Mind the Gap Project

Guidelines

Definitions

"**Mind the Gap**" or "**Mind the Gap Initiative**" is a collaborative initiative that is currently composed of the Cybersecurity Self-Assessment scheme led by the MDIA, and the Cybersecurity Improvement scheme led by Tech.mt, with the MCA, as the authority responsible for E-Commerce, assisting from a design and promotional aspect.

"Cybersecurity Self-Assessment Scheme", "**Cybersecurity Self-Assessment**", or "**Self-Assessment**" refers to a scheme under Mind the Gap, that is derived from the TAAF level 0 Self-Assessment programme, in which the Applicant carries out a self-evaluation of their cybersecurity maturity levels.

"**Cybersecurity Improvement Scheme**" refers to a complementary scheme under Mind the Gap that is managed by Tech.mt which provides funding for the improvement of Cybersecurity maturity levels.

"**Mind the Gap Portal**", or "**Portal**" refers to the online portal through which the Mind the Gap initiative schemes may be undertaken.

"**Applicant**" refers to the e-commerce service provider, be they an individual or a company, that is applying to undergo the Cybersecurity Self-Assessment.

"**Maturity levels**" refers to a measurement of the Applicant's level of Cybersecurity robustness for a specific aspect.

"**Acknowledgement**" refers to an official reference provided by the MDIA through the Mind the Gap Portal that may be shared publicly to showcase that the Applicant has undergone the Cybersecurity Self-Assessment.

"**E-commerce**" means a service provided at a distance, through the internet, by electronic means.

"**MDIA**", or "**Authority**" refers to the Malta Digital Innovation Authority, established by the **Malta Digital Innovation Authority** Act, Chapter 591 of the Laws of Malta.

"**Tech.mt**" is a foundation established in partnership with the government of Malta and the Malta chamber of commerce to promote the national strategy for technology and innovation.

"**MCA**" means the **Malta Communications Authority** established by the Malta Communication Authority Act; Chapter 418 of the Laws of Malta.

"**TAAF**", or "**Technology Assurance Assessment Framework**" refers to the MDIA's overarching framework intended to cater for different levels of assurances, which the Cybersecurity Self-Assessment has been derived from (at level 0). More information on TAAF is available at https://mdia.gov.mt/taaf/.

"**Terms and Conditions**" refers to the complementary "Cybersecurity Self-Assessment Scheme Terms and Conditions" document as published on the MDIA's website and available through the Mind the Gap Portal.

1 Mind the Gap Initiative

Mind the Gap is a collaborative initiative between the MDIA, Tech.mt and the MCA that seeks to make available schemes to assist Maltese businesses in mapping out their Cybersecurity maturity levels to identify any gaps in their operations.

Mind the Gap is currently composed of two complementary schemes:

i) **Cybersecurity Self-Assessment Scheme**: A self-evaluation tool, driven by the MDIA, for e-commerce providers to analyse their cybersecurity maturity levels.

ii) **Cybersecurity Improvement Scheme**: A fund of up to €10,000 per Applicant, driven by Tech.mt, to provide financial assistance to those who undergo the Cybersecurity Self-Assessment and would like to improve their maturity levels.

