THE HAUNTED LIGHTHOUSE LIMITED

Consultancy & Compliance Briefing

National Infrastructure Security Bill 202x

Readiness Guide for Isle of Man Professional Services Firms

April 2026 -- Version 1.0

What this guide covers

The National Infrastructure Security Bill (NISB) will impose significant new compliance obligations on Isle of Man businesses -- including the technology suppliers and IT support firms serving professional services clients. This guide answers the questions a managing partner or compliance officer would actually ask, in plain English.

Inside this guide:

-- Am I in scope, and at what tier?
-- What does my supply chain assessment need to look like?
-- What standards should I be aligning to now?
-- What are the penalties for non-compliance?
-- A worked example: a 30-person law firm.

About the author

Alan Wright is Director of The Haunted Lighthouse Limited (Co. No. 138512C), an Isle of Man based data protection, cybersecurity, and sovereign infrastructure consultancy. The company holds current Cyber Essentials certification and is registered with the ICO. Alan publishes the Sovereign Auditor newsletter at sovereignauditor.substack.com.

Important notice

This guide is based on the NISB V05 draft bill and the January 2026 consultation response. The Bill has not yet been enacted. Details may change as the Bill progresses through Tynwald and secondary legislation is drafted. This is a general guidance document and does not constitute legal advice.

1. Background -- What is the NISB?

The National Infrastructure Security Bill (NISB) is Isle of Man draft legislation designed to impose minimum cybersecurity and resilience standards across sectors deemed critical to the Island's economy and public safety. It is modelled closely on the UK's implementation of the EU NIS2 Directive, with additional provisions drawn from the UK Telecoms Security Act 2021.

The Bill was published for public consultation in December 2025. The consultation closed on 9 January 2026. Thirteen responses were received. The Department of Home Affairs has confirmed the Bill will proceed with some definitional amendments, and it is expected to reach its First Reading in the House of Keys later in 2026. It has not yet been enacted. No obligations are currently in force.

Secondary legislation -- including the assurance framework regulations, cybersecurity standards, and registration conditions -- will follow separately, each with its own consultation process. This means the detailed compliance requirements are not yet written. However, the structural framework is clear enough to allow organisations to assess their position and begin aligning now.

Key point: The Bill creates the framework. The operative detail comes in secondary legislation. Acting now -- before those regulations are drafted -- puts you ahead of the compliance curve and gives you an input into consultation processes that will determine what the standards actually require.

2. Am I In Scope?

Whether the NISB applies to your organisation depends on two variables: the sector you operate in, and how many workers you engage. The Bill's Schedule sets out eleven sector tables, each listing sub-sectors with three worker-count columns: 50 or more workers; more than 25 but fewer than 50; and more than 5 but fewer than 25.

Organisations with five or fewer workers are either unclassified or out of scope entirely in most sectors. Below five workers, the Bill does not impose registration obligations.

The three tiers

Essential provider -- the highest tier. Annual compliance returns, independent certification every three years, full assurance framework, subject to inspection and assessment notices, financial penalties up to £2 million or 2% of global turnover.

Important provider -- the middle tier. Compliance returns every three years, assurance framework, inspection powers apply, penalties up to £1 million or 2% of global turnover.

Unclassified provider -- the lowest tier. Must comply with minimum resilience and cybersecurity standards set by regulation. Must have regard to responsible authority guidance. Non-compliance with guidance alone does not create direct legal liability, but failure to meet minimum standards does.

Key sectors for professional services firms and their suppliers

The sector most immediately relevant to Manx law firms, financial services organisations, and their IT suppliers is Table 1: Communications and Digital Services. The following sub-sector classifications apply:

Sub-sector	50+ workers	25--49 workers	5--24 workers
Managed Services	Essential	Important	Unclassified
Managed Security Services	Essential	Important	Unclassified
IT Support Services*	Essential	Important	Unclassified
DNS Providers	Essential	Essential	Essential
Domain Name Registration	Important	Important	Important
Cloud Service Providers	Essential	Important	Unclassified

** IT Support Services is explicitly defined in the Schedule as: technical support and maintenance for ICT systems and infrastructure of Essential or Important Entities -- i.e. supply chain. This definition means that an IT MSP or managed security provider supporting a regulated firm is potentially a registered provider in its own right.*

Other sectors relevant to professional services clients

Financial services -- commercial banks, investment banks: Essential (50+), Important (25-49), Unclassified (5-24). Regulated by IOMFSA as the responsible authority rather than CURA.

