|  |  |
| --- | --- |
| Company Name: |  |
| Project Number: |  |
| Company Contact Name: |  |
| Contact Email Address: |  |
| Document Date: |  |

# Background and next steps

This Cyber security report is to be completed by the Cyber consultant. It will summarize their Interviews with key company personnel, investigations of current company practice, and contain a review of the technical implementation of both on-site and cloud software being used. It is supplied to EI as part of the grant claim process.

Part 1 of the document is the consultants’ credentials, and their overall score of the companies’ Cyber posture.

Part 2 is a more in-depth analysis of the Companies Cyber Security, following the headings and approach as recommended by the NCSC (National Cyber Security Centre, <https://www.ncsc.gov.ie/> )

Part 3 is an action plan. The Cyber Review grant is only a first / next step to improving Irish companies’ security posture; it will reduce the chance of an incident, and/or reduce the severity of its impact, but it can never guarantee 100% coverage. It is highly recommended the client company follows the steps agreed in this plan.

Part 4 is confidential to the company, detailing specific vulnerabilities (if any) found during the Cyber Review.

* This information should be provided to the company (and the company alone i.e. not Enterprise Ireland) after the consultant has been paid.

**Grant Payment:** Details of the Excel checklist to make to make the claim are at [www.enterprise-ireland.com/cybersecurityreview](http://www.enterprise-ireland.com/cybersecurityreview)

# Part 1 – Summary and Consultant Credentials

|  |  |  |
| --- | --- | --- |
| Consultants Opinion of Clients current Cyber Risk Score |  |  |
| * 1 to 10 – 1 being extreme risk, 10 being an exemplar of best practice. * Companies are scored keeping in mind their peers in similar sectors and of similar size but are not truly comparable between companies. * The score represents an opinion only, based on the consultant’s expertise and is intended to prompt discussion. |  |  |

|  |  |
| --- | --- |
| Consultant Name: |  |
| Consultant Company Name: |  |
| Consultant Qualifications and date achieved (1): |  |
| Consultant Email Address: |  |
| Consultant Declaration (2): | |  | | --- | | 1. I have complied with our own data protection obligations in respect of the personal data that I supply to Enterprise Ireland and that I am entitled to disclose such personal data to Enterprise Ireland; | | 1. I will ensure that a copy of Enterprise Ireland’s Data Protection Notice ([Grants Data Protection Notice | Enterprise Ireland (enterprise-ireland.com)](https://www.enterprise-ireland.com/en/legal/privacy-notice-data-protection/grants-data-protection-notice) is provided to data subjects (e.g. employees) whose personal data I provide to Enterprise Ireland as part of this application. | | 1. I understand that, information submitted as part of this grant claim will be shared by Enterprise Ireland to the NCSC (National Cyber Security Centre) on a confidential basis. | |
| Consultant Signature (3) : | *Insert name as text or copy-paste image of signature* |

(1) Noting that EI reserves the right to spot or otherwise request proof of the relevant consultant qualifications, and their equivalence the standard set by the NCSC, prior to payment.

(2) Information on how Enterprise Ireland’s processes personal data as part of funding, vestment and other supports is available at [Grants Data Protection Notice | Enterprise Ireland (enterprise-ireland.com)](https://www.enterprise-ireland.com/en/legal/privacy-notice-data-protection/grants-data-protection-notice).

(3) For the purposes of validating Electronic Signatures made on this form, the Electronic Commerce Act (2000) and subsequent amendments are deemed to apply.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

# Part 2 – Company Specific Report

The following headings have been recommended by the NCSC as a high-level format, following the detailed best practice they share with larger and public sector organisations.

* Guidelines at link <https://www.ncsc.gov.ie/guidance/> , in particular the document [Cyber Security Baseline Standards Self-Assessment Form](https://www.ncsc.gov.ie/pdfs/Cyber_Resilience_Self-Assessment_Framework_Version_1.4_Jan_23.xlsx)
* It is expected that most client reports will be “T-Shaped” – a good coverage of the headings listed below with a deep dive of between 3 and 5 areas identified as being key risks within the time supported by the grant.
* While Consultants are free to evolve the headings below, EI retains a quality control mechanism to ensure client needs are being met by consultants.

#### Software Updates

##List the activities investigated and details of good practice / items needing remedied.



#### Data Backups

##List the activities investigated and details of good practice / items needing remedied.



#### Access Management

##List the activities investigated and details of good practice / items needing remedied.



#### Antivirus

##List the activities investigated and details of good practice / items needing remedied.



#### Network Security

##List the activities investigated and details of good practice / items needing remedied.



#### Device Management

##List the activities investigated and details of good practice / items needing remedied.



#### Cloud Risk

##List the activities investigated and details of good practice / items needing remedied.



#### Data Security

##List the activities investigated and details of good practice / items needing remedied.



#### Website and Social Media Security

##List the activities investigated and details of good practice / items needing remedied.



#### Remote working

##List the activities investigated and details of good practice / items needing remedied.



#### Third Party Risk

##List the activities investigated and details of good practice / items needing remedied.



#### Cyber Awareness Training and Culture

##List the activities investigated and details of good practice / items needing remedied.



#### Cyber Incident Response and Business Continuity Planning

##List the activities investigated and details of good practice / items needing remedied.



#### Cyber Governance

# Part 3 – Company Specific Actions

Using the Headings set out above, list actions to remedy any weaknesses found.

While a small number of follow-on actions for the consultant is allowed, the focus should be on items achievable by the client’s team. E.g. Actions such as

* Applying for support under the NCSC follow on (“Cyber Remediation Grant”), more information at ncsc.gov.ie
* Use of funded third level Cyber Security courses via third level institutions and Skillnet.
* Use of specified industry resources e.g. videos on good security Hygiene from Providers such as Apple Microsoft and Google)

Actions should be written in a way that it can clearly recognized when they are complete i.e. they should be specific, measurable, achievable, realistic and timebound.

Where there is no action recommended under a specific heading, it should be clearly labelled as “no action recommended in this area”.

## Suggested format

#### Heading A (matching Headings from Part 2)

**Action 1**

* Identify the specific action to be carried out to remedy vulnerabilities.
* Owner within the client company
* Date to be achieved by.
* Priority (Low | Medium | High | Urgent)
* Estimate effort / cost to carry out action to a reasonable level.

# Part 4 – Confidential – Company Vulnerabilities

This section is to be shared in confidence with the client company only (i.e. it should **\*not\*** be sent to Enterprise Ireland).

Detail any Vulnerabilities identified during the preparation of this report, noting that a search for vulnerabilities was not the primary focus of work carried out and may require further investigate.

Format of the report to mirror headings in Part 2 and 3 or follow industry standard practice.