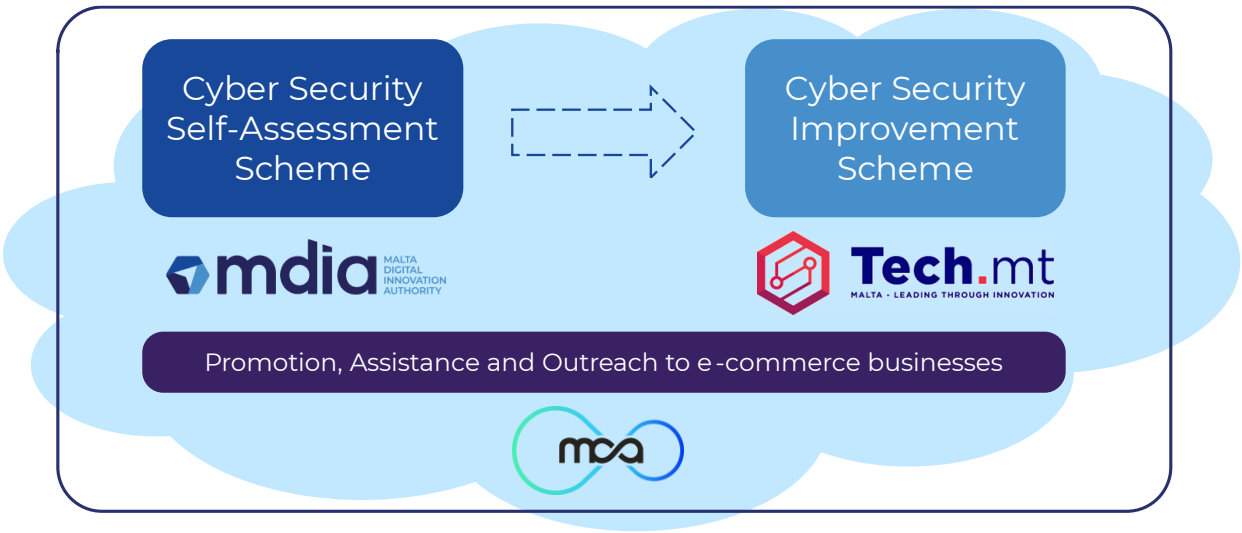

Figure 1: The Mind the Gap initiative

These two schemes are presented on the Mind the Gap portal, to put them within the same digital platform ensuring a seamless transition for Applicants looking to avail themselves of both schemes.

2 Introduction

Cybersecurity awareness is growing not only amongst the businesses that operate e-commerce services online, but also amongst the public. Due to this increasing appreciation for security online end-users have grown to have a certain level of expectations in relation to the cybersecurity features of the portals that they use and transact through.

The Cybersecurity Self-Assessment scheme is led by the MDIA with the technical and promotional collaboration of Tech.mt and the MCA. It aims to assist local businesses that provide e-commerce services with an opportunity to understand their level of cybersecurity maturity, while also providing them with the option of publicising their efforts in monitoring and improving their cybersecurity through an acknowledgement issued by a National Authority.

The Cybersecurity Self-Assessment is primarily an educational tool derived from the MDIA's Technology Assessment Assurance Framework as a level 0 using a self-assessment methodology. The Self-Assessment is in the form of a questionnaire of about 50 questions that should take a round 2-3 hours to complete and will provide the Applicant with a score indicating the maturity levels. This enables it to provide an opportunity for businesses to directly gauge their maturity in this regard, hence providing a low barrier to entry.

Other than providing a level of insight into the e-commerce platform's cybersecurity standing, the Cybersecurity Self-Assessment will be able to provide information on any weaknesses (gaps) or strengths that have been identified through the process, so that weaknesses may be rectified or improved. Furthermore, the MDIA provides the option to issue an official acknowledgement of the cybersecurity maturity level that may be shared publicly, subject to the applicable Terms and Conditions being accepted.

A separate scheme offered and managed by Tech.mt has been set up to provide financial assistance to businesses (subject to availability of funds), in addressing any gaps they may identify through the Cybersecurity Self-Assessment.

About the MDIA

The MDIA was established back in 2018 through the Malta Digital Innovation Authority Act, together with the Innovative Technology Arrangements and Services Act, that states what are the powers granted to the Authority.

The Authority serves a dual role. On the one hand, it is a regulator specifically focused on innovative technology and forms part of the entities strategically established in the Maltese ecosystem. On the other, it is also a promoter of innovative technologies. This is done through various incentives that are announced from time to time.

More information about the MDIA may be found at https://mdia.gov.mt/

About Tech.mt

Tech.mt aims to position Malta as a quality, creative, tech-savvy country, and promote Malta as a suitable set-up for foreign direct investment, whilst also promoting the local technological industries abroad.

Tech.mt shall be instrumental in taking the Technology industry to the next level, as it will seek to make the world notice the huge potential the technology sector in Malta has to offer as it boasts on the economic performance and financial stability of the island. We acknowledge that data is the new oil, Tech.mt wants to be part of the IOT evolution and be on the forefront of the global digital revolution that we are experiencing.

To encourage human resources and aid growth in the Technology, Tech.mt plans to partner with Education Institutions to position Malta as a vibrant location for tech talent and in turn attract human capital to our shores. Furthermore, Tech.mt is working closely with academic institutions to better understand how the local STEM and IT curricula can be made more attractive to be chosen as the basis for a career in technology. We also need to consider new areas of specialisation revolving around digital & creative technology.