Health -- healthcare providers, medical equipment manufacturers, pharmaceutical companies, public health agencies: Essential (50+), Important (25-49), Unclassified (5-24).

Public administration -- all central government departments responsible for public administration under the Government Departments Act 1989: Essential at all sizes with no worker threshold escape.

Five-worker floor: sub-5-worker organisations drop out of most sectors entirely. However, the type of work -- not just the headcount -- determines exposure. A sole practitioner cybersecurity consultant is unlikely to be a registered provider. A 10-person IT managed services firm supporting regulated clients almost certainly is.

3. What Must I Do If I Am In Scope?

Registration

Registration is mandatory for any organisation the Schedule classifies as essential, important, or unclassified. It is not voluntary. Registration conditions -- what information must be provided, in what form, and on what timescale -- will be set by regulation under section 10. Those regulations do not yet exist. When they are published, they will be subject to consultation.

Risk management duty (section 26)

Every registered provider must take appropriate and proportionate technical, operational, and organisational measures to manage risks to the critical national infrastructure and to prevent or minimise the impact of security incidents on service recipients.

The measures must include at minimum:

- Risk analysis
- Incident handling
- Business continuity planning
- Supply chain security -- including assessment of the vulnerabilities of each direct supplier, with identified risks recorded in a risk register
- Human resources security, access control policies, and asset management

The supply chain security requirement is explicit and auditable. Registered providers must be able to demonstrate they have assessed their suppliers, not merely that they have contracts in place.

Security measures duty (section 27)

The Department may specify particular measures in writing that one or more providers must take -- identifying, reducing, or preparing for security incidents. This is the mechanism for issuing sector-specific requirements without primary legislation. Measures can be applied to an individual provider, a group, or a category.

Assurance framework (section 23)

Essential and important providers must comply with an assurance framework set by regulation. This will cover: security and risk assessments; business continuity plans and their independent assessment; notification of changes in functions; independent certification of compliance; on-site and off-site supervision; and audit.

The assurance framework regulations have not yet been drafted. The Department has confirmed that standards will align with established frameworks including ISO 27001, ISO 27002, NIST, COBIT, and SOC2. Organisations already working towards these certifications are ahead of the curve.

Compliance returns (section 25)

Essential providers must submit annual returns setting out how they have complied with the assurance framework. In year three after registration, and every three years thereafter, the return must be certified by an independent assessor rather than a senior officer alone.

Important providers submit returns every three years rather than annually. Unclassified providers have no return obligation.

If a provider fails to submit a return, the responsible authority can commission one independently and charge the cost back to the provider.

Incident notification (sections 30-31)

Where a security incident occurs that may have a significant impact on the critical national infrastructure in which a provider operates, or on the goods, services, or facilities it provides, the provider must notify the technical authority (the IoM Cyber Security Centre):

- Initial notification: within 24 hours of becoming aware of the incident
- Interim report: within 72 hours of the incident occurring or the potential threat arising
- Final report: within one month of the incident being dealt with

Significance is assessed by reference to: the duration of disruption; the number of persons affected; the geographic area affected; and the extent to which activity is disrupted. Incident reporting is confidential to the technical authority -- onward disclosure is sanitised to prevent the source being identified.

4. The Supply Chain Obligation -- What It Means in Practice

Section 26(3)(d)-(5) creates an explicit and auditable supply chain security duty. Registered providers must:

- Take into account the vulnerabilities specific to each direct supplier
- Assess the overall quality of goods, services, and facilities provided by each direct supplier
- Record identified supply chain risks in a risk register maintained by the provider

This creates a compliance dependency that runs in both directions. A Manx law firm that is a registered provider needs something to put in that risk register against each of its IT suppliers. An entry that reads 'supplier confirmed they are secure' is not an assurance; it is a circular reference. An entry that reads 'supplier holds current Cyber Essentials certification, is ICO registered, and provided a security brief dated [date]' is an evidenced control.

For technology suppliers and IT managed services firms serving regulated clients: your clients are going to start asking you for evidence of your security posture. Getting ahead of those requests -- with a structured brief, a current certification, and a documented control set -- is both a compliance contribution to your clients and a commercial differentiator for you.

The supply chain duty does not require registered providers to audit their suppliers comprehensively. It requires them to assess vulnerabilities and record risks. A supplier that makes that assessment straightforward -- by presenting clear, current evidence of its controls -- reduces compliance burden for its clients and strengthens the relationship.

