Threshold
Supporting Ireland's Renters

REQUEST FOR TENDER

Virtual Chief Information Security Officer (vCISO) Services

Document Type	Request for Tender (RFT)
Service Area	Virtual Chief Information Security Officer (vCISO) Services
Version	1.0 For publication
Date	July 2026
Contracting Authority	**Threshold**
Submission Deadline	**5.30pm on Friday, August 7th 2026**

1. Background and Context

The contracting organisation is an Irish registered charity operating in the rental housing / renters' rights and homelessness prevention sector with approximately 80 staff across 5 locations. The organisation handles personal data of a sensitive nature in connection with the delivery of its services and is subject to the General Data Protection Regulation (GDPR) and the Irish Data Protection Act 2018.

The organisation does not currently employ a dedicated cybersecurity function. It is seeking to appoint an experienced provider to deliver virtual Chief Information Security Officer (vCISO) services on an ongoing, structured basis to provide senior cybersecurity leadership, governance oversight, and regulatory compliance support proportionate to the size and risk profile of the organisation.

2. Scope of Services Required

Tenderers are invited to submit proposals for the delivery of the following services:

2.1 Strategic Leadership

The appointed provider shall define and maintain a cybersecurity strategy and roadmap appropriate to the organisation's size, sector, and risk profile. This shall include translating cyber risk into business risk in terms suitable for presentation to the Board and senior leadership and establishing security as a governed organisational function with measurable objectives and progress indicators.

2.2 Governance, Risk, and Compliance

The appointed provider shall establish, maintain, and continuously improve a structured governance, risk, and compliance (GRC) programme aligned to the organisation's regulatory obligations and risk profile. This shall include as a minimum:

- Development and maintenance of a live information security risk register, reviewed on a defined and regular cycle;
- Establishment and ongoing tracking of a security maturity model with measurable progression milestones;
- Definition of roles and responsibilities across the organisation's cybersecurity programme, including documented ownership and accountability structures;
- Development, maintenance, and periodic review of security policies, standards, and procedures appropriate to the organisation;
- A governed action and remediation log tracking all identified risks, controls, and improvement activities, with clear ownership and target dates;
- Assurance reporting that provides the organisation's leadership and board with timely, accurate visibility of security posture and compliance status.

The provider shall drive alignment with applicable cybersecurity frameworks and regulatory requirements. These shall include at a minimum GDPR, Cyber Essentials (or equivalent), and ISO/IEC 27001. Tenderers should confirm in their submission which additional frameworks they are qualified to advise upon, including but not limited to NIS2, NIST CSF 2.0, DORA, and ISO 9001.

2.3 Operational Oversight

The appointed provider shall chair regular security review meetings and maintain active oversight of cybersecurity activity across the organisation on a month-to-month basis. This shall include attending relevant internal meetings where cybersecurity matters are discussed, tracking agreed actions to closure, and reporting progress to senior leadership on a regular cycle.

The role of vCISO in overseeing Threshold cyber environment will have regard to the following:

1. Threshold sets policies (with vCISO actively supporting the definition of those policies)
2. Party (to be determined) implements the technical elements of those policies (e.g. patching, SIEM) and demonstrates to the vCISO that they have done the work satisfactorily
3. vCISO oversees this work to ensure it fully meets policies – or if not then exceptions are captured and risk assessed – plus assesses compliance with policies that are not directly related to the party managing the infrastructure (e.g. policy of least privilege, password rotation, phishing tests etc.)
4. vCISO keeps COO abreast of all of the above activity and seeks input and decisions as required
5. Board report reflecting all of the above is produced on the agreed frequency

2.4 Incident Readiness and Response

The appointed provider shall ensure the organisation maintains a tested incident response capability appropriate to its risk profile. This shall include:

- Development and maintenance of incident response playbooks covering the organisation's primary threat scenarios;
- Participation in tabletop or desktop exercises with the organisation's leadership team on a regular basis;
- Availability of qualified support if a real security incident occurs, including the ability to translate technical events into business decisions;
- Support with any notification or reporting obligations arising under GDPR, the Irish Data Protection Act, or other applicable legislation.

2.5 Third-Party and Supplier Risk

The appointed provider shall maintain an independent oversight function in respect of the organisation's critical IT and service suppliers. Where the appointed provider is itself a supplier of other services to the organisation, tenderers must demonstrate how conflicts of interest will be explicitly identified and managed, and how the vCISO function will retain independence in its assessment of other suppliers.