Tech.mt is also focusing its energies on engaging the youth community. Youths are major stakeholders who are constantly using digital technology thus, encouraging youth participation in the transformation of the digital economy is crucial.

About the MCA

The MCA was established on the 1st of January 2001 and is the statutory body responsible for the regulation of the various electronic communications sectors, which include fixed and mobile telephony, Internet, and TV distribution services. Furthermore, the Authority regulates two other sectors which are the postal services, as well as the eCommerce sector.

More information about the MCA may be found at https://www.mca.org.mt/

Technology Assurance Assessment Framework

The Cybersecurity Self-Assessment programme is derived from the MDIA's Technology Assurance Assessment Framework ('TAAF') and emerges from the TAAF Level 0 category Self-Assessment programme.

TAAF provides for tailored technological reviews, assessment and assurance at varying levels and a wide spectrum of technology solutions, across different risk appetites. The Cybersecurity Self-Assessment will specifically focus on the operators of e-commerce services.

More information on the TAAF may be found at https://mdia.gov.mt/taaf/ or by contacting the MDIA at https://mdia.gov.mt/contact/.

3 Conditions for Eligibility

This section outlines the requirements that Applicants must agree to and abide by when undergoing the Cybersecurity Self-Assessment.

The Applicant must:

- Represent an e-commerce service that is either based in Malta or whose solution being analysed is specifically aimed towards the Maltese user base.
- Have legal ownership of the service that is subject to the Self-Assessment.
- Accept that the MDIA may request evidence to substantiate claims and answers made by the Applicant and agree to cooperate with the Authority.
- Present a solution that is fully compliant with the laws of Malta.
- Provide information which, to the best of their knowledge, is accurate and up to date.
- Be fully aligned to all requirements and clauses defined in the Cybersecurity Self-Assessment Terms & Conditions.

The Applicant may appoint any individual, be they internal or external to the Applicant's business, to conduct and carry out the Self-Assessment for them.

While the above present the general eligibility criteria, the MDIA's regulatory team may conduct further due diligence on applicants on a case-by-case basis at their discretion.

4 Cybersecurity Self-Assessment

The Cybersecurity Self-Assessment is in the form of a questionnaire that is made up of 50 questions and is designed to take around 2 to 3 hours to complete and is intended to be taken by an individual with a technical IT background and who is also familiar with the Applicant's technological solution, and processes.

The Applicant may carry out the assessment by logging onto the online *Mind the Gap* portal (as published on the MDIA website) and following the on-screen instructions. By logging on the *Mind the Gap* portal, the Applicant is assumed to have read, accepted and agreed to abide by these guidelines, as well as terms and conditions, and any other associated documentation as published by the MDIA.

Should the Applicant identify aspects of their cybersecurity standing that they would like to improve, the Cybersecurity Improvement Scheme led by Tech.mt will be providing a limited fund with financial assistance to aid in doing so. While funding is limited it may be renewed from time to time, and when available, the *Mind the Gap* portal will provide the facility to apply directly for the Cybersecurity Improvement Scheme.

Assessment Process

The *Mind the Gap* portal will first request basic information to identify the Applicant, and the solution subject to assessment and will then proceed to pose a structured set of questions. Clear on-screen instructions are provided to assist in the undertaking of the self-assessment. Each question will have 6 specific maturity level descriptions associated with it so that the Applicant may easily tick the maturity level that applies. The Applicant may either provide a rating to the question according to the maturity level or mark the question as not applicable to their solution. If the question is marked as not applicable, so the score will not be negatively affected by its non-applicability. On the other hand, if the Applicant is unable to adequately assess the maturity level, they may also answer the question by '*Do not know*'.

Upon completion the Applicant will be presented with the overall score and the score per category. This will enable the Applicant to determine where the cybersecurity strengths and weaknesses lie, depending on the Applicant's self-determined expectations, targets, and objectives.

Sample Questions

This section provides a set of varied sample questions that form part of the Cybersecurity Self-Assessment to give an idea of the format, type of questions and the expected response.

Sample Question 1 – Identity and Access management

Question	
How is multi-factor authentication used in the e-commerce application/ platform/ infrastructure?	
0 - Limited	No Multi-factor authentication is currently used
1 - Initial	Multi-factor authentication may be used on a limited basis.
2 - Managed	Multi-factor authentication is only used for remote access for privileged users (e.g., administrators).
3 - Defined	Multi-factor authentication is only used for remote access for all users.
4 - Quantitatively Managed	Multi-factor authentication is required for use of privileged access.
5 - Optimised	Multi-factor authentication is required for use of privileged access and access to any sensitive/confidential data.
N/A – Not Applicable	This question does not apply to me.
Do Not Know	I do not understand the question.

