An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC NCC-IE Cyber Security Improvement Grant

Financial Support to SMEs

Terms of Reference

V1.3 Jun 2025

ncsc.gov.ie

NCC
NATIONAL CYBERSECURITY COORDINATION AND DEVELOPMENT CENTRE
IRELAND

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Table of Contents

Cyber Security Improvement Grant

Purpose of this Document

The purpose of this document is to outline the terms of reference for the NCSC NCC-IE Cyber Security Improvement Grant. This document outlines the background to the grant, the eligibility criteria, application, assessment and award processes and ongoing monitoring of the grant projects.

This document provides all the relevant information on the scheme for potential grant applicants. It also outlines the requirements which must be considered before applying.

This document is not a legally binding agreement. However, it aims to set out, in clear language, guidelines for participants in the grant scheme, to ensure fairness, transparency and equal opportunity.

1. Introduction

1.1 The National Cyber Security Strategy

The vision behind the 2019 National Cyber Security Strategy is to allow Ireland to continue to safely enjoy the benefits of the digital revolution and to play a full part in shaping the future of the Internet. In May 2023 the NCSC published the Mid-Term Review of the National Cyber Security Strategy. In it, existing and new measures are set out over 8 strategic pillars:

1. National Capacity Development
2. Critical National Infrastructure Protection
3. Public Sector Data and Networks
4. Skills
5. **Enterprise Development**
6. Engagement
7. Citizens
8. Governance Framework and Responsibilities

Recognising that the digitisation of our industry has increased exponentially, and with it increased cybersecurity risk, existing and new **Enterprise Development measures** focus on the need for a whole-of-Government approach to supporting cyber security enterprises, and the need to support SMEs to make themselves sufficiently secure from cyber risk.

In 2023 the NCSC successfully secured EU funding through the Digital Europe Programme (DIGITAL) for the development and implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE), including a €2m provision for grants for SMEs to improve cybersecurity resilience.

1.2 NCC-IE Project

The NCC-IE grant agreement sets out an Action Plan delivered over five work packages:

1. Project Management and Coordination,
2. Functioning NCC,
3. Community Development,
4. IT Collaboration Platform, and
5. Financial Support Programme (grant scheme).

The project is intended to realise, at a practical level, the tasks of the NCC-IE assigned to the NCSC and as set out in EU law (Article 7 of Regulation 2021/887).

1.3 The Financial Support Programme (FSTP)

The purpose of the Financial Support Programme (FSTP) is to increase cybersecurity of Irish small and medium-sized enterprises, by making businesses aware of cybersecurity as a business risk and raising cybersecurity maturity levels. The grant scheme will align with the upcoming National Cybersecurity Scheme, incorporating the security requirements for NIS2 compliance as well as a more basic level for SMEs.

This grant support will enable Irish small and medium-sized enterprises to know and understand the level of cybersecurity of their IT systems with the help of an external advisor and to plan the necessary improvements to protect themselves against cyberattacks and the risks they bring to their business operations.

The NCSC has partnered with Enterprise Ireland to develop a **2-phased Cyber Security Review and Improve Grant Scheme for SMEs**.

Phase 1, **Cyber Security Review Grant,** is led by Enterprise Ireland, offering SMEs access to cyber security experts who will conduct an independent review of the company's cyber security status, identify vulnerabilities, and develop a clear roadmap to enhance security measures. Eligible companies can avail of 80% funding for a €3,000 security review. The assessment will involve on-site and remote assessments, staff interviews and reviews of business policies. A report will be produced which rates the company's current level of cybersecurity, recommends actions needed to increase the level of cybersecurity including technical, physical and organisational safeguards, ranks the actions in priority based on risks to the business, and provides a time and cost estimate of the remediations.

Phase 2, **Cyber Security Improvement Grant,** is led by the NCSC, offering 80% of the cost of implementing recommended actions from the remediation plan for a maximum grant of up to €60,000

per project. Companies who have already availed of the Enterprise Ireland grant can apply for the NCSC grant with the following supporting documents:

1) Enterprise Ireland Cyber Security Review Grant Letter of Offer,
2) The Enterprise Ireland Cyber Security Report,
3) a Statement of Work, and
4) Quote(s) from service providers for the goods or services to be procured for the project or evidence of an open tender process on eTenders.

