Funded by the European Union
NextGenerationEU

mita

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
MALTA

GOVERNMENT OF MALTA
MINISTRY FOR THE ECONOMY, ENTERPRISE AND STRATEGIC PROJECTS

Cyber Assess Scheme: Call Document

Date: 5th February 2024
Version: 1.0

Malta Information Technology Agency, Gattard House, National Road, Blata l-Bajda HMR 9010 Malta
Telephone: (+356) 21234710
Web Site: www.mita.gov.mt

Table of Contents

01. Introduction

This document provides information on the Cyber Assess Scheme and is aimed at assisting applicants in the compilation of the application form and its submission.

This Call Document may be reviewed, updated, and amended from time-to-time by the Malta National Cybersecurity Coordination Centre throughout the lifetime of the measure.

01.1 Delegation of authority

The Malta National Cybersecurity Coordination Centre ("the NCC") operates within the Malta Information Technology Agency (MITA) and is responsible for supporting cybersecurity capacity building at a national level.

The Cyber Assess Scheme project is fully funded by the Recovery and Resilience Facility fund which is part of the NextGenerationEU Programme. MITA serves as the project coordinator, empowering the NCC to perform the tasks related to coordination, management, control, and implementation of the Cyber Assess Scheme.

01.2 Scope

The Cyber Assess Scheme is designed to enhance the cybersecurity resilience of Maltese businesses by providing specialized expertise and services, emphasizing simplicity to remove barriers and make its benefits easily accessible. This initiative empowers businesses to proactively address cyber threats, strengthen local enterprises, and reduce supply chain risks. In this respect, tailored offerings include technical and business acumen for assessing IT systems and infrastructure (excluding SaaS, PaaS, SCADA, OT, and personal devices), and addressing information security threats.

A minimum of 30 Maltese entities are intended to benefit from one of the services being Vulnerability Assessments, Penetration Testing, Security Architecture Reviews, Risk Assessment, and Audit & Reviews, at no cost.

The Cyber Assess Scheme aligns with the long-term vision of enhancing the global competitiveness of Maltese businesses by establishing a reputation for robust cybersecurity practices. Furthermore, it fosters economic stability and growth by creating a secure business environment that attracts and retains investment.

01.3 Duration of the measure

The Cyber Assess Scheme is expected to remain operational until 31st July 2024, or until all services are consumed.

01.4 Budget

The allocated budget for this scheme is set at €150,000, made available through the Recovery and Resilience Facility Fund, which is part of the NextGenerationEU Programme, to provide a free of charge service to eligible enterprises.

01.5 Implementation

The scheme shall be managed on a first-come, first-served basis, subject to service availability.

To ensure business's cybersecurity needs are met with expertise, MITA is collaborating with industry leaders for the provision of the five services. In this manner, MITA will not be processing any data exchanges between the respective MITA contractor and applicant. The MITA contractor will be in direct contact with the applicant to complete the assignment. Commitment will be formalised between MITA and the applicant if the application is accepted. These services will then be delivered remotely by the contractor until Quarter 3 of 2025.

02. Service Guidelines

The Cyber Assess Scheme covers a comprehensive list of services which will all be provided in accordance with and guided by the highest cybersecurity principles, free of charge. In this manner, to ensure equitable distribution and effective utilization of resources, specific allocations have been established for each service category.

02.1 Vulnerability Assessments

Vulnerability assessments provide insight as to which assets are susceptible to cyber-attacks by providing detailed reports of the weaknesses in the systems scoped for testing. The severity of these weaknesses is measured through authenticated or unauthenticated scans as requested by the applicant. The assessments also document easily identifiable vulnerabilities, showing how they were discovered. The vulnerabilities are listed with prioritization based on CVSS scores, and recommendations for remediation are provided.

Vulnerability scanning supports IPv4, IPv6 and hybrid networks, whilst Technologies/Operating Systems supported are the following: AIX, Junos, SQL Server, Alma Linux, MacOS X, SuSE, Amazon Linux, Mandriva, Ubuntu, Android MariaDB, Virtuozzo, CentOS MongoDB, VMware ESX, CISCO, MySQL, VMware ESXi, Citrix, Netware, vSphere, DB2, NewStart CGSL Windows, Debian Oracle, F5 Networks, Oracle Linux, Fedora OracleVM, Fortinet Palo Alto, FreeBSD, PhotonOS, Gentoo, PostgreSQL, HP-UX Red Hat, Huawei, Rocky Linux, Hyper-V, iIBM iSeries, Scientific Linux, Informix/DRDA, Slackware, Apple iOS, Solaris.

For the vulnerability assessment service, between 5 and 25 devices/components can be scanned. As an alternate option, applicants can opt to have 1 web application assessed.

02.1.1 Provision of Vulnerability Assessments

Service provision will be capped to **12 businesses** with a **maximum of 4 business days each**, covering the below steps:

- Vulnerability identification

Vulnerability testing can be run via authenticated and unauthenticated scans:

Authenticated scans: Allow vulnerability scanners' system access to networked resources using remote administrative protocols and authenticate using provided system credentials. Authenticated scans should include information but not be limited to access to low-level data such as specific services, configuration details and accurate information about operating systems, installed software, configuration issues, access control, security controls and patch management.

Unauthenticated scans: Scans that do not provide system access to networked resources, which can result in false positives and unreliable information about operating systems and installed software. However, they can provide visibility into which vulnerabilities on the system/s are easily identifiable without having credentialed access to the system/s.