5. What Standards Should I Be Aligning To Now?

The Department confirmed in its January 2026 consultation response that cybersecurity standards under the NISB will align with established international frameworks rather than creating IoM-specific requirements. The frameworks cited explicitly were: ISO 27001, ISO 27002, NIST Cybersecurity Framework, COBIT, and SOC2.

For most IoM professional services firms and their IT suppliers, the practical entry point is Cyber Essentials -- the UK government-backed certification covering the five foundational technical controls: boundary firewalls and internet gateways; secure configuration; access control; malware protection; and patch management.

Cyber Essentials is not equivalent to ISO 27001, which is a full information security management system. However, it addresses the controls most commonly exploited in commodity attacks, and holding a current certification demonstrates a baseline assurance posture that will be directly relevant to supply chain risk assessments under the NISB.

Beyond Cyber Essentials, organisations should be considering:

- A documented risk register -- the NISB explicitly requires one; building it now means it exists when the regulation requires it
- An incident response procedure -- documented, tested, and owned by a named individual
- A business continuity plan -- required under the assurance framework; a simple, tested plan is better than an elaborate one that lives in a drawer
- A data protection framework -- GDPR compliance under the IoM's Data Protection Act 2018 is a parallel obligation; the two regimes share common ground in risk assessment and incident response

6. Penalties for Non-Compliance

The NISB creates a tiered penalty regime. Civil penalties are imposed by the responsible authority (IOMFSA for financial services; CURA for everything else). Criminal liability runs alongside, with officers of corporate bodies personally liable where they authorised, permitted, or failed to take reasonable steps to prevent a contravention.

Provider tier	Maximum civil penalty	Daily cap (continuing breach)
Essential provider	Greater of £2M or 2% global turnover	Included within maximum
Important provider	Greater of £1M or 2% global turnover	Included within maximum
Unclassified provider	Greater of £500k or 1% global turnover	Included within maximum
DVN/DVD contravention (any tier)	Up to 10% relevant turnover	£100,000 per day

These are maximum penalties. The responsible authority must apply a proportionality test considering: the duration of the contravention; steps taken to mitigate; the degree of cooperation; and what is appropriate and proportionate. Appeals lie to the Infrastructure Security Tribunal, with a further right of appeal to the High Court on a point of law.

Criminal penalties for contraventions of core duties (sections 22, 25, 26, 28-31, 39, 68, 70) are: on summary conviction, a fine up to five times level 5 on the standard scale or up to six months custody; on conviction on information, an unlimited fine or up to two years custody.

Officer liability under section 82 applies to directors, secretaries, partners, and anyone purporting to act in those capacities. The registered agent of an Isle of Man company is specifically included. This is not a theoretical risk -- it is a direct personal exposure for the individuals running regulated entities.

7. Worked Example -- A 30-Person Law Firm

Scenario: Cormorant Legal Limited is a Douglas-based law firm with 30 fee earners and support staff. It uses a local IT managed services provider, DataPath IOM Limited, which has 12 employees and provides IT support, managed security monitoring, and cloud backup services. Cormorant's client data is stored partly on a Microsoft 365 tenancy and partly on a local NAS backed up offsite.

Is Cormorant Legal in scope?

Cormorant Legal is not in the Financial Services sector -- it is a professional services firm. It does not obviously fall within Table 1 (Communications and Digital Services) as a provider. Whether it falls within another sector depends on whether it provides goods, services, or facilities to critical national infrastructure -- if it acts as legal advisers to regulated entities, it may be a vendor under section 5, but not a registered provider in its own right.

On a plain reading: Cormorant Legal is probably not a registered provider. However, it is a direct client of DataPath IOM, which is almost certainly in scope.

Is DataPath IOM in scope?

DataPath IOM has 12 employees and provides IT support and managed security services to professional services firms. Table 1 classifies IT Support Services (defined as supply chain to Essential or Important

entities) as Unclassified at 5-24 workers. It classifies Managed Security Services as Unclassified at 5-24 workers. DataPath IOM falls into the Unclassified tier.

As an unclassified registered provider, DataPath IOM must: register with the responsible authority; comply with minimum resilience and cybersecurity standards set by regulation; and have regard to responsible authority guidance.

What does this mean for Cormorant Legal?

