Cyber Security Centre for the Isle of Man

Department of Home Affairs

Rheynn Cooishyn Sthie

PROPOSED NATIONAL INFRASTRUCTURE SECURITY BILL (NISB)

Guide

NISB aims to improve the resilience of the Islands critical national infrastructure, enhancing the protection of our essential services against a cyber attack.

Version 3.0

Contents

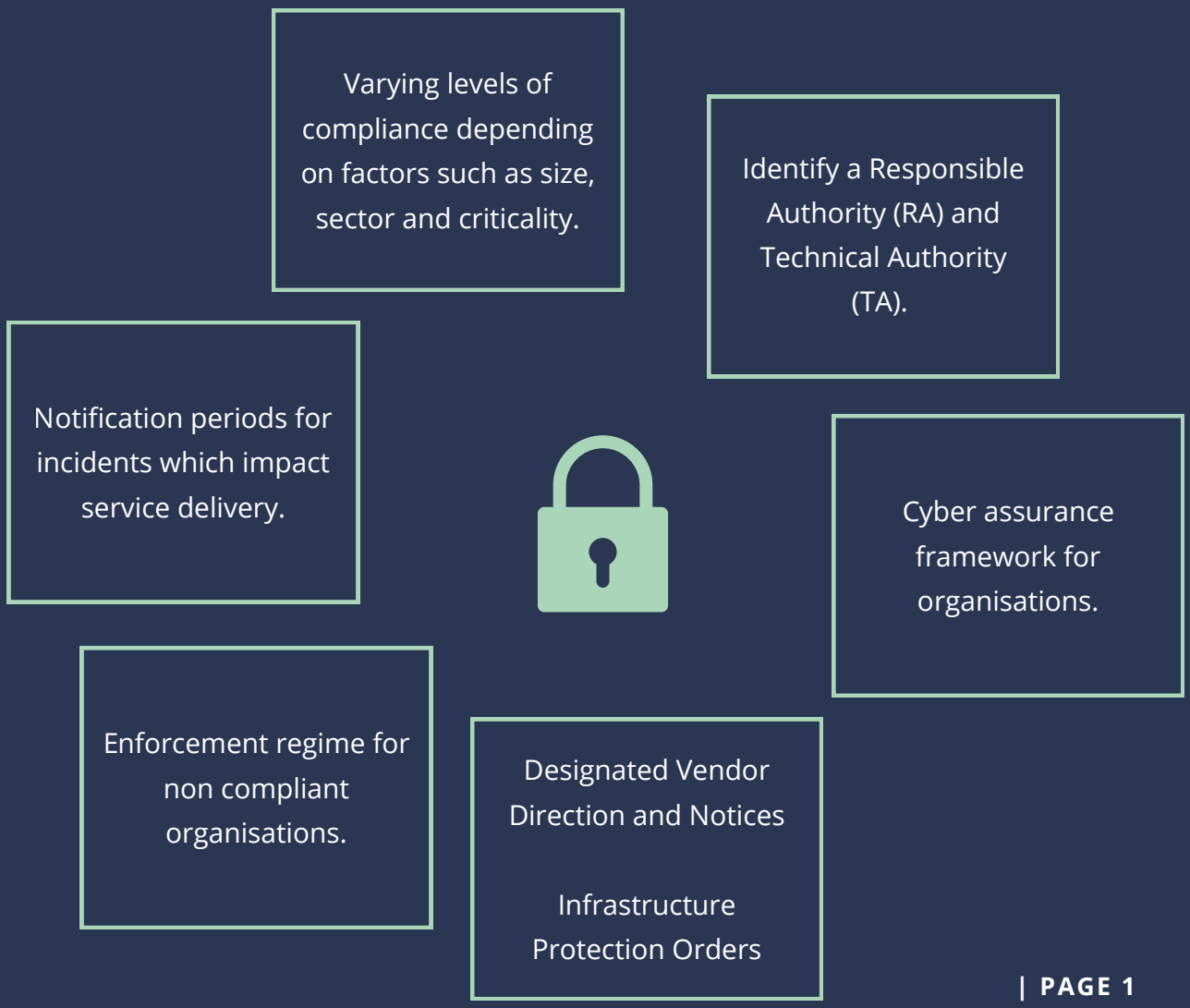
Introduction

Isle of Man residents should have confidence in the security and resilience of national infrastructure sectors to deliver essential goods and services. Essential services provided by both public and private sectors – such as our electricity grid, water supply and telecommunications systems should be able to withstand and recover from hazards that might disrupt their functions.

Unfortunately, hostile providers and criminals have recognised that this dependency creates an opportunity for what have become known as 'cyber-attacks'.

The Department of Home Affairs wishes to introduce a National Infrastructure Security Bill to raise levels of cyber security and resilience for core services on the Isle of Man, which rely heavily on digital services.