- Vulnerability analysis

In the vulnerability analysis stage, the following steps will be taken:

1. Identifying the responsible components and root cause of each vulnerability, with manual verification to minimize false positives.
2. Determining the age of vulnerabilities.
3. Assessing exploitability based on CVSS 3.1 format.
4. Evaluating the exploit code maturity using CVSS 3.1 format.

- Risk assessment

The applicant will be presented the Risk scores. For each vulnerability, the vulnerability ranking will include CVSS scores.

- Remediation

The applicant will be guided in terms of prioritization of vulnerabilities according to CVSS 3.1 format, accompanied by recommendations for remediation.

02.2 Penetration Testing

Penetration testing involves both manual and automated testing to replicate real-life cyber-attacks, mapping out potential breach paths that attackers might take. The primary objectives are to validate the effectiveness of existing security controls based on specified goals and scope, ensuring they adequately protect the system or assets in question. Covert testing is used to evaluate the response capabilities of IT and security personnel when faced with simulated cyber-attacks.

In cases where vulnerabilities are identified and deemed exploitable, detailed documentation is provided, illustrating the breach methods used for each vulnerability. Additionally, the service offers recommendations for remediation to prevent the recurrence of these vulnerabilities and enhance overall cybersecurity defences.

02.2.1 Provision of Penetration Testing

Service provision will be capped to **3 large businesses** with a **maximum of 8 business days each**, and **6 SMEs** with a **maximum of 6 business days each**, as follows:

Guided by *The Penetration Testing Execution Standard* and *NIST SP800-115 Technical Guide to Information Security Testing and Assessment*, the penetration testing activities to be included, but not limited to, are:

- Intelligence Gathering
- Threat Modelling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting which would align with the PTES Reporting section and the PTES Technical Guidelines – Reporting section. The report will include clear explanation on the identification and explanation of vulnerabilities, with associated recommended remedial actions, step-by-step attack replication instructions, evidence of compromise/verification with screenshots and solutions. Detailed technical reports and executive summary reports with recommendations and a remediation plan with prioritised actions for risk mitigation are also included.

02.3 Security Architecture Reviews

Security architecture reviews involve assistance and guidance in the development and design of architectures that effectively manage identified risks through appropriate controls. It includes the identification and articulation of risks at both abstract and detailed levels in systems and services design.

This service provides guidance on reducing the likelihood of exploiting vulnerabilities and minimizing the impact in case of a compromise. It offers support for secure development, building, deployment, operation, and management of systems and services. Additionally, the service advises on adopting and securely implementing common architectural blueprints or patterns. Applicants are guided in selecting technologies that adequately mitigate potential vulnerabilities identified in system architectures. Furthermore, the service simplifies technical security analysis into easily understandable language for both technical and executive audiences, facilitating better decision-making and understanding of security measures.

02.3.1 Provision of Security Architecture Reviews

Service provision will be capped to **3 businesses** with a **maximum of 10 business days each,** as follows:

Security architecture assessments align with at least one of the below Threat Modelling approaches and where technically possible with Zero Trust Architecture principles as per NIST.SP.800-207:

- Draft NIST Special Publication 800-154, Guide to Data-Centric System Threat Modelling
- STRIDE
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- IDDIL/ATC

The final report is intended to include a threat model for the systems under review, including a list of potential attack vectors and means to mitigate these. Recommendations on adopting and securely implementing common architectural best practices are also included.

02.4 Risk Assessments

The risk assessment and management service offers guidance and advice to applicants to determine the appropriate approach to risk assessment based on their specific activities and desired business outcomes. Working collaboratively, this service helps applicants gain a realistic understanding of cybersecurity risks related to their business objectives.

The service includes the conduct and documentation of the risk assessment, assisting the applicant in identifying and addressing cybersecurity risks that align with its goals. As a result, such assessments will help facilitating informed security and business decision-making processes, providing the applicant with comprehensive support in managing cybersecurity risks effectively.

Cybersecurity control recommendations are provided to ensure comprehensive management of identified risks.

Additionally, the service helps in developing and documenting tailored risk management plans that align with the applicant's business objectives and activities. Furthermore, the service assists applicants in developing adaptive approaches to continuously manage evolving risks, considering changes in the business, threat landscape, and technology.

02.4.1 Applicability of Risk Assessments

The risk assessment and management service can be conducted at all three tiers in the risk management hierarchy — including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level).

For the risk assessment service, applicants must opt for one of the 3 specified tiers.

Tier 1 includes, for example:

- organization-wide information security programs, policies, procedures, and guidance;
- the types of appropriate risk responses (i.e., risk acceptance, avoidance, mitigation, sharing, or transfer);
- investment decisions for information technologies/systems;
- procurements;
- minimum organization-wide security controls;
- conformance to enterprise/security architectures;
- monitoring strategies and ongoing authorizations of information systems and common controls.

Tier 2 includes, for example:

- enterprise architecture/security architecture design decisions;
- the selection of common controls;

- the selection of suppliers, services, and contractors to support organizational missions/business functions;
- the development of risk-aware mission/business processes;
- the interpretation of information security policies with respect to organizational information systems and environments in which those systems operate.

Tier 3 includes, for example:

- design decisions (including the selection, tailoring, and supplementation of security controls and the selection of information technology products for organizational information systems);
- implementation decisions (including whether specific information technology products or product configurations meet security control requirements);
- operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions).

