Office of Cyber-Security
& Information Assurance

Oik son Shickyrys Lectraneagh as Sauçhys Fysseree

CSC

Cyber Security Centre
for the Isle of Man

NATIONAL INFRASTRUCTURE SECURITY BILL (NISB)

Consultation Response

1. Background

Isle of Man residents should have confidence in the security and resilience of national infrastructure sectors to deliver essential goods and services. Essential services – 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 entities 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 security and resilience for core services on the Isle of Man, which rely heavily on digital services.

The Department ran a consultation to seek views from interested parties on the key policy principles that would be used to draft the National Infrastructure Security Bill.

This report provides a summary of the responses received.

2. Overview of responses

The public consultation opened on the 5 February 2024 and closed on the 25 March 2024. The Department received 53 responses to the consultation, 48 of which were received via the consultation hub. The 53 responses comprised:

- 36 Members of the public
- 7 Private Companies
- 6 Government Departments, Offices or Boards
- 1 Industry Body
- 1 Local Authority
- 2 not identified

Principle 1: Protection of the Island's National Infrastructure should be supported by legislation

Principle 2: Those sectors that form the Island's National Infrastructure should be identified and included in the scope of the legislation

Q1: Listed below are sectors which could be included in the scope of the legislation. Please tick those ones which you feel are part of the Isle of Man's National Infrastructure and add any you may feel have been omitted.

There were 45 responses to this part of the question.

Option	Total	Percent
Energy – including Electricity, Oil and Gas	45	84.90%
Transport – including Air, Sea and Road	43	81.13%
Financial Services – including banking and market infrastructure	33	62.26%
Health – For example, Hospitals, Research and Public Health Laboratories, Primary Care, Mental Health Services, and Social Care	41	77.35%
Blue Light Services – For example, Police, Fire & Rescue, and Ambulance	40	75.47%
Water – drinking and waste	43	81.13%
Digital infrastructure – including Internet Exchanges, DNS* providers, Cloud computing, Data Centre services, content delivery networks, trust service providers, electronic communication network providers and publicly available electronic communication services	41	77.35%
Information Communication Technology (ICT) service management (business to business)	25	47.17%
Government – public administration, entities of central government	39	73.58%
Space – operators of ground based infrastructure that support the provision of space-based services – excluding public electronic communications networks.	15	28.30%
Postal and courier services	28	52.83%
Waste management	29	54.71%
Chemical manufacturing, production, and distribution	16	30.19%
Food production, processing and distribution	32	60.37%
Manufacturing	17	32.07%
Digital providers	17	32.07%
Research	11	20.75%

Other (Please specify)	12	22.64%
Not Answered	8	15.09%

Commentary

Based on responses received, the sectors listed within the consultation were felt to represent the Isle of Man's National Infrastructure.

The information provided will be used to form the basis of a definition of the Isle of Man's National Infrastructure.

Following approaches taken in other jurisdictions once a definition has been drafted, the Department will seek to engage with those sectors who would be in scope and determine whether a sector would meet the definition and any threshold that might be set.

Some comments on this question were as follows:

'*Whether a sector should be included in the scope of the legislation depends upon how reliant we are upon it. Whether it is the sole provider, such as the MUA or the Steam Packet, or whether its customer base represents a significant percentage of the population (e.g. gas), or whether it is so integrated into society that the disruption of its services has a profound impact on the normal everyday life of Island businesses and residents'.*

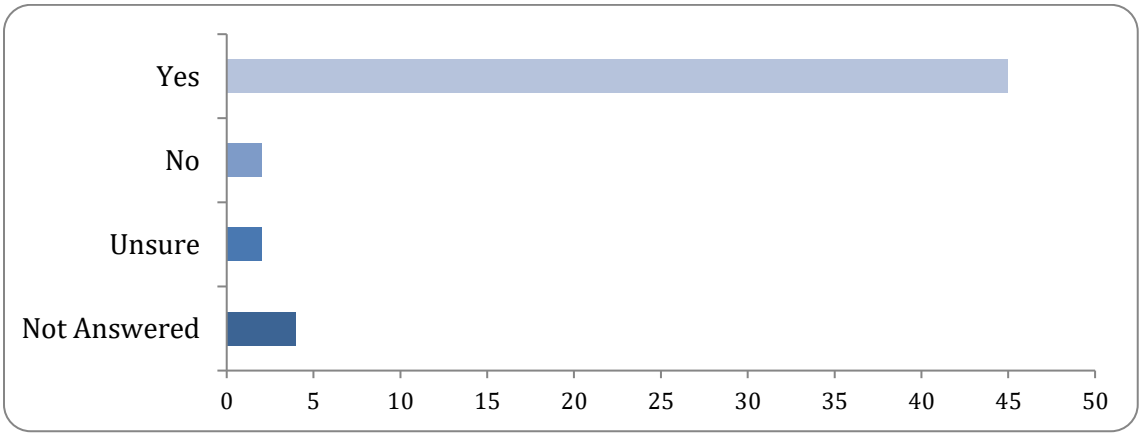
'*Once the Department has outlined what it means to be a part of the island's national infrastructure, it will be possible to undertake an assessment of whether a sector meets the definition and threshold. We would welcome an opportunity to discuss this with the Department and agree a definition for "National Infrastructure on the Isle of Man" before agreeing which sectors and/or organisations should be included within that definition.'*

