An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC NCC-IE Cyber Security Improvement Grant

Financial Support to SMEs

Terms of Reference

V1.1 Oct 2024

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 process and ongoing monitoring the grant projects.

This document provides all the relevant information on the scheme for potential grant applicants. It also outlines the terms and conditions which should 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) Cyber Security Report,
3) a statement of proposed works, and
4) a quote(s) from a service provider(s) to undertake the work.

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 will open on **8 October 2024** and the deadline for completed applications is **8 December 2024.**

Subject to budget, a second round of applications may be opened in January 2025.

1.6 Grant Budget

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

The NCSC will reimburse 80% of costs 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.

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

1.7 Implementation

Projects financed under the Cyber Security Improvement Grant scheme must be implemented and claimed by **30 June 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.

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. The CYBER+ALT Grant Scheme will operate within this regulatory framework.

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

2. Description of the Grant

2.1 Eligible grant recipients

Eligible companies are client companies of Enterprise Ireland with an assigned Development Advisor.

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 above this amount.

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

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 are strongly recommended to engage with up to three service providers before making a choice of a provider with 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 Expected Outcomes

The company will implement recommended actions from the Cyber Security Review and will 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 will be undertaken and compared with the original review. This review will be mandatory for each Cyber Security Improvement Grant application, and must be included in the project costs.

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.

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 Cyber Security Report
- A statement of proposed works, and
- Quote(s) from service providers for the works to be carried out as part of the project.

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

Applications received will be checked for completion and an acknowledgement will be issued by email to confirm same. If there is any information missing, the applicant will be contacted and asked to submit the missing information. 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 **8 December 2024.**

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.
Project compliance viability	Proposed end date Jan – June (1-6).

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 set out in 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 that a Letter of Offer of Grant Agreement will issue in due course.

3.7 Letter of Offer of Grant Agreement

Successful applicants will be issued a Letter of Offer of 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.

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 30 June 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 any queries please contact ncc-ncsc@ncsc.gov.ie