2.6 Reporting

The appointed provider shall produce reports tailored to the needs of the organisation's leadership, executives, and Board as required. All reports shall be written in plain, non-technical language, suitable for a non-specialist audience, and shall be ready to present without amendment by the organisation.

3. Service Delivery Model

Tenderers shall describe their proposed service delivery model, including:

- The proposed engagement model (e.g. retained days per month, or other) and how this will be structured to meet the organisation's needs;
- How the service will be tailored to the organisation's specific context, sector, and current security maturity, rather than delivered as a standardised offering;
- The qualifications and experience of the individual(s) who will be named and responsible for day-to-day delivery;
- How the provider will operate as an active, named participant in the organisation's governance structure, rather than in an advisory-only capacity;
- Availability and escalation arrangements in the event of a security incident outside of regular scheduled engagement days.

4. Minimum Requirements

Tenderers must demonstrate the following minimum requirements to be considered for evaluation. Failure to meet any of these criteria will result in disqualification from the competition:

- **Cybersecurity leadership experience:** Demonstrable experience delivering vCISO, interim CISO, or equivalent senior cybersecurity leadership services to organisations of comparable size, sector, or complexity.
- **Data protection knowledge:** Demonstrated working knowledge of GDPR and Irish data protection law, including obligations relevant to data controllers handling sensitive personal data.
- **Cyber Essentials / baseline compliance:** Demonstrated experience supporting organisations in achieving or maintaining Cyber Essentials certification, or an equivalent recognised baseline security standard.
- **Information security frameworks:** Demonstrated experience aligning organisations to ISO/IEC 27001 or an equivalent recognised information security management framework.
- **Professional indemnity insurance:** Current professional indemnity insurance of not less than €1,500,000 and public liability insurance of not less than €13,500,000. Tenderers must provide valid certificates of insurance with their submission.
- **Data protection compliance:** A formal Data Processing Agreement or equivalent contractual data protection provisions must be available for inclusion in the contract prior to commencement.

5. Desirable Criteria

The following are considered desirable but are not mandatory requirements. Tenderers are invited to address any or all of these in their submission:

- The provider organisation holds current certification to ISO 27001:2022 or ISO 9001:2015 in its own right;
- Demonstrable experience working with Irish charities, not-for-profit organisations, or public benefit entities;
- Experience advising on NIS2 obligations or equivalent EU cybersecurity regulatory compliance;

- Familiarity with the Data Protection Commission of Ireland's guidance, enforcement approach, and audit methodology;
- Availability to deliver staff security awareness sessions as part of or alongside the engagement.

6. Evaluation Criteria

Submissions that satisfy all minimum requirements set out in Section 4 will be evaluated against the following criteria. Tenderers are advised to structure their submission to address each criterion directly.

Evaluation Criterion	Weighting
Technical capability and proposed methodology	**20%**
Relevant experience and qualifications of named personnel	**25%**
Proposed service model and engagement structure	**25%**
Value for money	**20%**
References from comparable engagements	**10%**
Total	**100%**

7. Submission Requirements

Tenderers shall include the following in their submission. Incomplete submissions may be excluded from evaluation:

- A written technical proposal addressing each element of Sections 2 and 3 of this document;
- Evidence of compliance with all minimum requirements set out in Section 4;
- Curriculum vitae or professional profiles of all named personnel who will deliver the service;
- A commercial proposal setting out day rates or engagement costs, **fully inclusive of VAT**, the proposed engagement model, and all relevant commercial terms;
- A minimum of two reference contacts from comparable engagements, available to be contacted by the contracting authority;
- Copies of current professional indemnity and public liability insurance certificates;
- A draft or template Data Processing Agreement for review.

8. Contract Terms

The initial contract term will be for 12 months duration from the date of commencement.

The contracting organisation reserves the right to extend the contract for up to two further periods of 12 months each, subject to satisfactory performance.

The contract may be terminated by either party with [

30 days written notice period.

The appointed provider will be required to execute the contracting organisation's standard terms and conditions, including a Data Processing Agreement, prior to commencement of services.

9. Clarifications and Contact

All queries relating to this Request for Tender must be submitted in writing to:

Cormac Lally, Chief Operating Officer at cormac.lally@threshold.ie
All queries must be submitted via the designated contact only. Tenderers must not contact any other staff member of the contracting organisation in connection with this competition.

Queries must be received no later than 5.30pm on Wednesday July 29th. Responses to all queries received will be issued to all tenderers simultaneously in the interests of equal treatment.

Canvassing of any officer, employee, or agent of the contracting organisation in connection with this competition will result in automatic disqualification.