Principle 3: The legislation should be equivalent to measures introduced in other jurisdictions whilst remaining flexible to meet the fast paced changes and threats to the national infrastructure

Principle 4: Any legislation introduced should be proportionate to the needs of the Isle of Man

Q2: Do you agree that the Isle of Man when drafting its own legislation should take into consideration similar legislation introduced in the UK, EU or elsewhere?

Option	Total	Percent
Yes	45	84.90%
No	2	3.77%
Unsure	2	3.77%
Not Answered	4	7.54%



Q2a: Are you aware of legislation in another jurisdiction which contains similar policy principles and consider that this might be a good model to review in the preparation of instructions for the legislation?

There were 50 responses to this part of the question

Option	Total	Percent
Yes	18	35.29%
No	32	62.74%
Not Answered	1	1.96%

Q2b: Where respondents said 'yes', comment which jurisdiction(s) contains

similar policy principles that might be a good model to review in the preparation of instructions for the legislation.

There were 17 responses to this part of the question

Q3: Any other comments on Principles 3 & 4?

There were 14 responses to this part of the question

Commentary

Responses support the principle that the Isle of Man should consider legislation introduced in other jurisdictions. However, two thirds of respondents were not able to say what other legislation should be used.

Of those that did suggest jurisdictions whose legislation could serve as a good model, the EU Network and Information Security Directive as well as the UK's Network and Information Security Regulations were the most referenced. With respondents stating that differing too far from these pieces of legislation may prove problematic for multi-jurisdictional businesses.

Furthermore, the key theme of proportionality was mentioned consistently, with respondents wishing to highlight the nature of island businesses when drafting any legislation.

Some comments are as follows:

'UK and EU. Deviating from their policies would prove problematic, particularly around digital infrastructure and cloud service which are designed for, and bound by, UK and EU law.'

'We do believe in taking other legislation into consideration e.g the NIS2 directive., the US NIST cybersecurity framework, and the new AI EU Act with associated conformity assessments. However, the uniquely different situation of a small Island Nation needs to be considered carefully'

'We agree that established legislation and security frameworks in other jurisdictions represent a sensible starting point for the Isle of Man in developing its own security framework, and thus we agree that the legislation in the UK, EU, and US can be an initial reference point for the Department. However, it would not be appropriate or proportionate to simply transpose aspects of each of those legislative frameworks into the Isle of Man's putative National Infrastructure Security legislation.'

Principle 5: A minimum level of resilience and security should be specified for each of the designated sectors of the Island's National Infrastructure

Principle 6: The ability to provide oversight and management of the sectors of the National Infrastructure should be established in order to ensure minimum levels of resilience and security are achieved

Q4: Cyber Assurance Frameworks (CAFs) exist to protect organisations by providing a standardised system of guidelines and best practice. If you are aware of CAFs that might provide a good model to review in the preparation of instructions for the legislation, please confirm which frameworks and why:

There were 20 responses to this question.

Some of the comments were as follows;

'*The UK NCSC already have a CAF process for use with UK Critical National Infrastructure organisations'*

'*We believe that the NCSC's Cyber Assessment Framework ("CAF") could act as a good model for a similar framework in the Isle of Man5 . The NCSC's CAF is already well-established, widely understood, and followed by numerous Government departments and Critical National Infrastructure providers in the UK. Following such a well-established model would enable National Infrastructure sectors/organisations in the Isle of Man to consider 'what good looks like' by looking at examples in the UK context and getting advice on implementation from the NCSC'*

Q5: If a competent authority was to be established, where do you think would be the most appropriate place for this authority to sit and why:

There were 48 responses to this part of the question.

Option	Total	Percent
Government Department (please specify)	7	13.20%
New Statutory Board	18	33.96%
Arm's length organisation	9	16.98%
Existing regulator where appropriate	10	18.86%
Other (please specify)	4	7.54%
Not Answered	5	9.43%

Q5a: Where respondents said 'Government Department', they were asked to specify which government department

There were 8 responses to this question

Some comments were as follows;

'Needs to be arm's length to hold departments to account'

'Government Department – Office of Cyber-Security & Assurance. For the avoidance of doubt, we believe that the legislation should enable the creation of one Competent Authority that is responsible for ensuring compliance and developing security frameworks for the Isle of Man.'