Although Cormorant Legal is not itself a registered provider, its IT supplier is. If Cormorant Legal's clients include entities that are registered providers -- financial services firms, healthcare organisations, public bodies -- those clients may need to assess Cormorant Legal as part of their own supply chain security duty under section 26. Cormorant Legal's own IT infrastructure becomes part of its clients' risk register.

The practical question for Cormorant's managing partner: can we demonstrate to our regulated clients that our IT infrastructure is appropriately secured? If DataPath IOM holds Cyber Essentials certification and can provide a current security brief, that evidence flows up the supply chain. If they cannot, Cormorant Legal's clients have a gap in their own compliance documentation.

What should Cormorant Legal do now?

- Ask DataPath IOM for their current Cyber Essentials certificate and a security brief
- Review Microsoft 365 configuration against Cyber Essentials controls -- particularly access control, patching, and malware protection
- Ensure the firm has a documented incident response procedure and knows the NISB's 24-hour notification timeline
- Begin building a supplier risk register -- even a simple spreadsheet listing suppliers, their services, and their assurance evidence is a defensible starting point
- Watch for the NISB's First Reading and the subsequent secondary legislation consultations -- these will set the operative standards

8. Timeline and Next Steps

The NISB is not yet enacted. No obligations are currently in force. The following is the expected legislative timeline based on information available as at April 2026:

- December 2025 -- January 2026: Public consultation on draft Bill
- January 2026: Consultation response published; Department confirms Bill will proceed with definitional amendments
- Later 2026 (expected): First Reading in House of Keys
- Date TBC: Bill passes through Tynwald, receives Royal Assent
- Date TBC: Commencement order issued by Department of Home Affairs (section 2 -- no date currently set)
- Date TBC: Registration conditions regulations published and consulted upon
- Date TBC: Assurance framework regulations published and consulted upon
- Date TBC: Resilience and cybersecurity standards regulations published and consulted upon

The gap between Royal Assent and commencement, and between commencement and operative secondary legislation, could be substantial. However, organisations that have aligned their controls to ISO 27001, NIST, or Cyber Essentials frameworks before the standards are set will be in a structurally better position when the detail arrives.

What to do now: (1) Establish whether your organisation falls within the Schedule. (2) If in scope, begin building the risk register and assurance documentation the Bill will require. (3) Engage with secondary legislation consultations when they are published -- these will determine what compliance actually looks like in practice. (4) Ensure your IT suppliers can evidence their security posture.

9. How The Haunted Lighthouse Limited Can Help

The Haunted Lighthouse Limited is an Isle of Man registered consultancy (Company No. 138512C) specialising in data protection, cybersecurity, and sovereign infrastructure. We hold current Cyber Essentials certification and are registered with the ICO.

We work with IoM professional services firms and their technology suppliers to build defensible, auditable compliance infrastructure. Our approach is direct and practical -- we produce documentation you can use, not reports that sit on a shelf.

NISB Readiness Assessment

A structured half-day review covering: in-scope determination; current control gap analysis against Cyber Essentials and ISO 27001 baseline; supplier risk register framework; incident response procedure review. Produces a written report you can present to clients, auditors, or the responsible authority.

Cyber Essentials Readiness

We know the Cyber Essentials assessment process from the inside. We can review your current controls, identify gaps, and prepare you for certification -- which is the baseline assurance evidence your clients will increasingly require under the NISB supply chain duty.

Supplier Security Brief

A branded, current security brief documenting your controls, certifications, and data handling practices -- the document your clients need for their supply chain risk register. Updated annually. Reduces the compliance burden on your clients and differentiates you from suppliers who cannot provide equivalent evidence.

Ongoing monitoring

We track NISB secondary legislation consultations and publish plain-English analysis via the Sovereign Auditor newsletter at sovereignauditor.substack.com. Subscribe to stay ahead of developments.

To discuss any of the above, contact us at:

alan@haunted.lighthouse.co.im

haunted.lighthouse.co.im/consultancy

Primary sources

National Infrastructure Security Bill 202x, V05 (draft). Isle of Man Department of Home Affairs.

NISB Consultation Response, January 2026. Isle of Man Department of Home Affairs. consult.gov.im/home-affairs/national-security-infrastructure-bill-nisb/

Cyber Security Centre for the Isle of Man. csc.gov.im/national-infrastructure-security-bill-nisb/

UK Telecoms Security Act 2021 (reference for DVN/DVD provisions). legislation.gov.uk

This guide was prepared in April 2026. It reflects the Bill as published in draft (V05) and the consultation response published January 2026. It does not constitute legal advice.