The diagram below illustrates some of the core elements of the proposed legislation.



1

WHAT IS THE NATIONAL INFRASTRUCTURE FOR THE ISLE OF MAN?

What systems and assets, including physical, digital, and organisational, are essential to the functioning of the Isle of Man and its economy.

What is the National Infrastructure for the Isle of Man?

One of the policy principles for the proposed National Infrastructure Security Bill (NIS-B) was that the sectors that form part of the Island's National Infrastructure should be identified and included in the scope of the legislation.

For the purposes of this legislation the National Infrastructure means the systems and assets, including physical, digital and organisational, that are essential to the functioning of the Isle of Man and its economy.

The National Infrastructure for the Isle of Man comprises of many elements, commonly known as sectors and within those sectors will be businesses and organisations working to deliver the services upon which we rely.

Within this wide collection of businesses and organisations, known as providers, some will be more critical to our daily lives and the Isle of Man economy than others. Equally some will be larger than others.

Critical National Infrastructure

In introducing any proposed legislation we need to be able to take into account the differences in levels of criticality within the National Infrastructure and the size of the providers who are delivering the services we rely on and apply any requirements in a proportionate manner.

From the research we have conducted we are proposing that the EU Network and Information Security Directive – 2 (EU NIS-2), the UK Network and Information Systems Regulations 2018 and the UK Telecommunications (Security) Act 2021 provide a basis on which we can address these differences.

Proportionality

Another policy principle for the proposed National Infrastructure Security Bill was that the measures introduced should be proportionate to the needs of the Isle of Man whilst also taking into account the type of service and size of the supplier. In order to ensure the necessary proportionality we are proposing that:

Whilst all providers operating in the Sectors of the Critical National Infrastructure will be required to register with the Responsible Authority(ies), there will be:

- Three levels of compliance depending on the size of the provider and the criticality of the service provided
    - These providers would be classed as either 'Essential', 'Important' or 'Unclassified' and this classification would determine the assurance regime they would be subject to

It is also proposed that the following criteria is used to define the size of a provider:

- Small 5-24 workers
- Medium 25-49 workers
- Large 50 workers and above

This is explained in more detail in section 3 of this guide, Essential and Important providers.

2

SECTORS OF THE CRITICAL NATIONAL INFRASTRUCTURE

From the results of the consultation held in March of 2024, it is apparent there is a need to classify elements of the National Infrastructure based on their level of criticality, similar to measures undertaken in the UK and EU.

Sectors in Scope

All sectors listed are part of the Island's Critical National Infrastructure. While some services have greater impact than others, the legislation will apply proportionately through provider classifications.

*It is proposed that the legislation will cater for changes to the sectors by allowing for adjustments

3

ESSENTIAL AND IMPORTANT PROVIDERS

The designation of 'Essential' and 'Important' will determine the assurance framework a provider will follow. Providers may be designated as 'Essential' or 'Important' depending on factors such as size, sector, and criticality.

Essential and Important Providers

Some providers operating in those sectors deemed to part of the Critical National Infrastructure (as shown in the following tables) will be required to register. However, only those providers assessed as 'Essential' or 'Important' will be required to adhere to an assurance framework.

The designation of a provider as either 'Essential' or 'Important' informs which level of assurance framework they will be required to follow.

If a provider is categorised as 'Essential' it is because an issue with service delivery could adversely impact public safety, security, health or economic stability. However, an organisations size will also be used to assess whether it is subject to 'Essential' or 'Important' levels of assurance.

Some sectors are deemed so critical that a designation of 'Essential' is applied for organisations of all sizes. While other sectors feature providers with multiple designations depending on an organisations size.

While EU NIS-2 has set out criteria for classifying providers as either small, medium, or large it was apparent from our research and feedback from the consultation that these would not be appropriate for the Isle of Man. We have therefore proposed new criteria more proportionate for the Isle of Man.

The tables overleaf have been amended as the drafting of the bill has progressed and illustrate the proposed designations for each sector, with some providers now out of scope.

There will be a general duty to adopt cyber security and resilience measures applicable to all registered providers within the legislation.

Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
Communications and Digital Services Category				
Communications Sector:	**Communications Providers**: Companies offering fixed and mobile telephony, broadband, and internet services.	Essential	Essential	Important
	Internet Service Providers (ISPs): Providers providing internet access and related services.	Essential	Essential	Important
	Broadcasting Services: Radio and television broadcasting networks and services	Essential	Important	Unclassifed
	Satellite Communications: Providers of satellite-based communication services.	Essential	Essential	Important
	Supporting Infrastructure: Undersea cables, and other critical infrastructure supporting communication networks	Essential	Essential	Important
Digital Infrastructure Sector:	**Data Centres:** Facilities housing computer systems and associated components, such as telecommunications and storage systems.	Essential	Essential	Essential
	Cloud Service Providers: Companies providing cloud computing services, including storage, processing, and software as a service (SaaS).	Essential	Important	Unclassified
	Domain Name System (DNS) Providers: Providers managing the internet's domain name system.	Essential	Essential	Essential
	Content Delivery Networks (CDNs): Networks of servers that deliver web content and services to users based on their geographic location.	Essential	Important	Unclassified
	Qualified Trust Service Providers	Essential	Essential	Essential
	Trust Service Providers: Providers providing digital certificates and other trust services.	Essential	Important	Important
	Internet Exchange Point providers	Essential	Important	Unclassified
	TLD name registries	Essential	Essential	Essential

Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
ICT Providers Sector:	**Managed Service Providers (MSPs):** Providers providing services related to the installation, management, operation, or maintenance of ICT products, networks, infrastructure, and applications.	Essential	Important	Unclassified
	Managed Security Service Providers (MSSPs): Providers offering security management services, including monitoring, and managing security devices and systems.	Essential	Important	Unclassified
	IT Support Services: Companies providing technical support and maintenance for ICT systems and infrastructure of Essential or Important Providers (i.e. supply chain)	Essential	Important	Unclassified
Digital Providers Sector:	**Online marketplaces**	Important	Important	Unclassified
	Search Engines	Important	Important	Unclassified
	Social Networking Platforms	Important	Important	Unclassified
Providers Offering Domain Name Registration Services		Important	Important	Important

Energy Category

Energy Sector:	**Electricity:** Power generation plants, transmission networks, and distribution systems.	Essential	Important	Unclassified
	Oil and Gas: Extraction, refining, transportation, and storage facilities.	Essential	Important	Unclassified
	District Heating: Systems providing heating and cooling services to buildings and industries.	Essential	Important	Unclassified
	Hydrogen: Production, storage, and distribution infrastructure for hydrogen energy.	Essential	Important	Unclassified
	Renewable Energy: Solar, wind, hydroelectric, and other renewable energy sources and their associated infrastructure.	Essential	Important	Unclassified

Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
Health Category				
Health Sector:	**Healthcare Providers:** Hospitals, clinics, and other facilities offering medical services.	Essential	Important	Unclassified
	Medical Equipment Manufacturers: Companies producing medical devices and equipment.	Essential	Important	Unclassified
	Pharmaceutical Companies: Providers involved in the production and / or wholesale distribution of medicines.	Essential	Important	Unclassified
	Public Health Agencies: Governmental bodies responsible for public health and safety.	Essential	Important	Unclassified
	Research Institutions: Providers conducting medical and health-related research.	Essential	Important	Unclassified
Water Category				
Water Sector:	**Drinking Water Supply:** Facilities and infrastructure for the extraction, treatment, and distribution of drinking water.	Essential	Important	N/A
	Wastewater Management: Systems for the collection, treatment, and disposal of wastewater.	Essential	Important	N/A
	Water Treatment Plants: Facilities that treat water to meet safety and quality standards.	Essential	Important	N/A
	Reservoirs and Storage: Infrastructure for storing water, including reservoirs and water towers.	Essential	Important	N/A
	Distribution Networks: Pipelines and other infrastructure for transporting water to consumers.	Essential	Important	N/A

Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
Transport & Delivery Services Category				
Transport Sector:	**Air Transport:** Airports, airlines, air traffic control systems, and supporting infrastructure.	Essential	Important	N/A
	Rail Transport: Railway operators, infrastructure managers, and supporting systems. (excl. heritage railways)	Essential	Important	N/A
	Road Transport: Road networks, traffic management systems, and public transportation services.	Essential	Important	N/A
	Maritime Transport: Ports, shipping companies, and maritime navigation systems.	Essential	Important	N/A
	Logistics and Freight: Providers involved in the transportation and logistics of goods.	Essential	Important	N/A
Postal and Courier Services:	**National Postal Services:** Government-operated postal services responsible for mail and parcel delivery.	Important	Unclassified	N/A
	Courier Companies: Private companies providing expedited delivery services for documents and parcels.	Important	Unclassified	N/A
	Logistics Providers: Providers offering logistics and transportation services for mail and parcels.	Important	Unclassified	N/A
	Sorting and Distribution Centres: Facilities where mail and parcels are sorted and distributed.	Important	Unclassified	N/A
Financial Services & Banking Category				
Banking Sector:	**Banks:** Commercial banks, investment banks, and central banks.	Essential	Important	Unclassified

Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
Public Administration Category				
Public Administration Sector:	**Central Government Departments:** government bodies responsible for public administration as defined in the Government Departments Act.	Essential	Essential	Essential
Space Category				
Space Sector:	**Satellite Operators:** Providers responsible for the operation and management of satellites.	Essential	Important	Unclassified
	Ground Stations: Facilities that communicate with and control satellites.	Essential	Important	Unclassified
	Launch Service Providers: Companies that provide launch services for satellites and other space assets.	Essential	Important	Unclassified
	Space-Based Services: Providers of services such as Earth observation and navigation.	Essential	Important	Unclassified
	Space Manufacturing: Providers involved in the production of spacecraft, satellites, and related components.	Essential	Important	Unclassified
Food & Manufacturing Category				
Food Sector:	**Food Processing**: Facilities that process raw agricultural products into consumable food items.	Important	Unclassified	N/A
	Food Packaging: Providers involved in the packaging and labelling of food products.	Important	Unclassified	N/A
	Food Distribution: Logistics and transportation services that deliver food products to retailers.	Important	Unclassified	N/A
	Wholesale: wholesale distributors of food products.	Important	Unclassified	N/A

Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
Manufacturing Sector:	**Industrial Manufacturing:** Facilities involved in the production of machinery, equipment, and industrial goods.	Important	Unclassified	N/A
	Consumer Goods Manufacturing: Companies producing goods for consumer use, such as electronics, clothing, and household items.	Important	Unclassified	N/A
	Pharmaceutical Manufacturing: Providers involved in the production of medical devices	Important	Unclassified	N/A
	Automotive Manufacturing: Companies producing motor vehicles, parts, and related components.	Important	Unclassified	N/A

Chemicals & Waste Management Category

Chemicals Sector:	**Chemical Manufacturing:** Facilities producing basic chemicals, specialty chemicals, and consumer chemicals.	Important	Unclassified	N/A
	Petrochemicals: Providers involved in the production of chemicals derived from petroleum and natural gas	Important	Unclassified	N/A
	Pharmaceuticals: Companies manufacturing medicinal chemicals and pharmaceutical products.	Important	Unclassified	N/A
	Agricultural Chemicals: Producers of fertilisers, pesticides, and other agrochemicals.	Important	Unclassified	N/A
	Chemical Storage and Distribution: Facilities and logistics providers involved in the storage and transportation of chemical products for industrial use.	Important	Important	Unclassified
Waste Management Sector:	**Waste Collection:** Services and infrastructure for the collection of industrial, and hazardous waste.	Important	Unclassified	N/A
	Waste Treatment: Facilities and processes for treating waste to reduce its volume, toxicity, or environmental impact.	Important	Unclassified	N/A

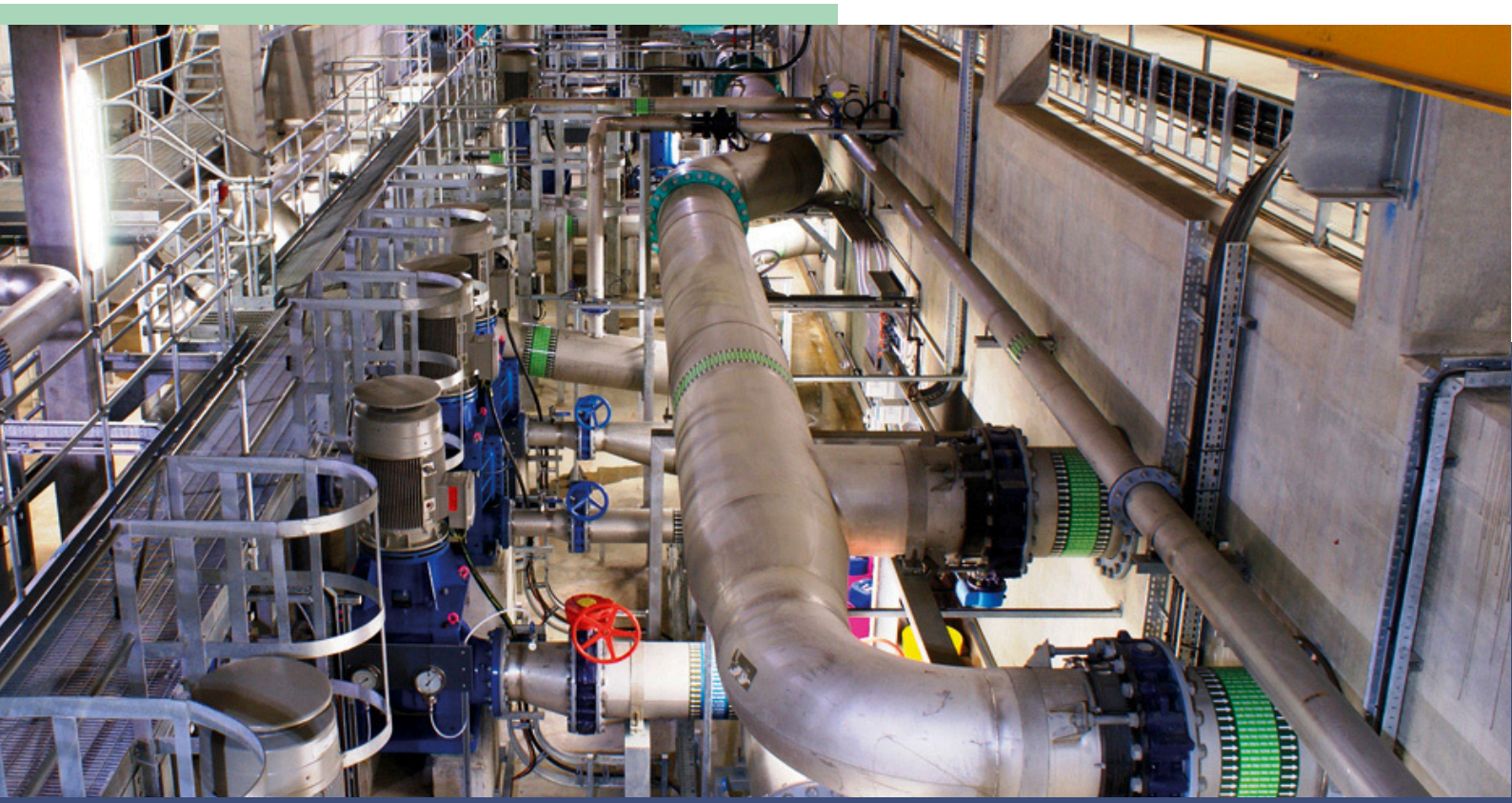
Sector	Subsector	Large Providers (50 Workers+)	Medium Providers (25-49 Workers)	Small Providers (5-25 Workers)
Waste Management Sector (Continued):	**Waste Disposal:** Landfills, incinerators, and other facilities for the final disposal of waste.	Important	Unclassified	N/A
	Recycling and Recovery: Processes and facilities for recycling materials and recovering energy from waste.	Important	Unclassified	N/A