Q5b: An additional option to comment on and justify respondent's selection was given.

There were 12 responses to this optional part of the question.

Some comments were as follows;

'*We would encourage adoption of a model in force elsewhere, be that the UK or potentially one of the other crown dependencies.'*

'*Possibly CURA or the ICO given they have existing regulatory powers, but would need to be suitably resourced with appropriate expertise'*

Q6: Who should provide oversight/monitoring for a competent authority?

There were 46 responses to this part of the question.

Option	Total	Percent
Government Department (please specify)	8	15.09%
Board (public sector)	6	11.32%
Board (public and private sector)	26	49.05%
Board (private sector)	6	11.32%
Not Answered	7	13.20%

Q6a: Where respondents said 'Government Department', they were asked to specify which government department

There were 8 responses to this question.

Some comments were as follows:

'There has to be independence but supported by a parent Government Dept such as CabO or DHA'.

'There should be a mix of private and public experts to oversight operation/implementation, which should report periodically to the Govt Dept, ultimately for public consumption.

Q6b: Any other comments for principle 5 & 6

There were 19 responses to this part of the question.

Some comments were as follows:

'The competent authority will require a depth of experience. Oversight and monitoring public and private sector board with aim of combining depth of experience with authority of Government policy.'

'Establishing a new competent authority for overseeing cybersecurity capabilities under the guidance of a board comprising private and public sector members presents a strategic advantage for the Isle of Man. It ensures dedicated focus, specialized expertise, balanced governance, enhanced collaboration, operational agility, and a commitment to innovation. This approach aligns with the National Infrastructure Security Bills (NISB) objectives to protect the nation's critical infrastructure from cyber threats and build a resilient digital environment for the future.

Commentary

Responses indicated a preference for using the UK National Cyber Security Centre's Cyber Assurance frameworks as an appropriate way to evidence compliance.

The ability to provide oversight, through the creation of a Competent Authority was also supported. However, there were different views on where the Competent Authority should sit and how this should be operated.

The Department will conduct some further research using examples from other jurisdictions before proposing a model for the Isle of Man.

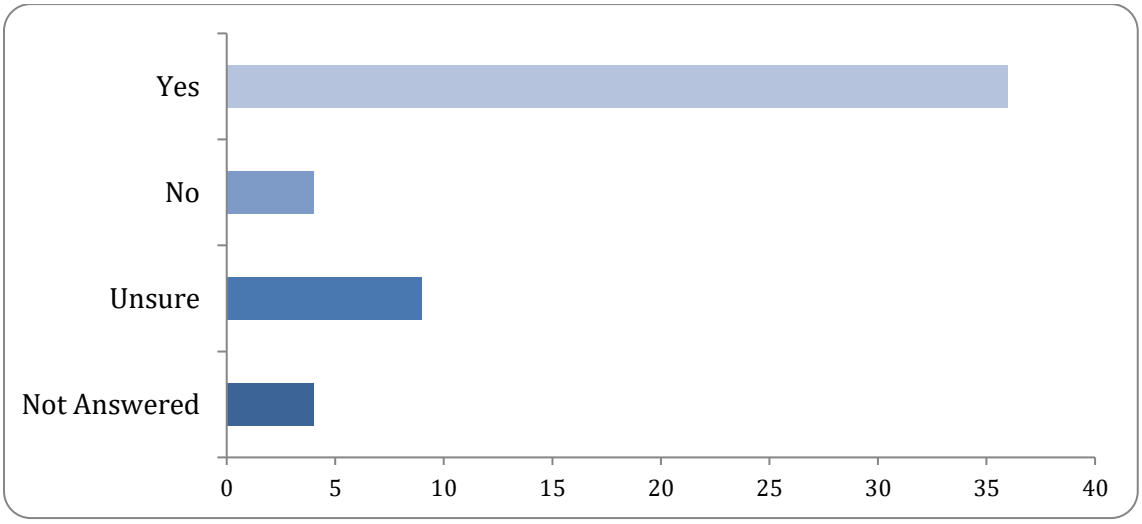
Principle 7: Support for the sectors of National Infrastructure should be provided by the introduction of a threat and incident management capability

Principle 8: Compliance framework

Q7: Should the threat and incident management capability (CSIRT) support and advise the Competent Authority/regulator in drafting the appropriate minimum levels of compliance as described in Principle 5?

There were 49 responses to this part of the question.

Option	Total	Percent
Yes	36	67.92%
No	4	7.54%
Unsure	9	16.98%
Not Answered	4	7.54%



Some comments were as follows;

'Yes- in drafting minimum levels of compliance for onwards consultation. However the segregation between policy setting and regulation should be maintained.'