02.4.2 Provision of Risk Assessments

Service provision will be capped to **3 businesses** with a **maximum of 10 business days each**, as follows:

According to the *NIST Special Publication 800-30 Risk Management Guide* and *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments*, the risk assessment and management activities to be included, but not limited to, are:

- System Characterization
- Identify Threat Sources
- Identify Threat Events
- Identify Vulnerabilities and Predisposing Conditions
- Analyse Controls
- Determine Likelihood
- Determine Impact
- Determine Risk
- Recommend Controls for Risk Management
- Document Results which will align with *APPENDIX K of NIST Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments*

02.5 Audit & Reviews

The audit and reviews service offers comprehensive guidance to applicants on maintaining and continuously improving their internal or external cybersecurity standards, policies, and procedures. Applicants can choose specific parts of their policies or procedures to be audited or reviewed, aligning with standards such as the “ISO27k” family, NIST CSF, and PCI-DSS.

The service also assists applicants in meeting certification or compliance requirements related to these standards. Additionally, for existing cybersecurity policies and procedures, applicants can opt for audits and reviews of specific parts of their policies/procedures/standards in line with a subset of the standards mentioned, assisted through recommendations of changes or improvements.

02.5.1 Provision of Audit & Reviews

Service provision will be capped to **3 businesses** with a **maximum of 10 business days each**, as follows:

Guided by the Guidelines for auditing management systems (ISO 19011:2018), the activities to be included, but not limited to, are:

- Determine any areas of interest, concern or risks to the auditee in relation to the specific audit
- Determine feasibility of audit
- Collect and verify information
- Audit evidence

- Evaluate evidence against audit criteria
- Generate audit findings
- Determine audit conclusions
- Conduct closing meeting & audit report

03. Eligibility

03.1 Eligible participants

The Cyber Assess Scheme is open to natural or legal entities engaged in economic activities formally recognised by relevant Government authorities in Malta.

03.2 Internet-facing services

The applicant must have at least one of the following eligible internet-facing services:

a. Corporate e-mail solution with a dedicated domain
b. File Transfer Protocol (FTP) solution managed by the applicant
c. Corporate VPN service
d. API endpoints connected to the corporate infrastructure managed by the applicant

03.3 Service limitation

Each participating entity is eligible for one service only.

03.4 Compliance with De Minimis State aid regulations

The aid under this scheme is granted as de minimis aid 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, as amended. In terms of provisions of this regulation, each single undertaking may not receive more than €300,000 in de minimis aid from any source of public funding (EU Funds and/or national funds) for the last three consecutive fiscal years.

Before filling in an application, applicants should first determine the amount of de minimis aid that the undertaking has received / applied for in the reference period and fill out the de minimis declaration form.

In determining the amount of de minimis aid received by the undertaking during the applicable reference period, the applicant must take into consideration the following:

- The total de minimis aid approved and received by the enterprises making up the single undertaking;
- Any state aid being applied for and / or de minimis aid pending approval;
- The amount of state aid applied for in the application being submitted under this grant scheme.

Single undertaking includes, all enterprises having at least one of the following relationships with each other:

A. One enterprise has a majority of the shareholders' or members' voting rights in another enterprise;
B. One enterprise has the right to appoint or remove a majority of the members of the administrative, management or supervisory body of another enterprise;
C. One enterprise has the right to exercise a dominant influence over another enterprise pursuant to a contract entered into with that enterprise or to a provision in its memorandum or articles of association;
D. One enterprise, which is a shareholder in or member of another enterprise, controls alone, pursuant to an agreement with other shareholders in or members of that enterprise, a majority of shareholders' or members' voting rights in that enterprise.

Enterprises having any of the relationships referred to in points (a) to (d) through one or more other enterprises shall also be considered to be a single undertaking.

Any de minimis aid received would have been notified to the undertaking by the grantor in writing. In this regard, applicants are to upload a signed copy of the de minimis declaration form.

It is the responsibility of the applicant to ensure that this declaration is correct and complete. Should it result otherwise, the application may be rejected or lead to an eventual recovery of funds subject to the applicable recovery rates as issued by the European Commission.

03.5 Application submission

A complete application form, as specified by the Scheme, must be submitted for consideration.

03.6 Additional provisions

The below solutions are outside of the scope of this Scheme:

a. Software as a Service (SaaS)
b. Platform as a Service (PaaS)
c. SCADA
d. Operational Technologies (OTs)
e. Personal devices

04. Application Process

Applications may only be filled in and submitted online through the NCC Funding Application Portal. It is important to note that the online application portal is customised to work best with the Google Chrome browser.

04.1 Registration and access to the NCC Funding Application Portal

To apply, one must first register to the online application portal, accessible through: nccfunding.gov.mt. This process needs to be conducted by the person who will be preparing and submitting the application on behalf of the applicant undertaking. This could either be an individual from within the undertaking, e.g. an authorised representative / employee / director / legal representative or the applicant himself / herself in the case of sole trader / self-employed, or an expert entrusted by the undertaking for this purpose.

A login window appears on screen as shown in Figure 1.

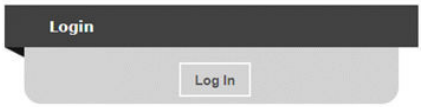


Figure 1: Login window

Upon clicking 'Log In', the system will divert to the e-id login page as shown below. Should the applicant not have a registered e-id, the applicant will need to contact the respective office to create an account.