Research Category

Research Sector:	**Research Institutes:** Organisations dedicated to scientific, medical, chemical and technological research	Important	Unclassified	N/A
	Collaborative Research Networks: Partnerships and consortia formed to advance research initiatives.	Important	Unclassified	N/A

4

PROPOSED ASSURANCE FRAMEWORK



A designation of 'Essential' or 'Important' will determine the level of assurance a provider is expected to comply with.

Proposed Assurance Framework

Depending on an providers designation they will be required to work to a framework to assure the Responsible Authority (see section 5) that it is compliant and secure.

The below diagram provisionally illustrates the difference in assurance frameworks that 'essential' and 'important' providers will have to follow.

Essential Providers	Important Providers
Annual Cyber-security & Resilience Risk Assessment and certification	Triennial risk assessment certifcation or post event on demand
Business Continuity Plans	Business Continuity Plans
BCP Annual Testing	BCP Testing
Continuous Improvement Regime	
Identify core service delivery roles and minimum staffing levels	Identify minimum staffing levels
Independent certified compliance every 3rd year	Independent certified compliance post-event as required
Registration of particulars	Registration of particulars
Circumstance change notification (immediate)	Annual verification of particulars
On-site and off-site supervision (incl audits)	Post-event supervision (incl audits)
Information requests	Information requests
Event notification Regime	Event notification Regime

*For registered providers there will be a general duty to adopt cyber security and resilience measures.