'I have answered yes because, in my experience, the partnership between CSIRTs and the Competent Authority/regulator in crafting compliance frameworks is not merely beneficial; it is essential for ensuring that the Isle of Man's cybersecurity regulations are grounded in practical, actionable intelligence. This collaborative approach ensures

compliance measures reflect the latest cyber threats and industry best practices, thereby enhancing the overall security and resilience of the national infrastructure. Adopting this approach aligns with global best practices and positions the Isle of Man as a proactive and informed cybersecurity governance leader. This argument rests on several foundational pillars that underscore the criticality of this collaborative approach.

Q8: Who should be responsible for operations of the CSIRT?

There were 46 responses to this part of the question.

Option	Total	Percent
Government	11	20.75%
The designated competent authority	31	58.49%
Private sector	1	1.88%
Other (please specify)	3	5.66%
Not Answered	7	13.20%

Some comments were as follows;

'To promote an open and collaborative relationship between the CSIRT and the Authority, the competent Authority should be responsible for the operations of the CSIRT. This will enhance the competent authority's understanding and oversight of the cyber landscape which it regulates. Regular communication between the CSIRT and the Authority can also be beneficial when considering the development and maintenance of the CAF, as the CSIRT will have a better understanding of the risk horizon than the Authority will. The Island should also consider looking to the UK system to garner support and operational delivery due to the close reliance of, connectivity and provision to the UK across near all of the Island's national infrastructure provisions.'

Q9: Do you agree that a competent authority should have the ability to:

There were 46 responses to this part of the question.

Option	Total	Percent
Issue enforcement notices	36	67.92%
Fine an organisation	32	60.37%
Pursue criminal prosecution	26	49.05%
None of the above	4	7.54%
Other (please specify)	9	16.98%
Not Answered	7	13.20%

Some comments were as follows:

'We agree that the Competent Authority should have the legislative powers to undertake investigations and take enforcement action, including financial penalties where appropriate to do so. However, we do not agree that it would be appropriate for the Competent Authority to pursue criminal prosecutions. Where potentially criminal conduct has been identified, the Competent Authority should pass this on to the Attorney General and Prosecution Division for prosecution, which is well-placed to provide an expert and objective view as to whether a prosecution would be appropriate given the circumstances.'

Q10: Should organisations that come under the scope of any legislation be required to conduct a self-assessment, outlining their compliance with a Cyber Assurance Framework (CAF)?

There were 46 responses to this part of the question.

Option	Total	Percent
Yes, self-assessment should be conducted quarterly	9	16.75%
Yes, self-assessment should be conducted six monthly	5	9.43%
Yes, self-assessment should be conducted annually	23	43.39%
Yes, self-assessment should be conducted but in an alternative timeline (please specify)	2	3.77%
No	5	9.43%
Unsure	2	3.77%
Not Answered	7	13.20%

Some comments were as follows:

'There needs to be a balance struck between firm's own internal and external audit processes, any self-certifications and potential for competent authority assessments. The Government must recognise cyber threat is a major cost area for firms today and is set to increase in the future - so measures adopted must be proportionate for the IOM and its constituents (costs) whilst still achieving the heightened security levels sought on this consultation.'

'Self-assessments should be required to be submitted annually, however, in the event of significant changes to an organization's cyber infrastructure, provision, etc. then recertification should be required. Rationale behind recertification is that it provides both

the authority, and the organisation with a better understanding of the threats and vulnerabilities within their infrastructure, giving the organisation an opportunity to put in mitigating factors, rather than wait for recertification of a cycle basis.'

Q10a: Where respondents said 'yes', but their timeframe was not listed, they were asked to specify what timeframe

Some comments were as follows;

'Yes, we believe that self-assessment and self-certification of compliance with the CAF would be an appropriate and proportionate approach. The regularity with which such an assessment should be conducted should be informed by (a) the size, scale, and complexity of the CAF, and (b) the risks faced by a given organisation or sector. We recommend that self-assessment should be undertaken on an annual basis or biannual basis, depending on the factors just described.'

'Full detailed (re-)certification measures should occur biennially (every other year/2 years). As with self-assessments, recertification should have to take place upon significant changes occurring within the entity's infrastructure. An annual high-level self-certification, and or statement of compliance, should be required from each registered entity to the authority'

Q11: In order to assure compliance with a CAF, independent certification measures might be required. Do you think independent certification measures should be required and if so, how often should they have to occur?

There were 48 responses to this part of the question.