Sample Question 2 – Network Security

Question	
How does the e-commerce application/ platform/ infrastructure employ wireless network infrastructure (Wi-Fi) for employees and third-parties?	
0 - Limited	An open, unencrypted, wireless network is implemented for employees and third-parties.
1 - Initial	A wireless network, using a weak encryption protocol (e.g., WEP), is implemented for employees and third-parties.
2 - Managed	A wireless network, using a weak encryption protocol (e.g., WEP), is implemented for third-parties, whilst WPA2 is configured for employees.
3 - Defined	Wireless networks for employees and third-parties are implemented, and are strongly protected (e.g., WPA2); networks are connected to, and confined within, a dedicated network segment.
4 - Quantitatively Managed	Wireless networks for employees and third-parties are implemented, and are strongly protected (e.g., WPA3); networks are connected to, and confined within, a dedicated network segment.
5 - Optimised	Wireless networks for employees and third-parties are implemented, and are strongly protected (e.g., WPA3); networks are sufficiently segmented and monitored (e.g., WIPS).
N/A – Not Applicable	This question does not apply to me.
Do Not Know	I do not understand the question.

Sample Question 3 – Software Security

Question	
Does the organization perform external attack and penetration assessments as a part of the software development process related to the e-commerce application/ platform/ infrastructure?	
0 - Limited	No technical testing is performed as part of the Software Development Life Cycle ('SDLC').
1 - Initial	Ad-hoc technical testing is performed as part of the SDLC.
2 - Managed	Some internal automated scanning is performed for high-risk systems related to the e-commerce application/ platform/ infrastructure.
3 - Defined	Internal testing and/or external automated scanning is required for all systems.
4 - Quantitatively Managed	Yes, grey box attack and penetration testing is performed for high-risk applications.
5 - Optimised	Yes, black box attack and penetration testing is performed as part of the SDLC.
N/A – Not Applicable	This question does not apply to me.
Do Not Know	I do not understand the question.

Note: As this relates to the Software Development Lifecycle, this sample question would not be applicable to entities that do not build and/or maintain their own e-commerce portal (but may purchase an off-the-shelf system or service), in which case it may be marked as N/A.

Question Categories

The questions of the Cybersecurity Self-Assessment are structured by category, with each of the categories containing one or more questions.

They are designed around a wide range of cybersecurity criteria so that any gaps in the maturity level, particularly if critical in nature, can be identified and subsequently rectified.

The categories are:

Category	General Description
Identity & Access Management	Identity and Access Management refers to the processes associated with managing the entire lifecycle of digital identities and profiles for people, processes, and technology.
Incident Response	The Incident Response category defines the formal function for reporting and responding to incidents that may adversely impact the organization's assets, operations, reputation, financial position, intellectual capital, or confidential information.
Operational Metrics	The Operational Metrics category encompasses any defined, repeatable measurement activity that aids the organization in understanding the various technology components and how it supports the business strategy.
Network Security	The network security category captures the policies, processes, tools, and technologies that are used to maintain security at the network level.
Operations	The Operations category encompasses all risks associated to change management, configuration management, communications and operations management, backup, physical and environment security, system planning and acceptance, operations access control
Policies	This category refers to the Information Security Policies that the organisation currently, enabling standardization and best security practices.
Privacy	The Privacy category captures on data is collected, disclosed to third parties, retained, and used and shared across an organization.
Logging & Monitoring	This category relates to the successful monitoring of logs from network devices, hosts, files, databases, and privileged user access to identify or be alerted of events that require further investigation due to the potential of being security events.
Software Security	The Software Security category encompasses how security is integrated with the Development lifecycle and software configuration of an organization.