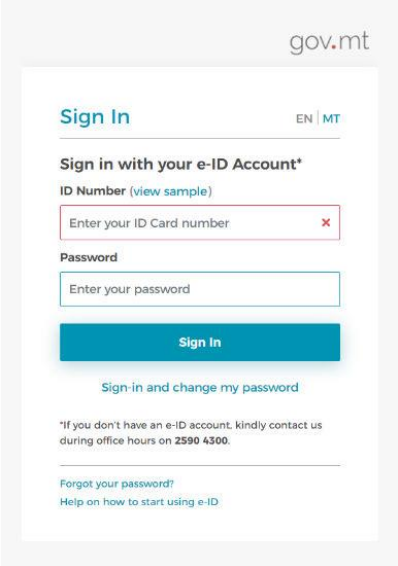
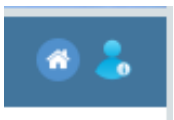


Figure 2: e-ID login window

Following registration and successful login, users can fill in and submit an online application form. **The applicant's user credentials should not be shared. The system will not allow multiple users to login to the same account at the same time. For security reasons, if multiple users attempt to login to the same account at the same time, the account will be disabled.**



Once logged in, there are two icons that appear at the top-right corner of the screen. These icons are visible in all of the application form screens. The 'Home' button will direct the user back to the home screen. The 'Person' button will give users the option to sign out.

Should ICT technical support be required, kindly contact the NCC on ncc.mita@gov.mt.

04.2 Selection of call

Once the user account has been successfully created, the user will be directed to log into the system. After logging in, the user will be directed to the home screen (shown in Figure 3) and will receive an email containing the user login and a link to activate the account.

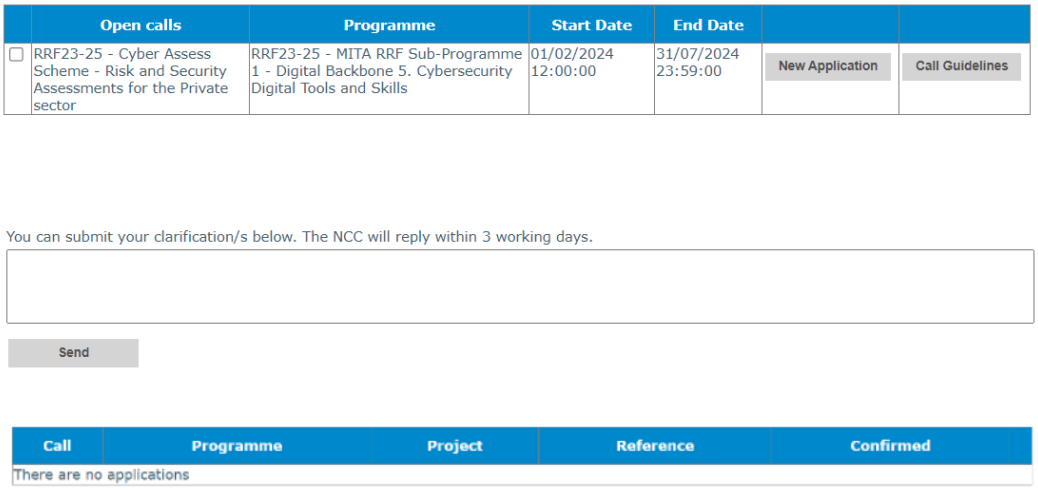


Figure 3: Home Screen

The home screen is divided into two sections. The upper section lists the **Open calls** and includes a **'New Application'** button. Once the correct call has been identified, in this case it would be 'RRF23-25 – Cyber Assess Scheme', the user is to click the **'New Application'** button to continue to the actual application form. The **'Call Guidelines'** button will allow the applicant to download a *.zip file* containing the related call documents.

In the section just below the open calls table, applicants are able to submit any clarifications they may have in relation to the call. To submit a clarification, the applicant would need to first select the tick mark for the respective open call and type in the clarification. Once the clarification has been completed, the applicant is to click the 'send' button. Clarifications will need to be made no later than 3 days before the call deadline. **To view previously submitted clarifications and respective answers,** the applicant is to tick mark the respective open call. Previously submitted clarifications and answers will then be shown in the section just below the previously saved application forms, 'Questions and Answers'.

The lower section of the home screen contains the details of any application forms that would have been previously created by the user. For new users, the lower section will appear empty as there would be no application forms created yet.

Once an application form is created, the **'**View' button found on the homepage, will allow the applicant to access the respective application form. It is relevant to point out that the system will allow the user to submit more than one project under any open call. In such cases, the user should click on the relevant 'New Application' button to create an additional application form if/and when required. If more than one application is submitted, the projects must demonstrate that they are stand-alone cybersecurity projects and that one is not dependent on the other.

Once the button 'New Application' is clicked, a new application is generated, and a page as shown in Figure 4 opens.

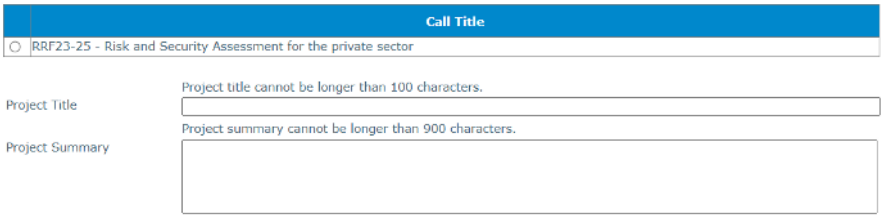


Figure 4: Project Title and Summary

The Project Title is to be created by the user. The Project Title should be a concise description of the project, and suitable to be retained as the permanent project name. Ideally this should not be longer than ten (10) words. **Note: once the 'Create' button has been clicked the field 'Project Title' cannot be amended.**

The Project Summary should be a short description of the proposed project. This section will serve as a summary of the project and therefore the information should be self-explanatory. As a minimum, the project summary should provide key details relating to the project, including the purpose of the project, what cybersecurity solution is being proposed, its key activities and the expected outcomes. (Max 900 characters)

The **'Create'** button will allow the user to proceed to the next step. Once this button has been clicked the information is saved in the system.