Option	Total	Percent
Yes, they should be required annually	22	41.50%
Yes, they should be required biannually	5	9.43%
Yes, they should be required triennially	5	9.43%
Yes, they should be required but in an alternative timeline (please specify)	3	5.66%
No, I don't think they should be required	4	7.54%
Unsure	9	16.98%
Not Answered	5	9.43%

Q11a: Where respondents said 'yes', but their timeframe was not listed, they were asked to specify what timeframe

There were 3 responses to this question

'They should not be scheduled but instead compliance should be readily observable at any time - scheduled audits use large amounts of resources as people drop everything to prepare for an audit - all evidence should be obtainable within 1 hour - this is more likely to drive compliance as continual reporting and adherence is the only way to solve this'

'Yes, we believe that self-assessment and self-certification of compliance with the CAF would be an appropriate and proportionate approach. The regularity with which such an assessment should be conducted should be informed by (a) the size, scale, and complexity of the CAF, and (b) the risks faced by a given organisation or sector. We recommend that self-assessment should be undertaken on an annual basis or biannual basis, depending on the factors just described.'

'Yes, we agree that independent certification of CAF compliance should be undertaken. This should be done on a risk-based approach, with higher risk organisations and sectors being audited more regularly than lower risk organisations and sectors. The regularity with which independent certifications take place should be informed by how often organisations and sectors are required to self-assess. For example, if the telecommunications sector is required to self-assess compliance with the CAF on an annual basis, then it would be sensible for telecommunication organisations to obtain independent certification on a bi-annual or triennial basis.'

Q12: Any additional comments about independent certification measures?

There were 11 responses to this part of the question.

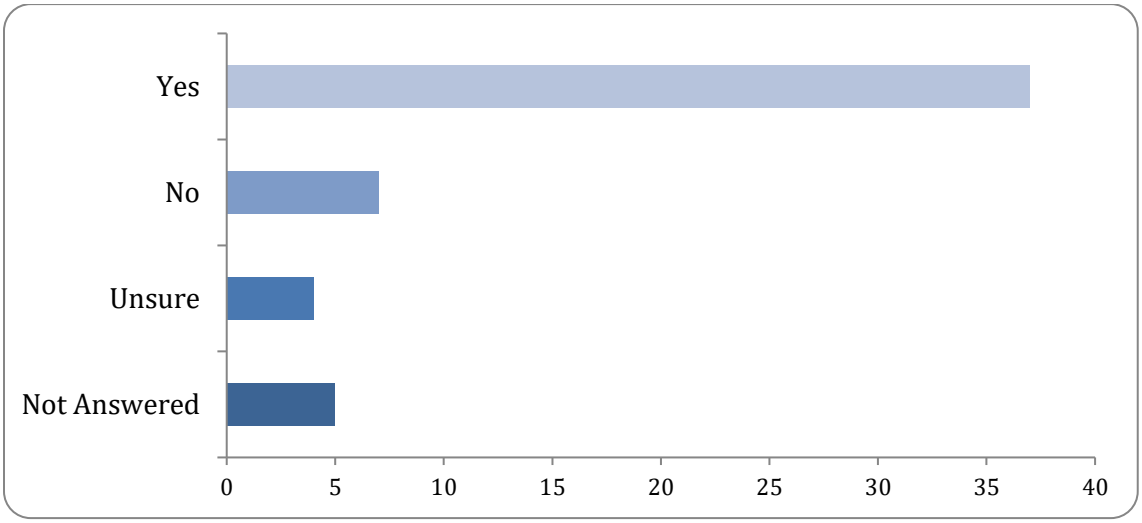
'There is a cost involved for these things and so every 3 years and an option for the authority to require in certain circumstances'

'Yes, we agree that independent certification of CAF compliance should be undertaken. This should be done on a risk-based approach, with higher risk organisations and sectors being audited more regularly than lower risk organisations and sectors. The regularity with which independent certifications take place should be informed by how often organisations and sectors are required to self-assess. For example, if the telecommunications sector is required to self-assess compliance with the CAF on an annual basis, then it would be sensible for telecommunication organisations to obtain independent certification on a bi-annual or triennial basis'

Q13: Should the Competent Authority have the authority to require an independent assessment as and when it sees fit?

There were 48 responses to this part of the question.

Option	Total	Percent
Yes	37	69.81%
No	7	13.20%
Unsure	4	7.54%
Not Answered	5	9.43%



There were 13 additional comments, some of which included:

'Rather than when it sees fit, the Competent Authority should have the authority to require an independent assessment based upon pre-defined criteria. This pre-defined criterion should be based upon and aligned to agreed SLA's / KPI's / CSFs/ CRFs relative to the sector and take the form of a decision matrix. Upon the relevant criteria being met, only then should the Competent Authority be able to use its authoritative powers and enforce an independent assessment.'

'Yes, we support this. However, where the Competent Authority decides that an independent assessment is required, it should be required to fully explain and justify this decision and, where appropriate, consult with relevant stakeholders.'

