TECHNOLOGY ASSESSMENT RECOGNITION FRAMEWORK

CONTROL OBJECTIVES

Guidelines

G-SPG-012
Rev. 1
29th November 2023

Contents

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

1 TARF Control Objectives

The Technology Assessment Recognition Framework (TARF) Control Objectives document presents the complete set of controls related to the framework.

Assessors may request a list in Excel format of the below control objectives from the MDIA, which includes further guidelines on descriptions of controls. It is important to note that such guidelines are not to be interpreted as being and are merely to serve as an aid to the Assessor.

> ***Note**: This document is meant to accompany the TARF Guidelines document. Please make sure you are familiar with the TARF Guidelines first before reviewing this document.*

1.1 TARF Summary

TARF provides a flexible framework for Assurance of technological products or services.

The Control Objectives applicable to the Applicant depend on the Applicant's selection of three (3) key criteria as part of the application process:

1. Assessment Level
2. Technology Domains
3. Control Types

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

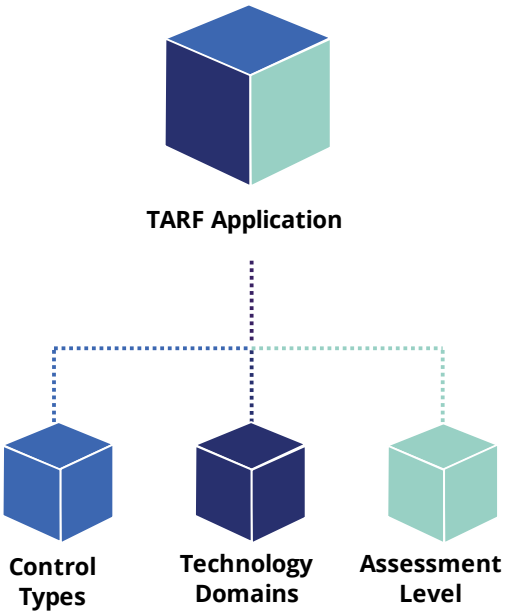

Figure 1 – The 3 key components of a TARF Application

1.1.1 TARF Assessment Levels

The Assessment Level determines the type of recognition to be issued by the MDIA and how onerous the controls to be assessed against should be.

The Assessment Level also determines the type of Assessment that needs to be carried out to satisfy the MDIA's TARF requirements, as well as the type of Assessor.

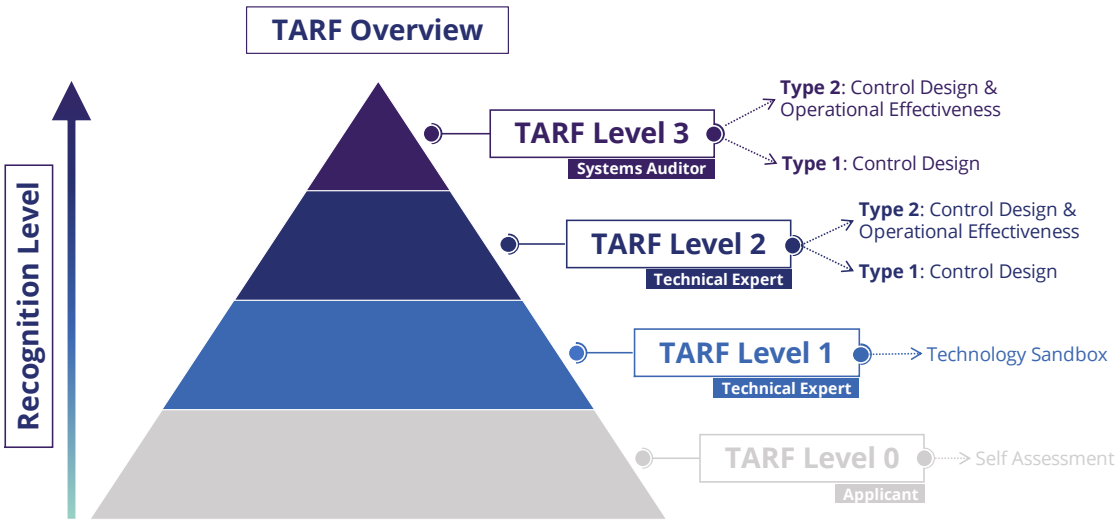

Figure 2 - an overview of the TARF Assessment Levels

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

> ***Note**: This document does not apply to TARF Assessment Level 0, since Self-Assessments are domain specific, and will each be governed by specific procedures and controls.*

1.1.2 Technology Domains

TARF provides controls for five (5) Technology Domains. The Applicant must identify the relevant Technology Domains at application stage.

These are:

1. General Innovative Technologies
2. Cloud Computing
    a. For Cloud Infrastructure Users; or
    b. For Cloud Infrastructure Providers.
3. Internet of Things (IoT)
4. Artificial Intelligence (AI)
5. Distributed Ledger Technologies (DLT)

1.1.3 Control Types

As part of the application process, the Applicant must also identify which Control Types are relevant to them and their IDPS, as each Technology Domain provides control types relevant to different categories of controls.

These are:

1. Accountability
2. Availability
3. Confidentiality
4. Integrity
5. Privacy

1.2 Definition of Acronyms

The below table defines the acronyms used in the control objectives.

Acronym	Definition
ISMS	Information Security Management System
DLP	Data Loss Prevention
IT	Information Technology

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

CSC	Cloud Service Customer
CLDP	Cloud Provider
IAM	Identity & Access Management
CSP	Cloud Service Provider
GDPR	General Data Protection Regulation
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
SIEM	Security Information and Event Management
CSOCs	Complementary subservice organization controls
DLT	Distributed Ledger Technology
AI	Artificial Intelligence
RTO	Recovery Time Objective
RPO	Recovery Point Objective

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

2 Selecting the relevant Control Objectives

While this document presents all the control objectives that may make up TARF, there are a significant number of possibilities, all depending on what the Applicant's selected as their Assessment criteria at application stage.