04.3 Step-by-step guidelines to complete and application form

04.3.1 General options

On the right-hand side of the application form, applicants will find 5 different function boxes: **Save**, **Print**, **Validate**, **Submit**, and **Delete** as shown in figure 5.

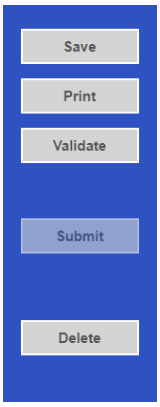


Figure 5: List of Function Options

It is important to note that '**Saving'** the document does not mean that the application form has been submitted to the NCC, but only that the information has been stored on the system. This means that the application form can still be updated/amended until the final version is submitted. It is recommended that the user saves regularly throughout the application process. If the user decides to sign out of the application form at any stage, the data which would have been saved will be retained. When the user decides to resume completion of the application form, by clicking the 'View' button in the homepage, the user will be redirected to the '**The Applicant**' section, which is the first section of the application form.

The '**Print**' function will allow the user to print the section that they are viewing. This will allow users to distribute the data internally without having to provide their credentials to third parties.

On the other hand, the '**Validate**' button should be used when the user wants to verify sections of the application form that have been completed. In order to confirm that the application form is being correctly filled in, it is recommended that sections are validated as soon as all the necessary information has been inputted. When the fields of the application form are filled in incorrectly, or data is missing, upon clicking the 'Validate' button an error notification will appear at the top of the page. The error notification will specify what the error is so that the user can rectify and save accordingly. Therefore, when filling in an application in different stages, the user will be prompted by an error if the 'Validate' button is clicked, as there would still be sections not yet filled in the full application form. If no errors are given, then the information inputted can be considered to be correct. Users are reminded that any changes made to a previously validated section will need to be re-validated. The applicant should validate the application form before saving it.

The **'Submit'** button will only be activated once all the sections have been validated. This function will result in the application being submitted for evaluation.

The **'Delete'** button will result in the permanent removal of the Application Form from the NCC Funding Application Portal. The applicant cannot delete an application once it has been submitted.

Applicants may generate **a copy of the online application form**, in PDF format, at any stage of the application form process. This can be done by clicking on the print functionality button that is available on the right-hand side of the screen which in turn will generate a screen informing the user that the application form is being exported. Applicants are to click on the "floppy disk" icon found at the top right corner of the screen and may generate this application form in Excel, Word of PDF format as required.

On the left-hand side of the application form, the user finds a list of all the sections of the application form. The user can navigate between the different sections by clicking the links shown in Figure 6.

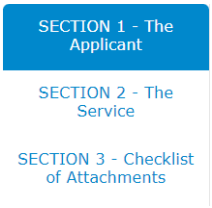


Figure 6: List of all Sections of the Application Form

04.3.2 Section 1 – The applicant

This section refers to the applicant undertaking that is seeking assistance through the scheme.

Section 2 consists of three (3) sub-sections which are described in further detail below:

04.3.2.1 Section 2.1 – Applicant details

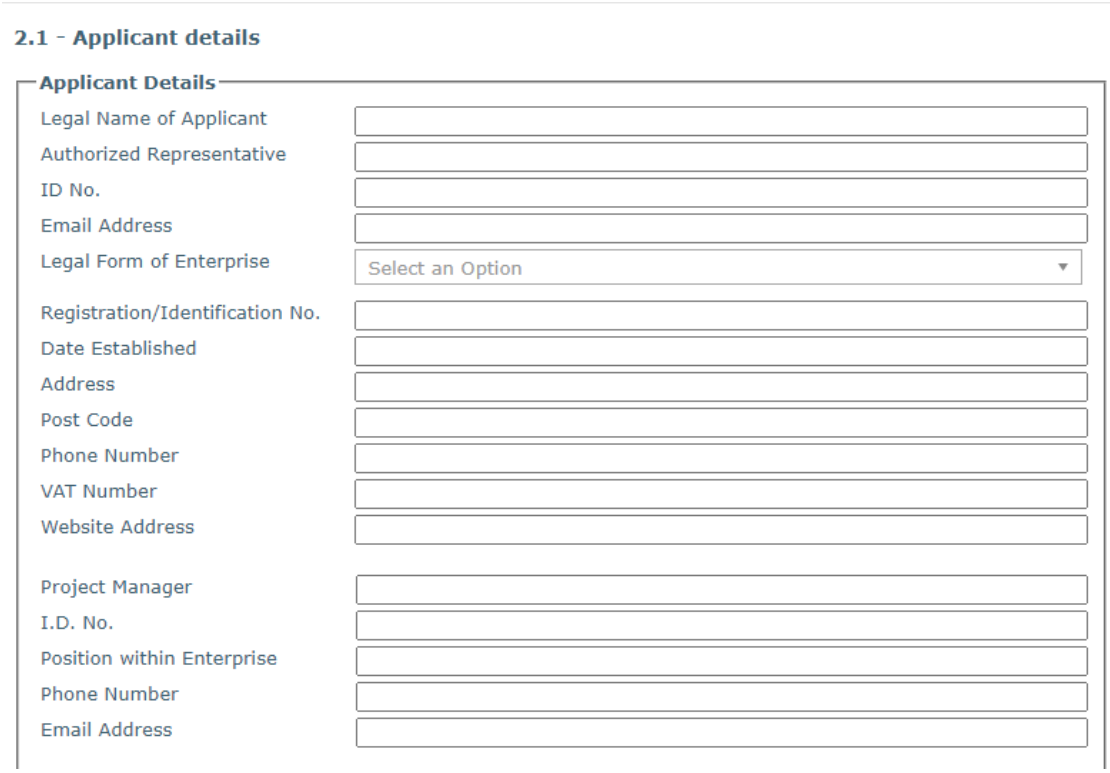


Figure 7: Applicant Details

The section 'Applicant Details' is shown in Figure 7 and the respective data fields are to be filled in by the user as follows:

Legal Name of Applicant – The applicant is to enter in this section its legal name that is:

- Limited liability companies – the name as defined in the Memorandum and Articles of Association;
- Partnerships and co-operatives - the name outlined in the deed of partnership should be inserted in this section; and
- Sole trader/self-employed persons - are to insert the name of the same self-employed person.

Authorised Representative – The authorised representative is an individual appointed by the applicant undertaking to enter into agreements on its behalf as outlined in the Memorandum and Articles of Association or pursuant to a declaration of the board of directors. A copy of the declaration is to be uploaded in Section 6 of the application form. In the case of sole traders/self-employed, this should be the name of the same self-employed person.

ID number – The identification number of the authorised representative is to be inserted.

E-mail Address – The email address of the authorised representative is to be included.

Legal Form of Enterprise – The user is to choose one of the options provided in the drop-down menu (see Figure 8).

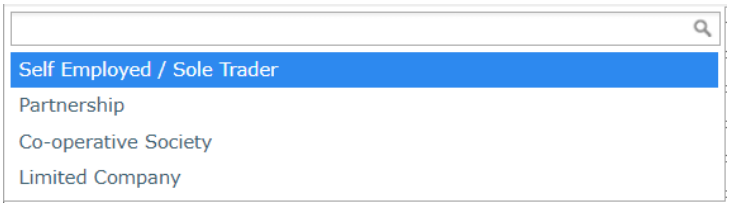


Figure 8: Legal Form of the Enterprise

Registration/Identification number – The Registration/Identification Number is the official registration number of the company or partnership in terms of the Companies Act, Chapter 386 of the Laws of Malta or the respective legal framework under which the applicant enterprise is registered. In those instances where the applicant is not registered under Chapter 386 of the Laws of Malta, the user is to upload the legal document constituting the enterprise under Section 6 of the application form. Sole traders/self-employed should enter their identity card number.

Date established – The user is to specify the date of establishment of the enterprise through the following:

A. For limited liability companies, the establishment date shall be the date of registration with the MBR;
B. In the case of self-employed, this shall be considered to be the date the person registered as a self-employed person with JobsPlus;
C. In the case of partnerships, the establishment date shall be considered to be the date of the deed establishing the partnership;
D. In the case of associations, the date of the statute establishing the association;
E. In the case of co-operatives, the establishment date shall be considered as the date of the registration of the co-operative with the Co-operatives Board;
F. In the case of others, the establishment date shall be considered as the date of registration of the organisation in terms of the applicable law of its establishment.

Registered address – The user is to insert the registered address of the enterprise.

Postcode – Insert the respective postcode.

Phone number – Insert the phone number of the enterprise.

VAT number – Insert the VAT number of the enterprise.

Website address – Insert the website address of the enterprise. In case the enterprise does not have a website, kindly input 'Not Applicable' in the field.

Project manager – The project manager is the person responsible for the implementation of the project. Only ONE project manager can be responsible for the project at any one time, even if the project is composed of different activities.

ID number – The identification number of the project manager is to be inserted.

Position within Enterprise – The user must provide the project manager's position within the enterprise. In case the project manager is someone external to the applicant enterprise, then this is to be specified accordingly.

Phone number – Enter the contact number of the project manager.

Email address – Enter the email address of the project manager.

The applicant needs to indicate the size of undertaking as shown in in Figure 12. The size of the undertaking is based on EU recommendation 2003/361 that can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

For more detailed information one may access the online 'User guide to the SME definition' from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm

Based on the aforementioned regulation, users are to primarily determine the linked and partner enterprises and subsequently fill in the details of the respective enterprises accordingly as shown in Figures 10 and 11. Should one need more space where to add any linked and/or partner enterprises, one can do so by clicking on the 'add another enterprise' button under the respective tables.

In the case where an applicant is an autonomous undertaking, or it has no linked and/or partner enterprises, the user is to insert the words 'Not Applicable' in the first row of the respective tables under Enterprise Name and Registration Number and a '0' under the column 'Shareholding %'. This will enable the proper saving and validating of data.

Enterprise Name	Registration Number
ABC Ltd.	C99999

Add an enterprise

Figure 9: Linked Enterprises

Enterprise Name	Registration Number	Shareholding %
ABC Ltd.	C99999	25

Add an enterprise

Figure 10: Partner Enterprises

One needs to then determine the size of the undertaking by calculating the headcount, turnover and balance sheet total of the applicant enterprise. This should be done by following the steps explained in the 'User guide to the SME definition'. This can be accessed from: https://ec.europa.eu/docsroom/documents/42921.

The table below also acts as a guideline on how the undertaking size can be determined:

Enterprise category	Staff headcount	Turnover	or	Balance sheet total
Medium Sized	<250	≤ € 50 m		≤ € 43 m
Small	<50	≤ € 10 m		≤ € 10 m
Micro	<10	≤ € 2 m		≤ € 2 m

Following these workings, the user is to then select one of the options from the list provided (refer to Figure 11) to specify the size of the undertaking.