Commentary

There was general support for the creation of a CSIRT that would act as a technical advisor to the competent authority. However, comments highlighted the need for segregation between policy setting and regulation.

The department will conduct further research into how this will work in practice.

There was agreement that the competent authority should be responsible for the operations of the CSIRT.

Respondents were also in favour of the competent authority having powers that ranged from enforcement notices through to criminal prosecution. Comments reflected that the competent authority needed these powers to ensure acceptable level of compliance.

Approval for self-assessment of compliance with a Cyber Assurance Framework was also provided. However, there were concerns that this should not create unnecessary work, or become a burden to the organisations.

The need for independent certification measures was also agreed upon by respondents. However, there were different views on the frequency on which these should happen. Alongside this there was also a clear majority in favour of a competent authority being able to require/conduct an independent assessment where justified.

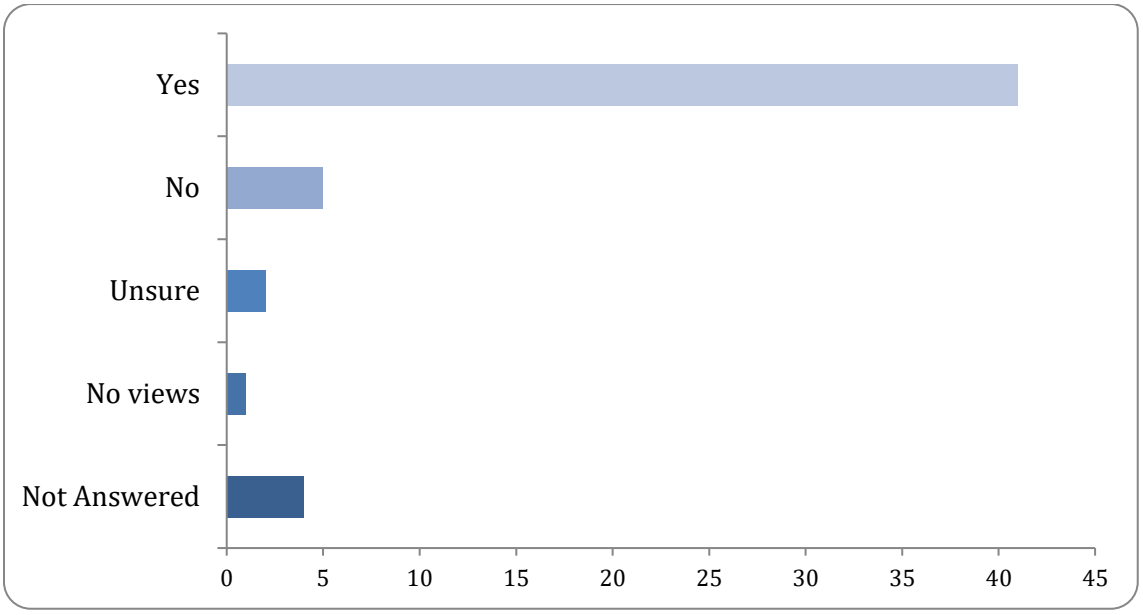
These comments will be taken into account when establishing a suitable compliance framework.

Principle 9: Reporting obligations

Q14: To ensure adequate protection of the National Infrastructure, do you agree that entities that fall under the scope of the legislation should be required to notify of emerging risks, issues or 'near misses'?

There were 49 responses to this part of the question.

Option	Total	Percent
Yes	41	77.35%
No	5	9.43%
Unsure	2	3.77%
No views	1	1.88%
Not Answered	4	7.54%



There were 19 additional comments added, some of which included:

'This is an important aspect of community safety. If the CA / CSIRT are alert to a potential risk or issue appropriate 'sanitised' advice and guidance can be issued in a timely manner.''

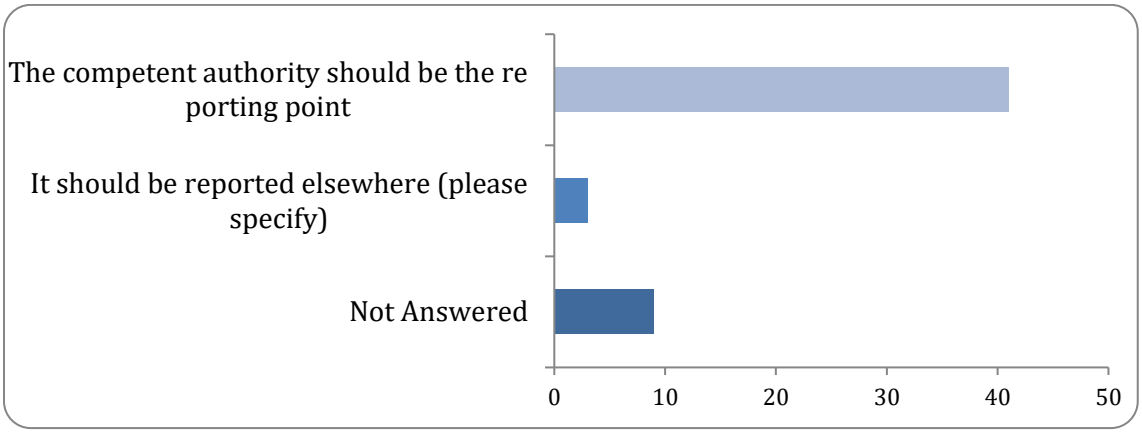
'Promoting an "Open Risk" culture on the island will provide a conducive environment for managing cyber risk, and will contribute to the overall security of the citizens.'

