs submissions. The GRA may, where appropriate, enter into a discussion with OESs and request further information on the reported items to back up its assessments. This may be to seek further clarification on CAF outcomes deemed as 'Not Achieved' or 'Partially Achieved'.

Should language within the self-assessment be unclear or ambiguous, the GRA will need to clarify this with the OES.

OESs are requested to be as clear and open as possible in their self-assessments and should contact the GRA at the earliest possible opportunity if they are unsure of anything at any point. Once OESs have completed their self-assessment, OESs should consider areas for improvement.

In the initial self-assessment, the GRA recognises that OESs may not have 'Achieved' in all categories. The key action is for OESs to undertake an accurate self-assessment and develop an improvement plan, where improvements are required.

Where OESs have provided justifications for items listed as 'Achieved', this will be accepted by the GRA and evidence is not expected to be submitted. A high-level justification should, however, be provided within the CAF self-assessment spreadsheet as to why an item is deemed to be 'Achieved'. These areas may still form part of OESs inspections.

4. Self-Assessment

It is the GRA's view that the principles-based approach is a more effective way of driving improvements to cyber security in the context of NIS, than an approach based on prescriptive rules. This is due to complex and rapidly changing areas within cyber security. OESs understand their own business better than any external entity and should be more capable of taking informed, balanced decisions about how they achieve the outcomes specified by the NIS principles.

The CAF was designed to provide an outcome-focused assessment against the 14 NIS principles across four objectives (NIS and CAF hierarchy and structure is set out in Annex 2). Each of the principles is linked to specific guidance which highlights some of the factors that OESs will usually need to take into account when deciding how to achieve the outcome and recommends some ways to tackle common cyber security challenges.

The principles are broken down into 39 contributing outcomes. Each outcome is associated with a set of **Indicators of Good Practice ("IGPs")** arranged in a table format. OESs should assess whether they can be considered 'Achieved', 'Partially Achieved' or 'Not Achieved' against each outcome. The result of applying the CAF is 39 individual evaluations that reflect to what extent an OES meets the IGPs.

IGPs are not intended to be prescriptive, there may be alternative sources of good practices, such as some international standards, frameworks or methodologies, which may be helpful to OESs, in managing cyber security risks.

The principles carry no assumptions about how the specified outcomes should be achieved. Assessment of contributing outcomes should involve the role of expert judgement and interpretation. It is for OESs to determine the most appropriate cyber security countermeasures to deliver outcomes within their organisational context, to manage cyber security risks. The GRA may, in some cases, provide additional guidance to OESs, on how the outcomes can be achieved.

OESs are expected to undertake a robust but realistic CAF self-assessment supported by evidence. The self-assessment is to be performed within the parameters set out in the scoping document. This may include both legacy and current networks and systems which are still in operation. It is highly recommended, that OESs commence assessments with the most critical sites and assets first.

It would be advisable to obtain some or all of the following prior to commencing self-assessment:

- Organisational and Governance Structure
- Reporting relationships
- Existing Roles and Responsibilities
- Existing Security Metrics
- Cyber Security Strategy
- Most recent Cyber Security Risk Assessments
- Existing / Planned Security Initiatives and Roadmap
- Existing Cyber Security and related Policies / processes / procedures / guidelines / standards
- Asset Inventory across locations
- Network Architecture
- Network Zoning Details
- Gain an understanding as to how the site and system(s) fit in the overall 'value' or 'supply' chain, to gain insight into business and operational criticality of each site and system(s)
- Identify the single point of accountability for each site, system and asset
- Identifying what assets and components are critical for the site

- For each main OT, obtain the number of independent instances of the system used to support the processes

Since the NIS requirements in the Act do not apply directly to the supply chain of OESs, it is the OESs' responsibility to put in place appropriate and proportionate cyber security countermeasures with their suppliers if necessary. OESs should ensure that suppliers have in place appropriate cyber security countermeasures to manage risks of their services being disrupted through the supply chain.