5

RESPONSIBLE AND TECHNICAL AUTHORITY

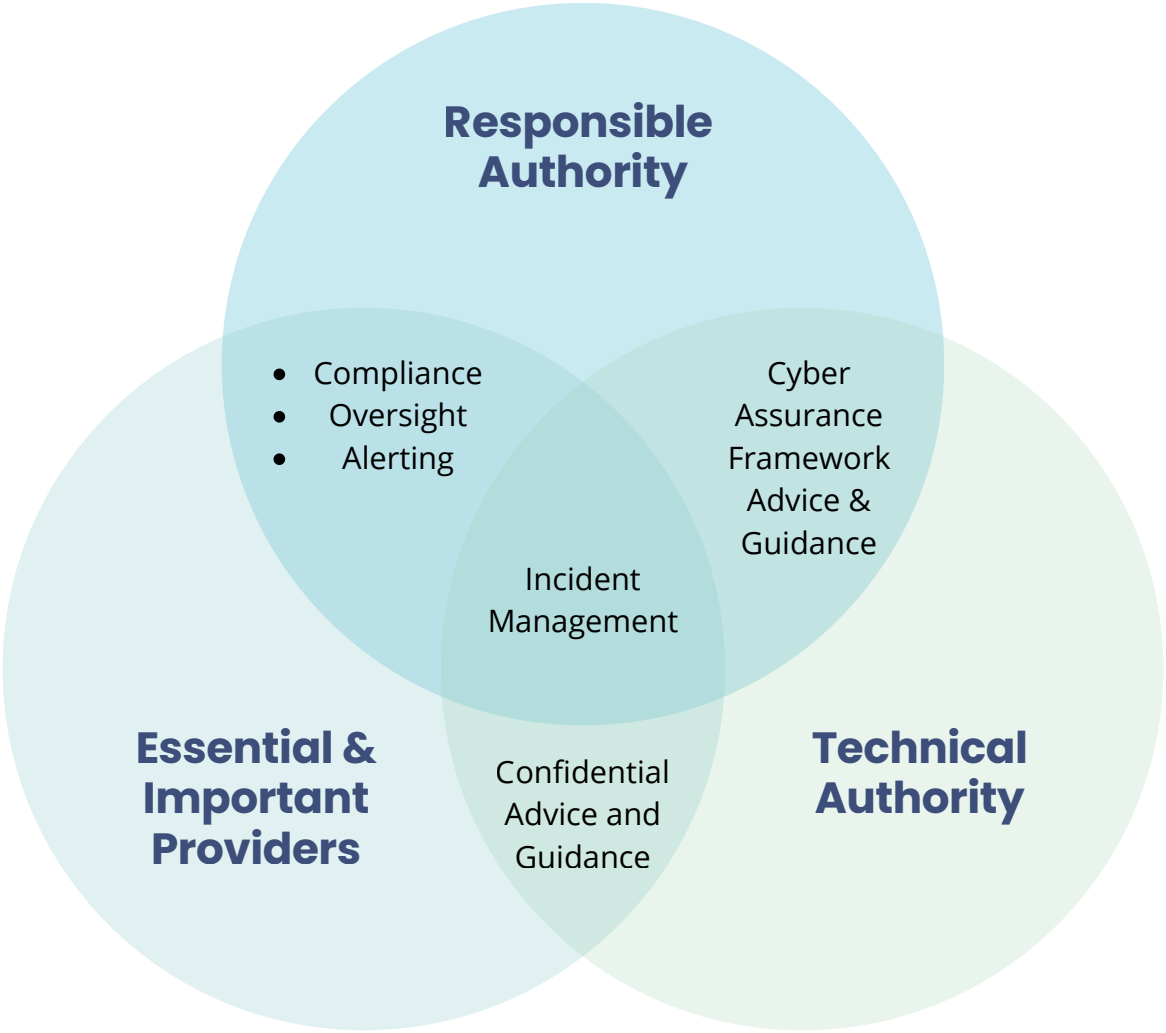
NISB will require the designation or establishment of Responsible Authority(ies), whose purpose will be to ensure compliance with the assurance framework. The Responsible Authority(ies) will be supported by a Technical Authority.

Responsible and Technical Authority

The ability to provide oversight, through a Responsible Authority was supported in the consultation conducted in March 2024. However, there were different views on where the Responsible Authority should sit and how this should be operated. The Responsible Authority will be advised on matters through a Technical Authority. While it was agreed the Responsible Authority should be supported by the operations of the Technical Authority, the exact structure is yet to be determined.

The Department has conducted some research using examples from other jurisdictions, and whilst it is still to be fully determined, there have been some suggestions that wherever possible efforts should be taken to minimise the number of regulators or Responsible Authorities a provider might have to report to.

The diagram below illustrates the relationship between the Responsible Authority, Technical Authority and those providers which fall under the scope of the legislation.



Functions of a Responsible Authority (RA)

The Responsible Authority(ies) will be responsible for the oversight and compliance regime associated with the requirements of the legislation. Amongst the requirements, it is envisaged they will:

- Be impartial and not conflicted
- Establish and manage registration and administration
- Ensure compliance
- Instigate investigations