'This needs to be seen as a shared resource for all bodies falling under the legislation and should be notified and shared (where appropriate) in a timely fashion'

Q15: If a competent authority with responsibility for implementing the proposed legislation is established, should they be the reporting point or should this be reported elsewhere?

There were 44 responses to this part of the question.

Option	Total	Percent
The competent authority should be the reporting point	41	77.35%
It should be reported elsewhere (please specify)	3	5.66%
Not Answered	9	16.98%



There were 10 additional comments added, some which included:

'The competent authority should have the power to nominate in case the technical capability is elsewhere. Time can be of the essence.'

'The Competent Authority should be the reporting point. This aligns with both the NIS Regulations 2018, and the NIS 2 Directive (which also allows reporting to the CSIRT as appropriate). Ultimately, the Isle of Man should use the NIS Regulations as the baseline for the NISB, therefore the reporting point should be the competent authority.'

Q16: When an incident occurs, what is an appropriate timeframe for organisations to notify the designated body?

There were 49 responses to this part of the question.

Option	Total	Percent
Within 24 hours after discovery	16	30.18%
Within 48 hours after discovery	7	13.20%
Within 72 hours after discovery	10	18.86%
Within 96 hours after discovery	4	7.54%
Other (please specify)	12	22.92%
Not Answered	4	7.54%

*There were 12 responses to the **other** section of the question.*

There were 29 comments to the question.

Comments that were received included:

'There has to be a scale. Urgent issues which could impact life or community should be immediate to allow for contingency planning'

'Often critical services can have a domino affect on other services - being able to react for all entities across the nation is important. Also where one organisation is attacked - others may also be being attacked at the same time - sharing of intelligence is vital'

'The UK NIS Regulations 2018 requires for Operators of Essential Services (OES's) to notify the designated competent authority about any incident which has a significant impact of the service it provides without undue delay, and in any event no later than 72 hours after the operator is aware that the incident has occurred (Regulation 11 (1)-(3))…..'

'We believe that a 72-hour reporting window is an appropriate timeframe. This is for two key reasons: 1. 72 hours will give the affected organisation sufficient time to become aware of the incident and undertake analysis to better understand the nature and scale of the impact. This will, in turn, enable the organisation to provide the Competent Authority with more accurate and comprehensive information about the incident, which will aid the Competent Authority in responding appropriately. 2. It is unclear whether the Competent Authority will be a 24/7/365 organisation or work within defined opening hours between Monday and Friday. If the latter, then, should an organisation become aware of a cyber-incident late on a Friday, it will not be beneficial or efficient to require the organisation to report the incident either late on the Saturday (24 hours) or Sunday (48 hours) if that notification will only be picked up by the Competent Authority on Monday morning (or Tuesday morning if it is a bank holiday).'

Q17: It has been proposed that those entities which fall under the scope of this legislation should only report incidents that are likely to impact the delivery of services. Do you agree with this?

There were 49 responses to this part of the question.

Option	Total	Percent
Yes	18	33.96%
No	27	50.94%
Unsure	4	7.54%
Not Answered	4	7.54%

There were 20 comments to the question, some of which included:

'It may be part of a bigger picture that will only be understood if fully reported. If you allow a determination of whether something should be reported this can introduce uncertainty in the incident response process. Also sharing of incident types allows intelligence sharing and a view of attackers methods and insider threat issues across all organisations may reveal patterns of behaviour that cannot be readily gleaned inside a single organisation'

'They should report any and all incidents. Any incident has the potential to eventually impact the delivery of services if not dealt with properly.

Any should be monitored and tracked for future reference..'

Q18: In your opinion, which of the following incidents do you feel entities that fall under the scope of this legislation should be compelled to report, noting that these may reflect current incident types that may advance or change in the future?

There were 49 responses to this part of the question.