Upon completion of the work the company will undertake another security review to demonstrate the impact of the project, with the ambition to **raise the cybersecurity maturity of 100% of NCC-IE grant recipients.**

In designing and developing the 2-phased scheme, both the NCSC and Enterprise Ireland have undertaken industry research, engaging with Munster Technological University to take insights from their research on SME cybersecurity needs, and with Cyber Ireland who conducted a successful cybersecurity maturity assessment pilot with their Business Growth Committee. Feedback has also been provided by multiple cybersecurity service providers in Ireland who have aided in the design of the grant scheme, ensuring it is attractive and accessible to SMEs and to cybersecurity solution providers.

1.4 Digital Europe Programme (DEP)

The Cyber Security Improvement Grant scheme is part-financed by the Digital Europe Programme (DEP) and part-financed through State funds (50%). The DEP funding has been awarded to the NCSC, on behalf of the Department of the Environment, Climate and Communications under project 101127902 – NCC-IE, under the Call/topic DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION. The project start date is 2 October 2023 and end date is 1 October 2025.

1.5 Grant opening and closing dates

This grant scheme opened on 8 October 2024. The current call for applications opens on 13 June 2025 and the deadline for submitting completed applications is **MIDDAY 31 July 2025**. Please note that Round 3 Projects financed under the Cyber Security Improvement Grant scheme must be implemented and claimed by 31 October 2025.

1.6 Grant Budget

The maximum budget allocated to the grant scheme is €2,000,000.

The NCSC will reimburse 80% of costs, exclusive of VAT, associated with implementing actions to improve cyber security of the company, according to the recommendations of the Cyber Security Review.

The minimum funding available to any one company/project is €20,000. Therefore, the minimum project cost is €25,000, ex. VAT.

The maximum funding available to any one company/project is €60,000 or 80% of the project cost, ex. V AT, whichever is the lesser.

The grant shall not cover VAT. Please ensure to specify ex./incl. of VAT for all costs provided in the application or in any other submissions to the NCC-IE.

1.7 Implementation

Round 3 projects financed under the Cyber Security Improvement Grant scheme must be implemented and claimed by **31 October 2025**. By this date, beneficiaries must ensure that:

- The investments have been procured, delivered and are fully operational as per the eligibility criteria and terms and conditions of the grant agreement,
- All relevant licences are in place.
- All reimbursement requests and documentation are submitted.

The project must be completed within a valid timeframe i.e. the end date can be no later than 31 October 2025 and the start date can be no earlier than the commencement date of the Grant Agreement (Sec. 3.7).

1.8 Regulatory Framework

Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union.

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R1046&qid=1535046024012

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme. This Regulation lays down a financial envelope for the Digital Europe Programme (the 'Programme') for the period 2021-2027.

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32021R0694

Aid will be awarded in accordance with the relevant terms and conditions of Commission Regulation (EU) 2023/2831 of 13 December 2023 on the application of Articles 107 and 108 of the Treaty on the Functioning of the European Union to de minimis aid.

The NCC-IE project is also administered in line with the Public Financial Procedures, the Public Spending Code and Circular 13/2014 - Management of and Accountability for Grants from Exchequer Funds.

https://www.gov.ie/en/collection/35923-public-financial-procedures-booklet/

https://www.gov.ie/en/publication/public-spending-code/?lang=en

https://www.gov.ie/pdf/?file=https://assets.gov.ie/207159/a813079b-8c9d-4b7a-9403-41e58d7b629c.pdf#page=null

A private entity which is subsidised 50% or more by a public body, when awarding contracts for goods, services or works is deemed to be a Contracting Authority. A Contracting Authority is responsible for ensuring that it is compliant with public procurement regulations SI 284 2016 and Government Policy as set out in Circular 05/2023.

https://www.irishstatutebook.ie/eli/2016/si/284

https://www.gov.ie/en/circular/36e3f-initiatives-to-assist-smes-in-public-procurement/

It is a grantee's obligation to ensure that the placement of all contacts for goods and services necessitated by the Project complies with Public Procurement Guidelines. A grant receiving body in receipt of public funding should be aware of the Statement of Principles for Grantees that is available at the following URL:

https://www.gov.ie/en/circular/10b42-circular-132014-management-of-and-accountability-for-grants-from-exchequer-funds/.