Functions of the Technical Authority (TA) for resilience and cyber-security

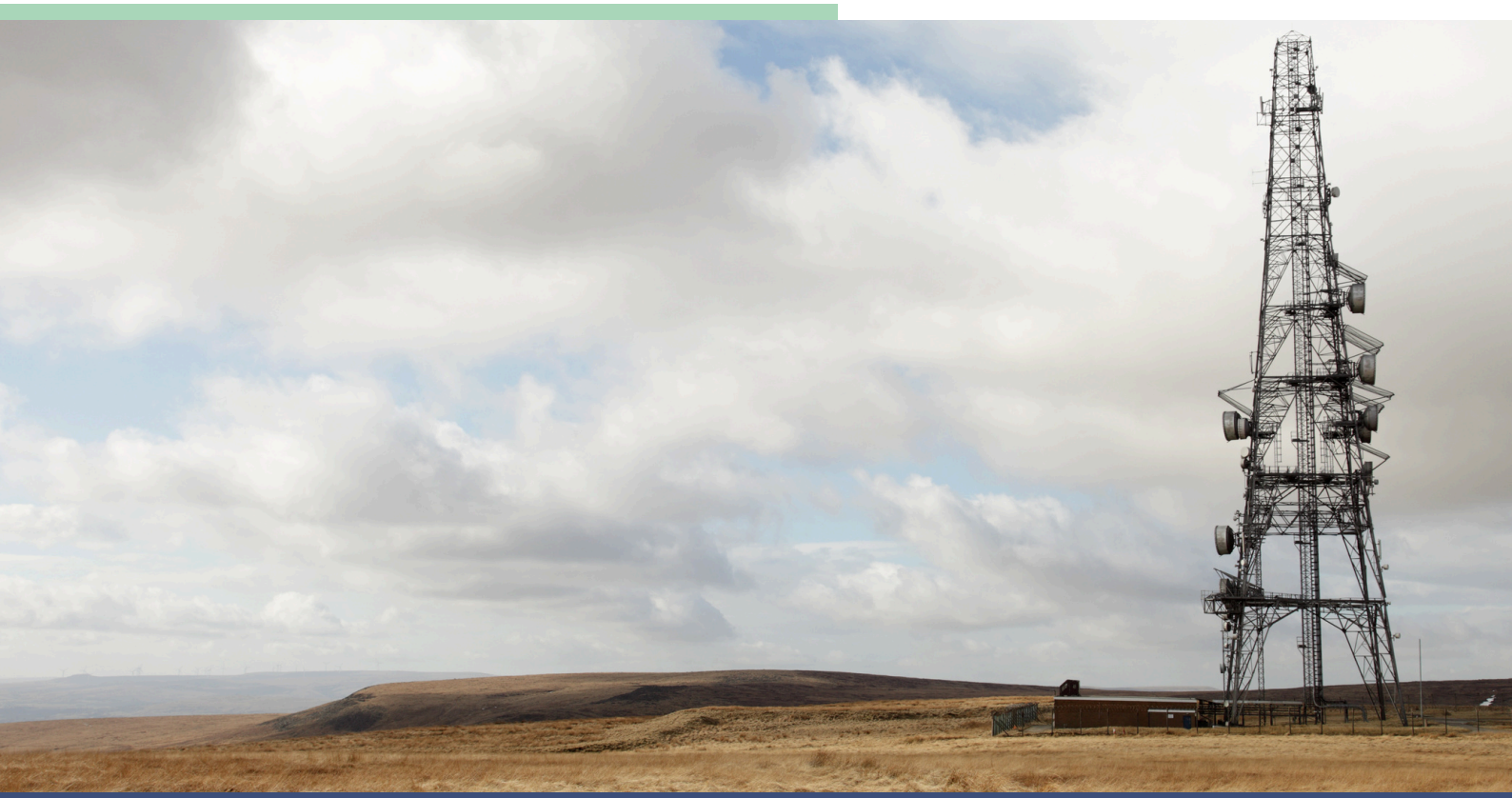
A technical authority is responsible for establishing, approving, and assessing conformance to technical, safety, and certification requirements and policies for products and processes.

Whilst the Responsible Authority(ies) will be the oversight and compliance body the Technical Authority will:

- Be impartial and not conflicted
- Provide independent advice and guidance to the RA on matters relating to NIS, resilience and cyber security, including compliance frameworks.
- Provide independent advice and guidance to the CNI providers on matters relating to NIS, resilience and cyber-security
- Provide incident management oversight
- Monitor intelligence, vulnerabilities, risks and issues
- Act as the cyber security single point of contact for other technical authorities/ jurisdictions
- Undertake resilience and cyber-security investigations and reports for the RA

6

DESIGNATED VENDOR NOTICES, DIRECTIONS AND INFRASTRUCTURE PROTECTION ORDERS



The Government and Responsible Authority will have the ability to control or restrict the use of certain equipment for use in the National Infrastructure and to takes steps to protect the services.

Designated Vendors

DESIGNATION OF HIGH-RISK VENDORS

Under the proposed legislation the Government, with the consent of Tynwald, will have the authority to designate a vendor as a high-risk vendor if the vendor is deemed to pose a significant risk to national security and critical infrastructure. Before making such a designation, the Government is required to consult with the responsible authority to ensure a thorough evaluation of the potential risks involved.

Should a vendor or provider be deemed high-risk, a direction or notice can be issued.

DESIGNATED VENDOR NOTICES AND DIRECTIONS

It is proposed that a Minister will have the authority to designate a supplier to the CNI a High Risk Vendor (HRV). This would be in the scenario where the risk of continued use of the supplier (HRV) has been identified as potentially a matter of national security or threat to the economy and society of the Island. Under these circumstances the Minister, may issue a Designated Vendor Notice (DVN) to the supplier identifying the risk and requesting a course of action to be considered to mitigate the risk.