Option	Total	Percent
Ransomware	40	75.47%
Receipt of phishing (email/text/voice)	19	35.84%
Compromise of third party supplier	37	69.81%
Impersonation attempts e.g website impersonation	26	49.05%
Fraud attempts such as gift card or invoice fraud	21	39.62%
Business email compromise	33	62.26%
Malware infection	37	69.81%
Intrusion detection	37	69.81%
Hacking (incl. attempts)	36	67.92%
Other (please specify)	13	24.52%
Not Answered	4	7.54%

*There were 16 responses to the **other** section*

Comments that were received included:

'In theory all of the above could ultimately lead to services being compromised. I would prefer to leave it at that level (e.g. impact service delivery) rather than provide and exhaustive list of examples. As new threats occur, so may new techniques that don't match to one of these scenarios'

'These incidents need to be examples but not exhaustive. I believe the definition of what needs reporting is the important part.'

'This could include any or all depending on the nature of the issue or risk. Binding Guidance is the important factor and based upon an assessment by impacted business. A failure to report or notify should carry a sanction'

Commentary

Respondents agreed that entities should notify the competent authority of any emerging risks, issues or ‘near misses’.

While the majority of respondents agreed that the competent authority should be the reporting point, comments reflected the need to consider the practicalities of this. For example, a competent authority may not be available on a 24-hour basis, and therefore consideration should to be given to a delegation of responsibility based on availability and skills.

There was no consensus on an appropriate timeframe and a range of opinions were expressed. For some respondents urgent notification was essential, whilst others believe that organisations need time to assess what incident is occurring.

This suggests that more consideration needs to be given to reporting timeframes, taking into account comparable legislation in other jurisdictions and other factors mentioned in the consultation, including defining what a reportable incident is.

The consultation asked whether an incident should only be reported if it was to affect the delivery of services, the majority of respondents felt that all incidents should be reported.

The consultation provided examples of reportable incidents and asked for views on whether these types of incidents should be reported. Respondents were keen to highlight that the definition of an incident was more important than a list of examples.

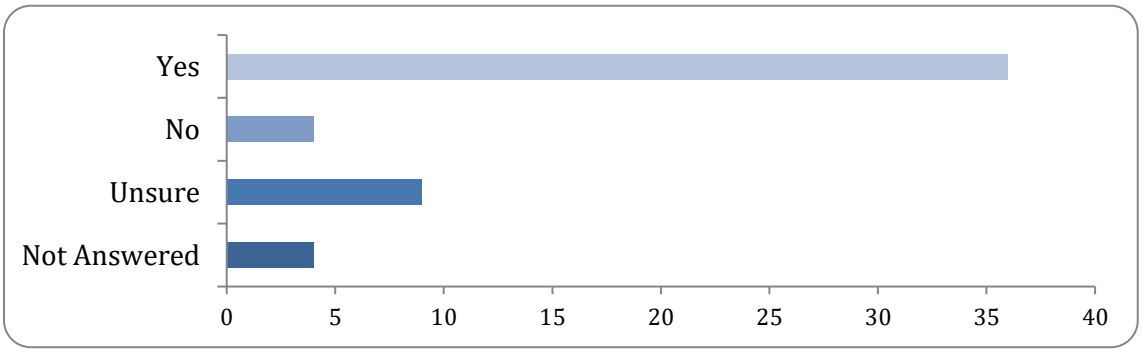
These comments will be taken into account when establishing a suitable definition of reportable incidents.

Principle 10: Transitional Arrangements

Do you agree that transitional periods should be determined by the requirements of each sector and the service delivered?

There were 49 responses to this part of the question.

Option	Total	Percent
Yes	36	67.92%
No	4	7.54%
Unsure	9	16.98%
Not Answered	4	7.54%



There were 16 additional comments, some of which included:

'It would be unfair to impose requirements without providing an opportunity for 'houses to be put in order' however the importance of protecting these sectors means such transitional arrangements would be in a reasonable timeframe or subject to sanctions. The CA might be provided with flexibility within any transitional arrangements providing they are proportionate and justified.'

'Yes. We strongly support the need for an appropriate transitional arrangement and a window within which National Infrastructure providers can become compliant with the new framework.'

'Yes, appropriate time should be given to allow transition to a new standard of security compliance and fine for delay in non-compliance proportionate to the organisations' ability to pay to avoid total loss of service. Consideration should be given to the size of the organisation and its ability to a) complete organisational change within set time frames and b) afford any fines. If the fines are too great this may result in the organisation deciding not to continue providing that service at all. The incentive to move to a stronger cyber security position needs to be balanced and proportionate, both in fines and risk to national infrastructure.'

Commentary

Responses agreed that there should be a transitional period but it was also acknowledged that there should a clear time limit and penalties for non-compliance following the agreed transitional period.