1.9 Public Procurement

The Public Procurement thresholds for goods and services are as follows:

Value (Ex. VAT)	Competitive Procedure
< €5,000	Written / verbal quotes (3 recommended but minimum of 1).
≥€5,000 < €50,000	1. Written quotes (minimum of 3) or 2. Can be advertised on eTenders as part of a more formal tendering process Note: Post contract, Contract Award information must be published on eTenders for all contracts over €25,000
≥ €50,000 < €143,000	National tender advertised on eTenders via RFT
≥ €143,000	EU tender advertised on eTenders & OJEU via RFT

Contracts for goods and/or services with an estimated value between €5,000 and €50,000 (exclusive of VAT) can be awarded on the basis of responses to written specifications (for example – issued via email) to at least three suppliers or service providers. The steps for below threshold procurement are outlined on pages 28 and 29 of the Public Procurement Guidelines for Goods and Services:

https://www.gov.ie/en/publication/c23f5-public-procurement-guidelines-for-goods-and-services/

If there is any significant deviation from the tendering guidelines, a written explanation for the deviation must be provided as part of the application.

Quotes must be comparable, and the specification and requirements used to obtain the quotes must be related to the recommended actions specified in Part 3 of the Enterprise Ireland Cyber Security Report and the tasks and deliverables specified in the Statement of Work. Please see Appendix B for an example of text that can be used for describing the Specification and Requirements when seeking quotes.

Quotes should be evaluated objectively against specified requirements, using a scoring sheet, and the suitable offer should be selected on the basis of this evaluation.

Where the total project cost is ≥ €50,000 a national tender must be advertised on eTenders via Request for Tender (RFT). eTenders is the national tendering website and can be accessed at the following URL:

https://www.etenders.gov.ie/Tenders should be evaluated using weighted criteria sheet and the highest scoring tender should be selected.

Applicants can seek support on public procurement and eTenders by contacting the Office of Government Procurement at support@ogp.gov.ie.

Important Note on Project Costs

Where project costs are close to the €50,000 threshold, applicants should consider running an open tender process on eTenders. If there is a cost overrun and the total project cost is greater than or equal to €50,000 and the goods and services of the project have not been procured by an open tender process on

eTenders, the project would be deemed to be incompliant with procurement rules and in breach of the terms of the Grant Agreement, and, as a consequence, claims would not be paid.

Contract Award Information

Contracting authorities are required to publish contract award information for all procurements over €25,000 (exclusive of VAT) on the eTenders website on completion of the award irrespective of whether the procurement was advertised on eTenders.

2. Description of the Grant

2.1 Eligible grant recipients

Eligible companies are client companies of Enterprise Ireland with an assigned Development Advisor that are SMEs, Irish registered, Irish/EU owned and controlled, in good financial standing, and have no history of failing to adhere to the terms and conditions of an Enterprise Ireland grant.

To qualify as an SME the staff headcount must be less that 250 and either the turnover must be less than or equal to €50 million or the balance sheet must be less than or equal to €43 million. More information on the definition of an SME can be found at the following URL:

https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en

In line with Commission Regulation (EU) 2023/2831 of 13 December 2023 on the application of Articles 107 and 108 of the Treaty on the Functioning of the European Union to de minimis aid, a single undertaking may not receive more than €300,000 in de minimis aid from any public funding (EU Funds and/or any other national funds) over a rolling period of three years. Therefore, applicants must submit an updated de minimis declaration on de minimis aid, in line with Commission Regulation (EU) 2023/2831.

2.2 Eligible actions and costs

The types of actions which may be undertaken as part of this grant are:

- Procurement of software/licences
- Provision of consultancy/advisory services
- Training of staff

Any direct costs associated with these actions will be eligible for funding.

Applicants must follow public procurement rules when engaging the services of a provider, obtaining 3 written quotes for services up to €50,000, or running an open tender process for services that are greater than or equal to €50,000.