5. Improvement Planning

Once OESs have submitted their self-assessment to the GRA, OESs should begin to develop improvement plans. Where the GRA carries out a review of the self-assessment, this may include assisting OESs in identifying the risks that require treatment through cyber security countermeasures. The GRA expects OESs to take a risk-based approach when considering where improvements are needed. The onus is therefore on OESs to identify risks in accordance with their own established methodologies and processes.

Improvement plans should set out the cyber security countermeasures OESs intend to take where they deem the risk to be above their own risk tolerance levels. All high risks above OESs risk tolerance levels should be identified with appropriate and reasonable cyber security countermeasures to reduce the risk to acceptable levels. Improvement plans may cover, short term measures, medium term measures or longer term measures, for which budget needs to be sought through business planning.

It is highly recommended that all cyber security countermeasures are considered in the order of people, process and technology. The rationale is that the underpinning process and technology can essentially be undone by the people, and the culture of security needs to be well embedded.

OESs may need to undertake a significant amount of work to put in place both a **Cyber Security Management System ("CSMS")** and the necessary technical cyber security countermeasures to manage risks appropriately.

6. Inspections

Section 49 of the Act grants the GRA powers to conduct inspections of OESs. The purpose for such inspections are to assess if OESs have fulfilled the duties imposed on them by section 41 of the Act.

The GRA may appoint a person to conduct the inspection on its behalf or direct the OESs to appoint a person approved by the GRA to conduct an inspection on its behalf. Any such person appointed by the GRA will be on such terms and in such manner that it considers appropriate.

The OES will pay all reasonable costs associated with an inspection and cooperate fully with the person conducting the inspection. OESs will also have to provide reasonable access to their premises including allowing an inspector access to copy or remove documents, including electronic information, and allow access to an inspector to seek relevant information from persons within the OES.

Section B – Cyber Incidents

1. NIS Incident Reporting

Incident reporting is invaluable to:

- build an understanding of the threats affecting the sector and provide early warning
- enable timely advice across the sector and cross-sector where appropriate
- support specific law enforcement response where required
- provide historical context when performing likelihood assessments in future

OESs **must** notify the GRA about any NIS incident which has a significant impact on the continuity of the essential service which that OES provides, 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 network or information systems, used in the provision of essential services with reference to the defined and agreed 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.

At this point the GRA will be aware of the incident but does not have a role in providing support for incident response. Reporting the incident to the GRA will have no impact on how the response process is handled.

A cyberattack may not be immediately identifiable as such, and so OESs may want to look for one or more of the following:

- related security breaches, including physical
- data copied to OT environment or connection of unauthorised removable media
- suspicious requests and/or instructions
- known activation of software or script
- unauthorised access and/or configuration changes to security software

The failure to notify the GRA of a NIS incident is a contravention of section 42 of the Act. However, an incident is not necessarily a contravention of the Act and therefore may not lead to enforcement action being taken.

After receipt of the notification, the GRA may, if appropriate, liaise with the Computer Security Incident Response Team ("CSIRT") or any relevant body to ensure that communications are aligned with the OESs and, if necessary, the general public are informed about the incident and any actions to take.

2. Incident Recovery

The GRA will generally seek to ensure that any necessary regulatory intervention during an incident is kept to a minimum to ensure OESs have the necessary time to respond and recover.

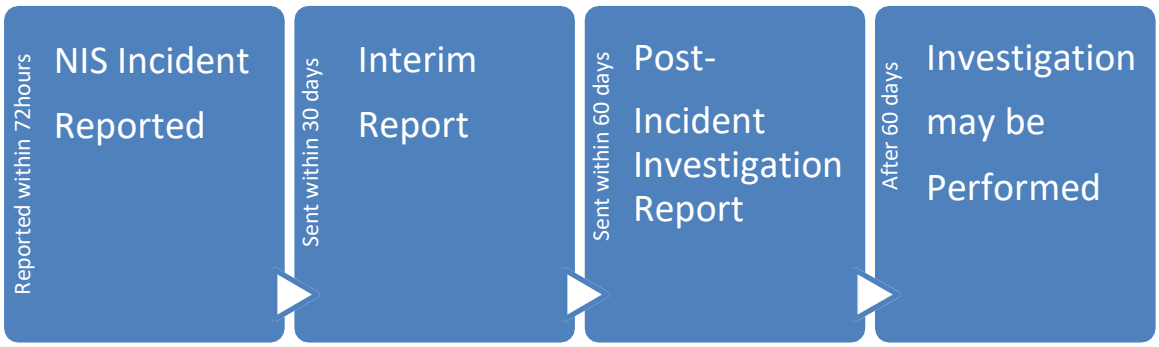
When systems and equipment have been made safe by the OESs, there are further priorities. These are listed in order of importance below:

1. Starting limited, degraded operation(s) where the risk to safety is acceptable, in accordance with accepted practice.
2. Returning the overall network system to 'normal state' of functioning.
3. Taking any and all remedial action where the point of breach has been identified.
4. Identifying, isolating and preserving evidence for forensic analysis.
5. Internal investigation into how systems were breached (this should not interfere with any official investigation that may be conducted under section 38(2)(b) of the Act).
6. Remedial action(s) to prevent further breaches.

Affected systems and equipment should be put into a safe state to prevent harm or damage occurring after the initial incident has taken place.

3. Post-Incident Recovery

The diagram below is a high-level process flow in relation to reporting and investigation by the GRA.



Within 30 days of a NIS incident being reported by an OES, the OES is expected to submit an interim report to the GRA.

Within 60 days of a NIS incident being reported by an OES, the OES is expected to submit to the GRA a post-incident investigation report with lessons learned. Although highly unlikely, it is noted that there may be circumstances that the incident is still ongoing at the 60-day mark. Should an OES believe it will not be able to meet this deadline, the OES should inform the GRA at the earliest opportunity.

Following the receipt of the post-incident investigation report, the GRA may decide whether or not the incident requires further investigation. The purpose of the investigation may be to:

- establish the cause of the incident and assess whether the incident was preventable;
- assess whether effective and reasonable risk management was in place;
- assess whether the OES had appropriate security measures in place; and/or
- assess how the OES responded to and managed the incident.

Should an investigation be appropriate, the GRA may use the OES developed post-incident investigation report as a basis for review. Once the investigation has concluded, the GRA may decide on any appropriate next steps. These may be, no action, advice or formal enforcement action.

Where a cyberattack has taken place, OESs should consider the risk from further cyberattacks and the likelihood of this occurring. OESs should capture lessons learned through formal reporting for continual improvement to manage times of crisis and disaster recovery. These lessons may be used to update OESs' emergency response and contingency plans.

Section C – Enforcement

Any enforcement action will be dealt with on a proportionate basis, which takes account of the seriousness of any contravention(s) of an OES' duties under Part 7 of the Act.

An OES duties are set out in sections 41 and 42 of the Act and include:

> *The security duties of operators of essential services*
>
> *41(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.*
>
> *(2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.*
>
> *The duty to notify incidents*
>
> *42(1) An OES must notify the designated competent authority about any incident which has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident").*

The occurrence of a NIS incident itself does not necessarily mean that there has been a failure by an OES to comply with its security duties or notification duties. The key factors for determining enforcement will be:

1. whether or not appropriate and proportionate security measures were in place and were being followed in terms of section 41 of the Act; and/or

2. whether NIS incidents are notified to the GRA in terms of section 42 of the Act.

Step 1: Advise and persuade

When any non-compliance is identified, the initial approach taken by the GRA will be to engage and discuss these with the OES. This will include discussing what the failing or deficiency is, how and when it should be addressed and in what timescale. The GRA may review any remedial actions proposed by the OES (including when these actions should be completed). Should this be appropriate, the GRA may follow up with further audit and/or inspections to ensure these actions have been addressed appropriately.

The GRA may issue information notices under section 48 of the Act requiring the OES to provide specified information to support any assessment of compliance.

Step 2: Enforcement notice

Where the initial collaborative approach has not worked or is not appropriate and/or it is clear that failings are not being addressed, a formal Enforcement Notice may be issued under section 50 of the Act. The Enforcement Notice will include the failings identified, the steps (if

any) to be taken to rectify the failures, the time period in which they must be completed and how and when representations on the Enforcement Notice may be made.