Figure 11: Size of Undertaking

Following the completion of this section, the user must save the application form by clicking on the **'Save'** button found on the right-hand side of the screen in order to populate the drop-down function found in the next question. **It is essential for all the fields are completed and validated before saving.**

Applicants are to provide a copy of the **audited financial statements and/or the management accounts** dated within the two financial years prior to the year of submission of the application for the applicant enterprise and all the linked and partner enterprises as specified in the Guidance Notes for the grant scheme:

- Audited financial statements and/or the management accounts dated within the two financial years prior to the year of submission of the application in relation to the applicant and the linked and partner enterprises. No documents would need to be submitted if a copy of these documents as outlined hereunder is already deposited with the Registry of Companies.

    - With the respect to the last financial year, the applicant enterprise is to submit a copy of the detailed (not abridged version) of the audited financial statements or the management accounts (Profit & Loss Statements/Income Statement and Balance Sheet/Statement of Assets and Liabilities) certified by a Certified Public Accountant. The abridged version may be submitted with respect to the previous year.

    - In the case of linked and partner enterprises with an obligation to present Audited Accounts/Annual Accounts at the Registry of Companies in terms of the Companies Act (Chapter 386 of the Laws of Malta), no documentation need to be presented subject to the condition that the last audited accounts/annual accounts declared are not earlier than for the two financial years prior to the year of submission of the application.

    - In the case of linked and partner enterprises without a legal obligation to prepare financial statements, the management accounts (Profit & Loss Statements/Income Statement and Balance Sheet/Statement of Assets and Liabilities) certified by a Certified Public Accountant.

    - In the case of a start-up established not over 2 years from the date of application not having the above documentation, a Profit & Loss Account/Income Statement, Cash Flow Projections and a Balance Sheet/Statement of Assets and Liabilities certified by a Certified Public Accountant.

- In the case of a sole trader/self-employed, a copy of the income tax return for the last 2 years together with a Profit & Loss Statement certified by a Certified Public Accountant.

In order to upload accounts, one is to first select whether the accounts that are going to be uploaded are for the applicant, or for a linked or partner enterprise. The relevant enterprise names will then be made available from the dropdown list and the appropriate enterprise is to be chosen accordingly. This dropdown list is populated from the information provided earlier in section 2.1. The accounts files are then to be uploaded by clicking on the choose file button which will open a window through which the documents can be uploaded. One should note that the annual accounts should be saved in one .pdf document or in a zip file. When the information has been filled and the correct accounts files chosen, the user can then choose to save the information by clicking on the **'Save Account'** button found on the bottom left of the form. Once the form has been saved, one can add the account details of additional linked or partner enterprises by redoing the process.

In order to delete any previously saved entries, one must first select the saved entry and then click on the 'Remove Account' button found at the bottom of the form. It is important to be sure before deleting entries as any deleted entries will not be recoverable.

In order to clear the form from any details entered before saving, one can click on the **'Clear'** button which is found on the bottom right of the form.

Alternatively, to change a single uploaded file simply click on the respective enterprise name, once the entry is highlighted in blue click on the **'Choose file'** button where the original file was uploaded, the line will still read **'No file chosen'** as this does not reflect previously uploaded documents, however, you can still upload the new file which will replace the previously uploaded one. Once the new file has been chosen, click on the **'Save account'** button. To check whether the new file was uploaded, click on the respective enterprise name, once the entry is highlighted in blue click on the **'View'** document button next to either Accounts 1 or Accounts 2, depending on where the document was uploaded. The saved file will be downloaded to your PC.

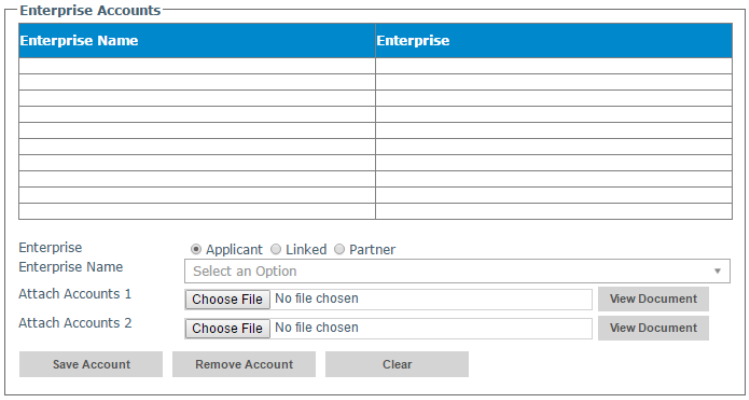


Figure 12: Enterprise Accounts

When uploading files, applicants need to ensure that no commas (,) are in the file name.

04.3.2.2 Section 1.2 – Applicant's core business activities

NACE Code – The user is to insert the digits of the NACE code describing the commercial activity of the enterprise. Automatically, the respective description of the activity linked to the particular NACE code will show in the space provided.

Applicants are to note that the NACE classification of an enterprise is usually available in the VAT Information Sheet received together with the VAT Certificate issued by the Commissioner for Revenue. In this regard, enterprises are to ensure that the NACE Code in this VAT Information Sheet truly reflects their actual primary economic activity.

In those cases where applicants do not have such documents, they may seek guidance from the Business Register at the National Statistics Office (NSO) in writing in order to determine the respective NACE Code.