Only costs agreed as part of the grant agreement, and incurred during the project period, are eligible.

The grant shall not cover VAT. Please ensure to specify ex./incl. of VAT for all costs specified in the application or in any other submissions to the NCC-IE.

All Round 3 Projects must be completed within a valid timeframe i.e. the end date can be no later than 31 October 2025 and the start date can be no earlier than the commencement date of the Grant Agreement (Sec. 3.7).

2.3 Eligible service providers

Grant applicants may choose to engage the services of one cyber security service provider to project manage and implement all the actions of the improvement plan, including procuring, software and training.

Alternatively, a cyber security service provider may assist the company to plan their improvement actions and tasks, while the company manages the procurement of other services themselves.

The company may use the same cyber security service provider who conducted their Cyber Security Review to carry out the improvement plan.

There is no published list of approved service providers related to this offer. It is the responsibility of the client company to identify and engage a suitable service provider for the project. Applicants must follow public procurement rules when selecting a provider and must ensure that the provider has the appropriate expertise, capability, and certification.Service providers engaged for this grant support may not be employees of, nor shareholders of, nor have a direct financial interest in the company, or contractual relationship with the company as their IT technology or services provider.

As part of the application assessment process, the NCSC may deem the proposed service provider unsuitable based on these or any other criteria that may arise and will engage with the applicant to discuss other options or deem the project ineligible. Please note that this is to ensure the efficient operation of the grant and does not guarantee the quality of the specific service provider chosen.

2.4 Required Outcomes

The company shall implement recommended actions from the Cyber Security Review and shall receive a report from the service provider(s) confirming the actions undertaken, follow-on steps to undertake and recommendations for ongoing cyber security.

A second Cyber Security Review shall be undertaken and compared with the original review. This review shall be mandatory for each Cyber Security Improvement Grant application and must be included in the project costs. The second Cyber Security Report should be consistent with the first Enterprise Ireland Cyber Security Report and produce a valid Cyber Risk Score that is comparable with the Cyber Risk Score of the Enterprise Ireland Cyber Security Report.

The expected outcome for each company using the NCC-IE Cyber Security Improvement Grant is a demonstrated increase in cybersecurity, and a reduced risk of attack.

2.5 Limitations

Only one Cyber Security Remediation Grant shall be approved per company or project

3. Application and Assessment Process

3.1 Application Form

The application form is available at https://www.ncsc.gov.ie/ncc-ie/grants_for_SMEs/ .

The document is in MS Word format. When complete, the applicant should save the document using the company name as the filename.

This application form must be submitted as part of the application. The application form must be complete. All fields are mandatory, and all three declaration boxes must be ticked for the form to be deemed complete.

3.2 Supporting Documents

When submitting the completed application form applicants must also submit:

- Enterprise Ireland Cyber Security Review Letter of Offer,
- A copy of the Enterprise Ireland Cyber Security Report
- A Statement of Work, and
- Quote(s) from service providers for the goods or services to be procured for the project or evidence of an open tender process on eTenders

The Enterprise Ireland Cyber Security Review Letter of Offer

The Enterprise Ireland Cyber Security Review Letter of Offer must be digitally signed and included in the application.

The Enterprise Ireland Cyber Security Report

The Enterprise Ireland Cyber Security Report must specify the Cyber Risk Score and list the qualifications of the consultant who performed the review. The report must also list the recommended remediation actions provided by the consultant. Additionally, the report must include the findings of the Enterprise Ireland Cyber Security Review assessment or refer to a report that contains these findings and is included in the application. The Enterprise Ireland Cyber Security Report must be submitted as part of the application. Documents that supplement the Enterprise Ireland Cyber Security Report can be submitted, however, any document submitted as an alternative to the Enterprise Ireland Cyber Security Report will not be accepted.

The Statement of Work

A Statement of Work (SoW) is a document that sets out the scope of work to be carried out and the sequence of tasks to be completed.

The Statement of Work should define the scope of the project and identify the project tasks and deliverables. Appendix C contains an example Statement of Work that can be used for guidance.