Step 3: Penalty notice

Where the OES has failed to take adequate steps to rectify a failure identified in an Enforcement Notice or the GRA is not satisfied with the representations made by an OES in response to such an Enforcement Notice, the GRA may impose a financial penalty under section 51 of the Act.

In determining the value of the financial penalty, the GRA will consider the appropriate and proportionate level within the prescribed limit by reference to the tiered limitations set out under section 51(6) of the Act.

If an infringement occurs which breaches Part 7 of the Act and another regulatory requirement or legislation, the GRA will have regard to this and where appropriate discuss the best approach.

Step 4: Reviews

It should be noted that section 52 of the Act sets out that an OES may request an independent review of penalty decisions taken by the GRA in order to challenge the following matters:

a) the grounds for imposing a penalty notice;

b) the sum that is imposed; and

c) the time period within which the penalty notice must be paid.

Any request to conduct a review must be made in writing and copied to the GRA setting out the reasons for requesting a review and any relevant evidence, within 30 days of receipt of the penalty decision.

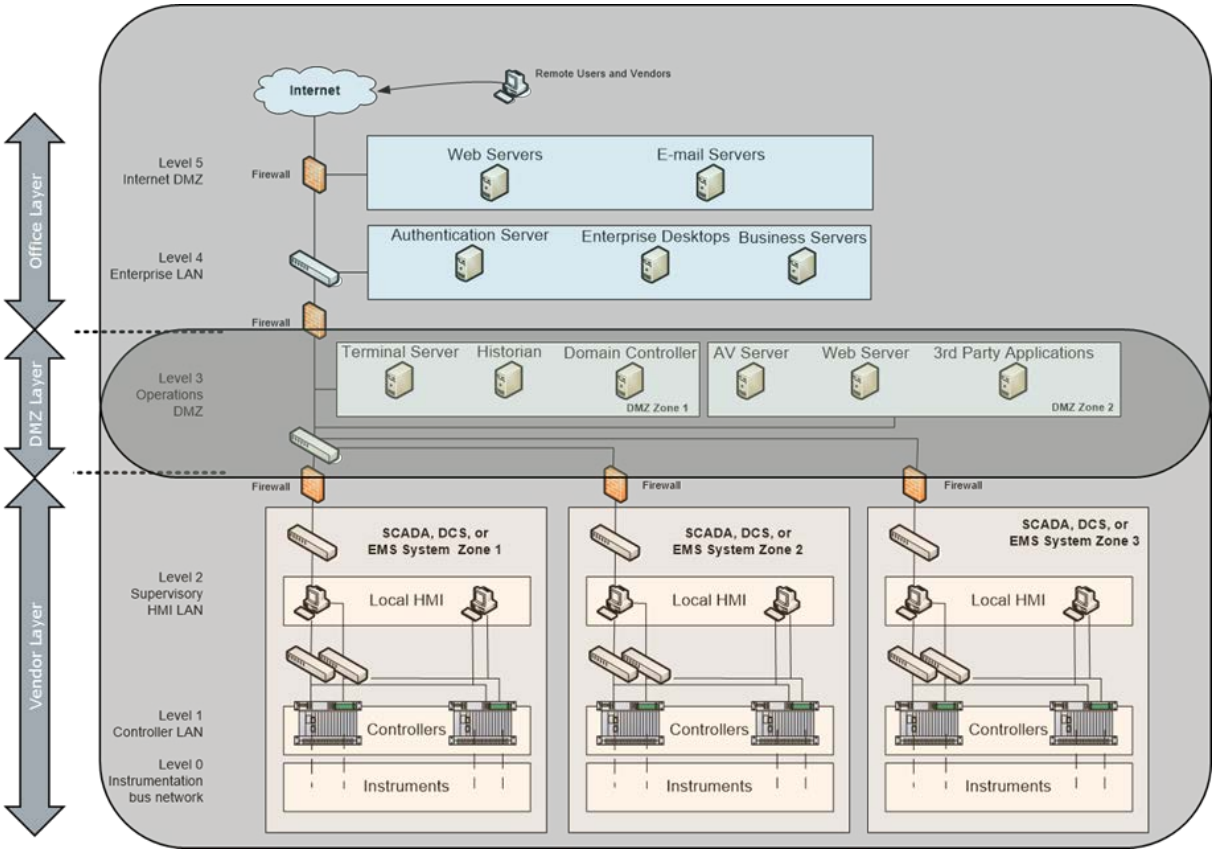
Annex 1 – Purdue Model

Purdue Model for ICS Security

The Purdue Model was developed in the 1990s, a part of Purdue Enterprise Reference Architecture (PERA), and is a reference data flow model for Computer-Integrated Manufacturing (CIM), i.e., using computers to control the entire production process.

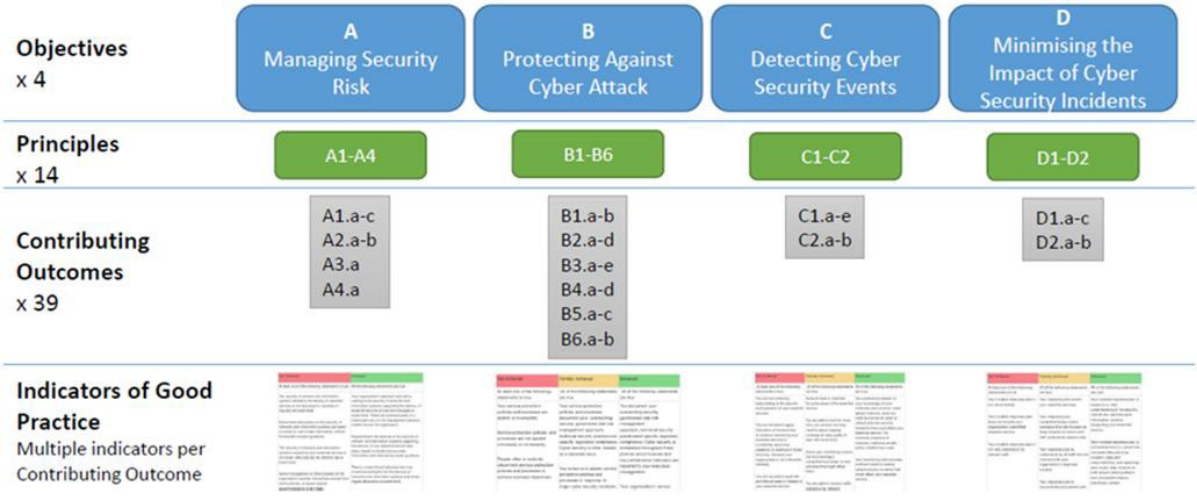