NSO Business Register

Tel: 25997353

E-mail: br.nso@gov.mt

As evidence of the applicant enterprise NACE Code, one is to submit either a copy of the VAT Information Sheet or a copy of the communication between the applicant and NSO in Section 6 (Checklist of attachments) of the application form as supporting documents.

As for start-up enterprises not yet having a VAT Information Sheet in hand, or any other enterprise which in line with VAT regulation are not issued a VAT number by the Commissioner for Revenue, these are requested to determine their respective NACE classification by referring to the NACE Rev. 2 classification which is available online.

In this section, one is to provide further details on the core business activities in which the enterprise is engaged in and provide a background description of the enterprise and its investment project (Max 5,000 characters).

04.3.3 Section 2 – The service

The applicant is to describe the service they would like to acquire through the Cyber Assess Scheme.

04.3.3.1 Section 2.1 – Service being applied for

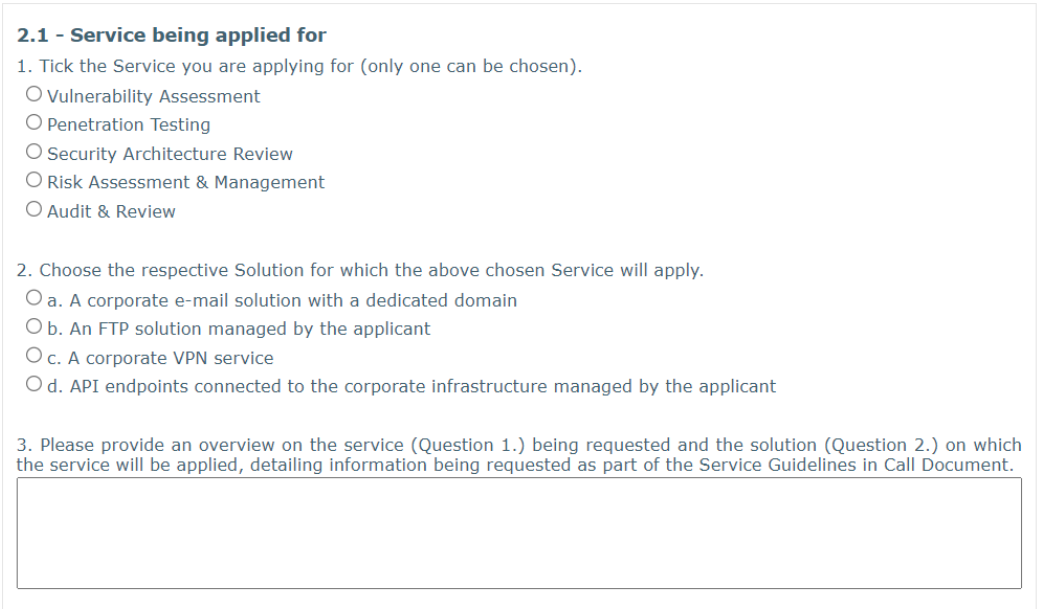


Figure 13: Service being applied for

For **Question 1.**, the applicant must specify the service for which they are submitting the application form. They can only choose one service option.

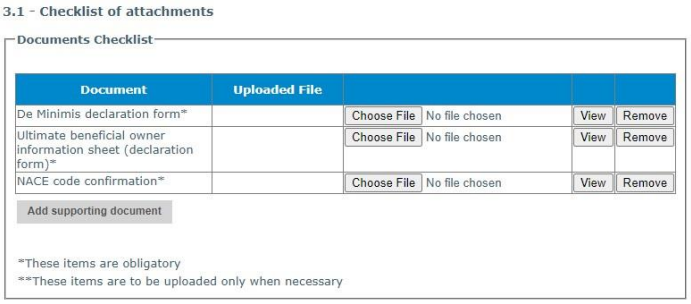
For **Question 2.**, the applicant must indicate the specific solution to which the service chosen in Question 1 will cover. They can only choose one solution option.

For **Question 3.**, the applicant must provide a detailed overview in line with *Section 02. Service Guidelines* of this Call Document, on the service being requested and the solution on which the service will be applied.

04.3.4 Section 3 – Checklist of Attachments

For ease of reference, a checklist has been provided in the application form as per figure 14.

The relevant uploading section displays an information table containing the name of the **uploaded file** (the column will be empty until a file is uploaded), a '**Choose File**' button, a '**View**' button and a '**Remove**' button.


3.1 - Checklist of attachments

Documents Checklist

Document	Uploaded File			
De Minimis declaration form*		Choose File No file chosen	View	Remove
Ultimate beneficial owner information sheet (declaration form)*		Choose File No file chosen	View	Remove
NACE code confirmation*		Choose File No file chosen	View	Remove

Add supporting document

*These items are obligatory
**These items are to be uploaded only when necessary

Figure 14: Checklist of Attachments

The applicant is required to upload the following mandatory documents identified in the above checklist with the application form.

a) **De Minimis declaration form**: a declaration by the single undertaking outlining a breakdown of the de minimis aid applied for and granted to the single undertaking over a period of the three fiscal years from the year of application.

b) **Ultimate Beneficial Owner Information Sheet (Declaration form)**: a scanned copy of a completed and signed Ultimate Beneficial Owner (UBO) information sheet, confirming the ownership of the applicant undertaking. This is to be signed by the authorised representative of the applicant. Should there be a change to one or more of the UBOs, the applicant must notify the NCC immediately and submit an updated UBO Information Sheet via email.

c) **NACE code confirmation**: The NACE confirmation shall be in the form of VAT Information Sheet or else a communication with the NSO Business Register including the four-digit code in the form of 11.11.