Category	General Description
Vendor Risk Management	This category is associated to the process for managing vendors, and the transfer and exchange to, or storage of information/data by the vendors.
Vulnerability Management	Vulnerability Management refers to the existing capabilities of an organization to identify, prioritize and remediate vulnerabilities and apply security patches.
Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets to that can be used to inform decisions regarding the subject's response to that menace or hazard.
Architecture	The architecture category is subjecting to manage the information security solutions and technologies that promote interoperability and manageability while meeting the organization's risk management needs.
Asset Management	IT Asset Management encompasses the infrastructure and processes necessary for the effective management, control and protection of the hardware and software assets within an organization, throughout all stages of their lifecycle.
Awareness	This category is associated with an organisation's security awareness program consists of all staff within an organization, including self-employed staff, contractors, and third-party service providers.
BCP/ DR	This category covers business continuity and disaster recovery concepts such as senior management support for Business Continuity Management, adequate skilled resources, process definition, business impact analysis, testing of plans, and metrics reporting.
Cloud Computing	This category is associated with the fundamental risks arising from the use of Cloud Computing
Data Protection	This category focuses on protecting data and heavily relates to an enterprise's goal to effectively manage data loss risks.
Host Security	This category covers the protection mechanisms and controls in place at the host level. Topics in scope for this section are: anti-virus, full disk encryption, malware protection, hardware access control and patch management

Self-Assessment Results

The detailed results provided to the Applicant will record the maturity levels (scored between 0 to 5 as per above table) in relation to: i) per individual question; ii) per category; and iii) as an overall maturity level. Scores are calculated by taking the average of the provided maturity levels for the question at either category level or overall, excluding any *Not Applicable* responses.

The score will be in the form of a number, which will indicate the level of cybersecurity maturity that the Applicant has attained. The table below serves to outline the general meaning of each of the maturity levels:

Maturity Level	General Description
0 - Limited	Limited to negligible technology and controls are in place, deployed in an inconsistent manner. No local processes are in place.
1 - Initial	Basic technology and controls are in place but deployed in an inconsistent manner. Limited local processes are in place with limited organizational support.
2 - Managed	Partial technological maturity is in place with a combination of some technology and tools; local processes covering some regions/business units or processes are repeatable.
3 - Defined	A defined maturity is in place with significant technology and tools for some key resources and people; processes defined for some regions and/ or business units.
4 - Quantitatively Managed	A mature capability is in place with advanced technology and tools for some key resources and people, consistent processes exist for some regions and/or business units.
5 - Optimised	An advanced capability is in place which is leading-edge technology and tools for all key resources and people, consistent process across regions, business units, and effective governance is in place.

Therefore, if an Applicant obtains a cybersecurity maturity score of 2.4, their level of maturity would sit right between *Managed* and *Defined*. As each e-commerce service application has different requirements, it will be down to the Applicant to determine which areas they would like to improve upon based on the obtained maturity levels. As this is a self-assessment, it is extremely important for the Applicant to note that the maturity levels deemed acceptable must be commensurate with the risk appetite of the Applicant as well as the technology context (i.e., how the technology is deployed, is being used, and the risks associated with that).

5 Issuance of Acknowledgement

The Applicant may request, via the *Mind the Gap* portal itself, to be provided with an acknowledgement of the obtained maturity levels, so that it may be published on their e-commerce service portal. This acknowledgement will be issued by the MDIA in an electronic manner, in the form of a unique URL that the e-commerce service operator may utilise.

The Applicant will be provided with three (3) options of formal acknowledgements that they may obtain:

1. An acknowledgement showing that the Applicant has participated in the Cybersecurity Self-Assessment Scheme
2. An acknowledgement showing the overall score (in addition to #1).
3. An acknowledgement showing the score at the level of every category (in addition to #2).

The Applicant is being provided with this option to ensure that if they identify any weaknesses in some categories that may still be relevant to them, but overall, still exhibit a satisfactory level of maturity, they may display the acknowledgement without necessarily publishing any categories they may have weaknesses in. Alternatively, should the Applicant wish to highlight their maturity levels across specific categories they may avail of the relevant option.

The acknowledgement will include the date on which the Cybersecurity Self-Assessment was taken and is valid for 1 year from date of issue. Obtaining the acknowledgment is entirely optional and left at the discretion of the Applicant.

Note: It is recommended that applicants should publish the acknowledgement that shows the participation without scores unless they specifically have a reason to do otherwise (which reason is left to the Applicant's discretion). The MDIA is not responsible for any repercussions that may result from publishing the acknowledgement.