Once a supplier has been identified as a HRV the RA can issue, to all parts of the CNI that potentially make use of the HRV, a Designated Vendor Direction (DVD) which will detail actions to be undertaken to mitigate the risk. This may be controls to be adopted or implemented through to a requirement to cease use.

IMPLEMENTATION

The RA will be required to oversee the DVN and any liaison with the HRV in regard to the identified risk that may be considered. The RA will then be charged to issue the DVD to any CNI providers that might be impacted or effected by the HRV risk.

Infrastructure Protection Orders

The Government will have the authority to issue a Infrastructure Protection Order where it appears that the critical service being delivered by an Essential Provider might be at risk of disruption.

The order, which is only applicable for a short period of time, can require a provider, organisation or other persons to ensure that the critical service named in the order is not adversely disrupted or impacted.

An infrastructure protection order may only be issued where there is a risk of disruption to a service delivered by an Essential Provider. It will be supported by a thorough risk assessment and will be timebound.

The Responsible Authority will be required to oversee any Infrastructure Protection Orders.

7

INCIDENT NOTIFICATION

Providers which fall under the scope of the legislation will be required to report some incidents within a certain timeframe.

Incident Notification

NISB will impose notification obligations in phases, for incidents which may have a 'significant impact' on service delivery. These notifications must be made to the relevant responsible or technical authority, depending on final legislation.

ASAP

EARLY NOTIFICATION

When a provider **suspects** a potential threat that **may** impact services or National Infrastructure, they must promptly notify the technical authority with relevant details.

Within 24 hours

REPORT

When a risk or event **affects** or is **going to affect** service delivery or National Infrastructure, they must promptly notify the technical authority with relevant details, including any additional information within 24 hours.

Within 72 hours

INTERIM REPORT

To be provided within 72 hours of an event or as required by the technical authority together with as much relevant information as might be required or requested by the technical authority.

As Requested or When Available

UPDATE REPORT

where new or relevant information becomes available or is reasonably requested by the technical authority.

Within 1 Month

FINAL REPORT

to be submitted within 1 month of event closure

As required, the Technical Authority **may** inform other providers whose service delivery may be impacted whilst maintaining levels of confidentiality.

Glossary

Responsible Authority (CA)	The body or bodies designated to have regulatory powers
Cyber Assurance Framework (CAF)	An approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible
Computer Security Incident Response Team (CSIRT)	The Computer Security Incident Response Team (CSIRT) is a team charged handling cyber-security incidents.
Critical National Infrastructure (CNI)	Hose components of the National Infrastructure whose disruption would severely impact national security, economic stability, public health, or safety as listed in Schedule 1 or otherwise designated as such.
Designated Vendor Direction	A direction issued by the Minister
Designated Vendor Notice	A notice issued by the responsible authority
Essential Providers	Providers operating in sectors identified as essential for the maintenance of critical societal and economic functions, including energy, finance, health, transport, water and digital infrastructure;
High Risk Vendor	Means a vendor who poses a significant risk to national security and critical infrastructure;
Important Providers	Providers operating in sectors identified that are essential for the provision of public services or have a significant impact on economic activity;
Infrastructure Protection Orders	An order issued by a Minister requiring certain steps to be undertaken where it is anticipated that a change of circumstances in connection with a provider or providers might adversely impact service delivery

Glossary

National Infrastructure	Means the systems and assets, including physical, digital, and organisational, that are essential to the functioning of the Isle of Man and its economy
Network and Information Security Directive (EU NIS2)	The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.
Network and Information Systems Regulations 2018 (UK)	Provides legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential and digital services.
Resilience	The ability of the national infrastructure to resist, absorb, recover from, and adapt to adverse events and disturbances.
Technical Authority (TA)	Expert-based advice and guidance in all aspects of cyber-security.
Telecommunications (Security) Act 2021	Requires telecoms providers, overseen by Ofcom, to design and manage their networks to protect against existing and future threats to the UK's network security
Unclassified Providers	A registered provider that is neither essential or important.

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

Issue	Description of Change(s)	Approval	Date of Issue
1.0	• Initial Issue	DHA/CSC	30/12/2024
2.0	• Tables and References to tables updated • Change of wording to CA and TA pages • Change of wording to designated vendor direction and notices and service protection orders	DHA/CSC	21/03/2025
3.0	• Tables updated • 'Competent Authority' has changed to 'Responsible Authority' • 'Entity' has changed to 'provider' • Service Protection Orders now read as Infrastructure Protection orders	DHA/CSC	TBC

Cyber Security Centre for the Isle of Man

Department of Home Affairs
Rheynn Cooishyn Sthie

Office of Cyber-Security & Information Assurance
Second Floor
27-29
Prospect Hill
Douglas
Isle of Man, IM1 1ET

T: +44 1624 685557

Isle of Man Government