The following is a list of headings that can be used in the Statement of Work:

- Background
- Goals/Objectives/Purpose
- Scope
- Tasks/Requirements (including task definitions and IDs, project milestones/completion dates)
- Deliverables (including a statement covering what must be delivered, when it must be delivered, and where it must be delivered
- Other Unique Requirements/Additional Considerations
- Schedule
- Budget

The tasks and deliverables specified in the Statement of Work must be related to the recommended remediation actions included in the Enterprise Ireland Cyber Security Report and be aligned with the specifications used to obtain written quotes or tenders.

The Statement of Work must include, as a deliverable, the second Cyber Security Review that shall be conducted when the actions of the Cyber Security Improvement Grant have been performed (Please see Section 2.4 (Expected Outcomes)).

All Round 3 Projects must be completed within a valid timeframe i.e. the end date can be no later than 31 October 2025 and the start date can be no earlier than the commencement date of the Grant Agreement (Sec. 3.7).

Quote(s) from Service Providers / Evidence of an Open Tender Process on eTenders

All costs specified in the application or in any other submission to the NCC-IE must be expressed in Euro. The grant shall not cover VAT. All costs specified must be ex./incl. of VAT.

The specifications used to obtain written quotes or tenders must be aligned with the remediation actions included in the Enterprise Ireland Cyber Security Report and be consistent with the tasks and deliverables specified in the Statement of Work.

3.3 Submission email

Completed application forms and supporting documents should be sent as attachments by email to ncc-ncsc@ncsc.gov.ie.

3.4 Assessment criteria

An acknowledgement will be issued by email to confirm received applications. Failure to submit all required information will result in the application being deemed incomplete and not progressing to assessment.

All applications and supporting documents must be received by **MIDDAY 31 July 2025.**

Where applicable, ranking criteria will be applied as follows:

Size of company	Small <50 = 5 points Med > 50 = 10 points
Cyber security risk rating	1 to 10 – 1 being extreme risk, 10 being an exemplar of best practice.

3.5 Assessment process

Gate 1: Complete applications will be queued for review.

Gate 2: After the application deadline all complete applications will be assessed to ensure they meet the requirements as set out in the Terms of Reference and the application form.

Gate 3: Where the total value of funding applied for exceeds €2,000,000, a ranking of grant applicants will be undertaken. The ranking will ensure the companies who have the higher risk of cyber-attack, and the lowest risk of non-compliance will be prioritised for grant aid.

All eligible applications will be submitted to the evaluation committee for review and approval.

3.6 Notification of results

Unsuccessful applicants will be notified of their result and will have the opportunity to submit an appeal within 10 calendar days.

Successful applicants will be notified of their results and will be advised of the next set of steps required to finalise the grant agreement.

3.7 Grant Agreement

Successful applicants will be issued a Grant Agreement, which should be reviewed carefully before signing and returning, as it will contain full terms and conditions of the grant funding, including monitoring and auditing provisions.

4. Monitoring, Reporting and Reimbursement

4.1 NCSC Monitoring of projects

The NCSC will monitor the implementation of all projects through the company's Grant Project Manager and may request updates on progress throughout the project lifecycle. The NCSC will also maintain contact with the service providers to confirm projects are progressing as expected. The NCSC will conduct selective audits of successful projects.

It is the responsibility of the grant recipient to report any changes to the project, in terms of actions, timelines or costs, to the NCSC.

4.2 Reporting

The company must provide the NCSC will report(s) confirming the activities carried out, and the costs associated. A cyber security service provider must perform a Cyber Security Review after the actions have been undertaken, and the result of the review must be shared with the NCSC.

4.3 Reimbursement claim

Grant recipients will complete the Claim Form and submit all supporting documents to the NCSC.

All claims must be submitted by 31 October 2025.

The NCSC will review each claim and process payments in order of the claims submitted.

4.4 Publication of results

Grant recipients may be required to support the NCSC in communicating and publicising the results and impacts of the Cyber Security Improvement Grant.

All communication must acknowledge support from the European Union and the respective fund in line Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021.

Further guidance on publicity will be available in the Cyber Security Improvement Grant Implementation Guide.