The model shows the interconnections and interdependencies of all of the main components of a typical Industrial Control System ("ICS"), dividing the ICS architecture into two zones – Information Technology ("IT") and Operational Technology ("OT") – and subdividing these zones into six levels starting at level 0.

At the base of the Purdue Model is the OT, the systems used in critical infrastructures and manufacturing to monitor and control physical equipment and operational processes. In the Purdue Model, this is separate from the IT zone, which can be found at the top of the model. In between, there is a demilitarized ("DMZ") to separate and control access between the IT and OT zones. Within the zones, there are separate layers describing the industrial control components found in each layer.



Annex 2 – Network and Information Systems and the Cyber Assessment Framework Hierarchy and Structure

Illustration of NIS and CAF Hierarchy and Structure



A: Managing Security Risk		*B: Protecting Against Cyber Attack*		*C: Detecting Cyber Security Events*		*D: Minimising the Impact of Cyber Security Incidents*	
A1: Governance	**A2:** Risk Management	**B1:** Service Protection Policies and Processes	**B2:** Identity and Access Control	**C1:** Security Monitoring	**C2:** Proactive Security Event Discovery	**D1:** Response and Recovery Planning	**D2:** Lessons Learned
A3: Asset Management	**A4:** Supply Chain	**B3:** Data Security	**B4:** System Security				
		B5: Resilient Networks and Systems	**B6:** Staff Awareness and Training				

This table is provided for illustration purposes only.

CONTACT US

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

(+350) 20074636
csc@gra.gi
www.gra.gi