Obligations

The MDIA reserves the right to request evidence or carry out a review (at the Authority's expense) in order to ensure the veracity of the information provided. The Authority may elect to undergo this process at any time while the acknowledgement is valid. In conducting such a review, the Authority, or one of its appointed representatives may request, among others, documentation, interviews, or on-site reviews. All information provided will be handled in strictest confidentiality and in line with the Terms and Conditions. Failure to cooperate may result in the acknowledgement being withdrawn.

6 Application Process

Once an Applicant reviews these guidelines, is ready to agree to the terms and conditions and verifies conformity with the Conditions for Eligibility (refer to section 3), they may proceed with undertaking the self-assessment.

To apply for the Cybersecurity Self-Assessment programme, an Applicant is required to visit the online *Mind the Gap* portal and follow the on-screen instructions.

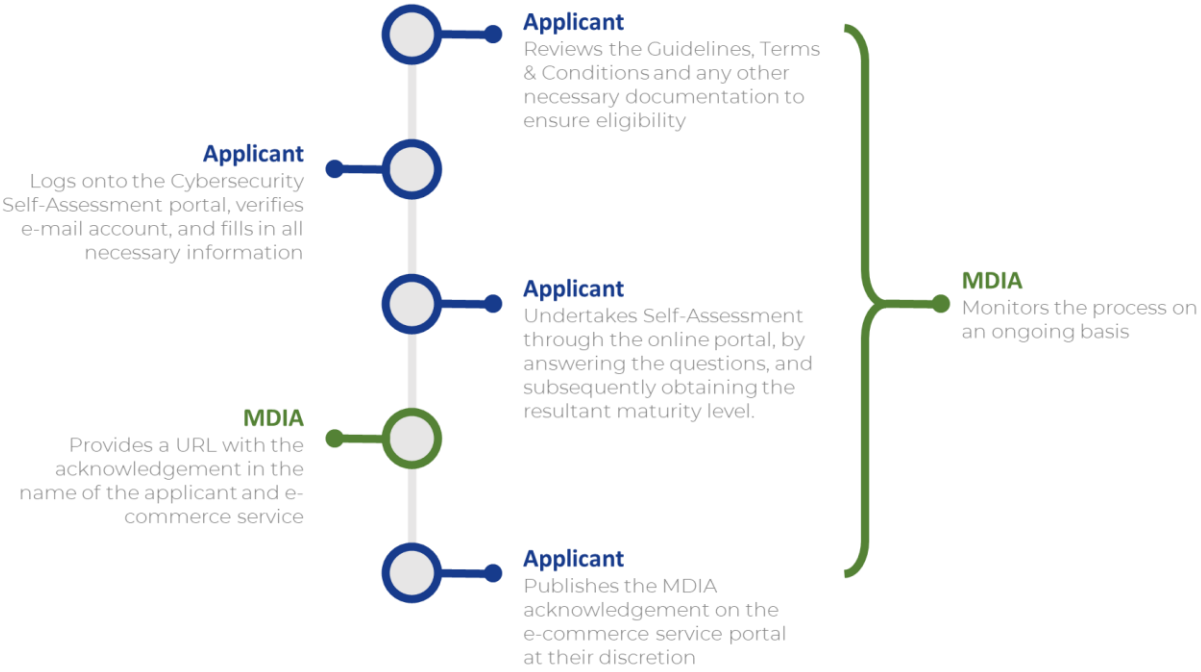

Figure 2 Cybersecurity Self-Assessment Process

Prior to undergoing the Cybersecurity Self-Assessment, the Applicant will be required to provide the below information through the *Mind the Gap* portal:

- Name of Applicant (e.g., business that owns the solution)
- Company Identification Number (such as Company Number)
- Name of solution in scope for the Cybersecurity Self-Assessment
- Name and Surname of the individual taking the self-assessment
- ID Number of the individual taking the self-assessment
- E-Mail address to send communication relating to the Cybersecurity Self-Assessment on

Ownership of the E-Mail address provided must be verified prior to proceeding with the undertaking of the Cybersecurity Self-Assessment.

If the Applicant is unable to complete the Cybersecurity Self-Assessment in one session, progress will be stored and may be continued at a later date, up to a maximum of 30 days.

Fees

In order to fully assist businesses in assessing their cybersecurity maturity levels, the Authority will be making the Cybersecurity Self-Assessment programme available at no cost to the Applicant.

Should the Applicant request for an acknowledgement to publish on their portal, this too will also be made available at no cost to them.