5. Data Protection

Data collected and stored as part of the application process will be done so in line with the Department of the Environment, Climate and Communications' Data Privacy Statement and Data Privacy Notice.

6. Contact Details

For assistance with queries please relating to the grant please contact ncc-ncsc@ncsc.gov.ie

For assistance with queries relating to public procurement or eTenders please contact the Office of Government Procurement at support@ogp.gov.ie

Appendix A: Statement of Principles for Grantees

Clarity
 	
• Understand the purpose and conditions of the funding and the outputs required.
 	
• Apply funding only for the business purposes for which they were provided.
 	
• Apply for funding drawdown only when required for business purposes.
 	
• Seek clarification from the grantor where necessary – on use of funds, governance and accountability arrangements.
	Governance
	
	• Ensure appropriate governance arrangements are in place for:
	  ○ oversight and administration of funding.
	  ○ control and safeguarding of funds from misuse, misappropriation and fraud.
	  ○ accounting records which can provide, at any time, reliable financial information on the purpose, application and balance remaining of the public funding.
	  ○ accounting for the amount and source of the funding, its application and outputs/outcomes.

Value for Money
 	
• Be in a position to provide evidence on
  ○ effective use of funds
  ○ value achieved in the application of funds.
  ○ avoidance of waste and extravagance
	Fairness
	
	• Manage public funds with the highest degree of honesty and integrity.
	
	• Act in a manner which complies with relevant laws and obligations (e.g. tax, minimum wages)
	
	• Procure goods and services in a fair and transparent manner.
	
	• Act fairly, responsibly and openly in your dealings with your Grantor

Appendix B: Request for Quotation Example

I am writing to you on behalf of [COMPANY NAME]. We recently received a grant from Enterprise Ireland to carry out a Cyber Security Review. We received a report outlining our risks and what improvements we should implement to improve our cyber security resilience.

We would like to implement the below recommended actions and would appreciate if you could provide a quote to carry out the work.

These are the actions which have been recommended for our company to carry out which we would like to implement immediately. The work must be complete by 31 October 2025.

[*LIST OF RECOMMENDED REMEDIATION ACTIONS FROM THE CYBER SECURITY REVIEW REPORT*]

Appendix C: Statement of Work Example

Statement of Work provided by **Cyber Security Service Provider Ltd.**

Company name	*Grant Applicant Company*
Project Manager	*Project Manager*
Date	*xx.xx.xxxx*

Scope of Work:

Grant applicant company carried out a Cyber Security Review in December 2024. They received a Cyber Security Report with a risk score of 2 (with 1 being the highest risk score).
Grant applicant company wishes to implement 5 recommended actions from the Cyber Security Report, and to decrease their risk score by a minimum of 2 points, as part of the NCSC NCC-IE Cyber Security Improvement Grant.
Cyber Security Service Provider Ltd. is pleased to carry out the below services.

Task number	Description	Start	End	Duration	Resource
1	Roll out MFA	01.09.25	14.09.25	10 days	Jerry Smith
2	Software inventory	01.09.25	05.09.25	5 days	Amy Murphy
3	Network segmentation	14.09.25	30.09.25	10 days	Jerry Smith
4	Cybersecurity Awareness training	01.10.25	14.10.25	3 days	Tom Casey
5	Retest Cyber Security Review*	15.10.25	18.10.25	3 days	Jerry Smith

*Compulsory element of all SoWs.

Deliverable	Description	Format
Implementation Statement of Work	- Final Statement of Work for the implementation, including any updates or refinements to scope, estimates, assumptions, or staffing based on Inception phase learnings	- MS Word
Test Strategy Document	- Identifies the approach, roles and responsibilities and overall management of the testing effort, including Functional/Unit Testing, System Integration Testing, Performance Testing, and User Acceptance Testing	- MS Word

Deliverable	Description	Format
Project Report	- Outlines all work carried out, outcome of each task, and recommended actions for continued improvement of cyber security.	- MS Word
Cyber Security Report	- Is consistent with the Enterprise Ireland Cyber Security Review and produces a valid Cyber Risk Score that is comparable with the Cyber Risk Score of the Enterprise Ireland Cyber Security Report.	- MS Word