The controls applicable to an IDPS depend on the Technology Domain, and Control Types identified.

This document presents all the control objectives for each Technology Domain, further categorised by Control Objective Domains they pertain to. In each control, the applicable Control Types are also listed.

> ***Note** that due to the permutations possible, some control objectives between Technology Domains may overlap. In this case the control objective is only deemed to be applicable one time for reporting purposes.*

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

3 General Innovative Technology Controls

The General Innovative Technology Controls refer to on-premises computing systems and services, including servers, storage, databases, networking, software, analytics, and automation.

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	IDPS General Controls					
GEN-1	The applicant communicates information about the system design to the customers or users of the service.	✓	✓	✓	✓	✓
GEN-2	The applicant communicates the design documentation of the system to customers or users of the service.	✓	✓	✓	✓	✓
GEN-3	The applicant imlemenents the system in line with the Blueprint submitted to the Authority.	✓	✓	✓	✓	✓
	Organisation of Information Security					
OIS-1	The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OIS-2	Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the on premises infrastructure.	✓	✓	✓	✓	✓
OIS-3	The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	✓	✓	✓	✗	✗
OIS-4	Information security is considered in project management, regardless of the nature of the project.	✓	✓	✓	✓	✗
	Information Security Policies					
ISP-1	The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
ISP-2	Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	✓	✓	✓	✓	✓
ISP-3	Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	✓	✓	✓	✓	✓
	Information Protection					
IP-1	Information handling policies and procedures are documented to ensure information protection.	✓	✗	✗	✓	✗
IP-2	Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	✓	✗	✗	✓	✗
IP-3	Information discovery capabilities are in place for both scanning internal unstructured and structured data.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IP-4	DLP technologies should be configured monitor and restrict external file transfers.	✓	✗	✗	✓	✗
IP-5	The organisation shall manage the inventory of its sensitive data and data owners	✓	✗	✗	✓	✗
	Risk Management					
RM-1	Risk management policies and procedures are documented and communicated to stakeholders	✓	✓	✓	✓	✗
RM-2	Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	✓	✓	✓	✓	✗
RM-3	Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	✓	✓	✓	✓	✗
	Human Resources					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-1	The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	✓	✓	✓	✓	✓
HR-2	The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	✓	✓	✓	✓	✓
HR-3	The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	the applicant used to provide the service in the production environment.					
HR-4	The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	✓	✓	✓	✓	✓
HR-5	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	✓	✓	✓	✓	✓
HR-6	Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	the confidentiality of the information exchanged between them.					
	Asset Management					
AM-1	The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	✗	✓	✓	✗	✗
AM-2	Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	✓	✓	✗	✗	✗
AM-3	The applicant has an approval process for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
AM-4	The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	✓	✓	✗	✗	✗
AM-5	Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	✓	✓	✗	✓	✗
	Physical Security					
PS-1	Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	✗	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PS-2	There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	✗	✓	✗	✗	✗
PS-3	The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	✓	✓	✓	✗	✗
PS-4	On premises data centres, are protected against external and environmental threats.	✗	✓	✓	✗	✗
	Operational Security					
OS-1	The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	✗	✗	✓	✗	✗
OS-2	The capacities of critical resources such as personnel and IT resources are monitored.	✗	✓	✓	✗	✗
OS-3	Policies are defined that ensure the protection against malware of IT equipment related to the on premises service.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-4	Malware protection is deployed and maintained on systems that provide in the infrastructure.	✓	✓	✓	✗	✗
OS-5	Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	✗	✓	✓	✗	✗
OS-6	The proper execution of data backups is monitored.	✗	✓	✓	✗	✗
OS-7	The proper restoration of data backups is regularly tested.	✗	✓	✓	✗	✗
OS-8	Policies are defined to govern logging and monitoring events on system components under the applicant's responsibility.	✓	✓	✓	✓	✓
OS-9	Policies are defined to govern the management of derived data by the applicant.	✗	✓	✗	✓	✓
OS-10	The security of logging and monitoring data are protected with measures adapted to their specific use.	✓	✓	✓	✓	✓
OS-11	Log data can be unambiguously attributed to an on premises customer.	✗	✓	✗	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-12	Access to the logging and monitoring system components and to their configuration is strictly restricted.	✗	✓	✗	✗	✓
OS-13	Systems for logging and monitoring are themselves monitored for availability.	✗	✗	✓	✗	✓
OS-14	Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	✓	✓	✓	✗	✗
OS-15	The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the on premises service, in accordance with policies for handling vulnerabilities.	✓	✓	✓	✗	✗
OS-16	Incident handling measures are regularly evaluated and improved.	✓	✓	✓	✗	✗
OS-17	System components are hardened to reduce their attack surface and eliminate potential attack vectors.	✓	✓	✓	✗	✗
	Identity, Authentication and Access Control Management					
IAM-1	Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	accesses to information have been duly authorized.					
IAM-2	Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓
IAM-3	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	✓	✓	✗	✗	✓
IAM-4	The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	✓	✓	✗	✗	✓
IAM-5	Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	✓	✓	✗	✗	✓
IAM-6	Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-7	Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	✓	✓	✗	✗	✓
IAM-8	The assets in and around the on premises service are managed in a way that ensure that access restrictions are enforced between different categories of assets	✓	✓	✗	✓	✓
	Cryptography and Key Management					
CKM-1	Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	✓	✓	✗	✓	✗
CKM-2	The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	✓	✗	✗	✓	✗
CKM-3	Appropriate mechanisms for key management are in place to protect the	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	confidentiality, authenticity or integrity of cryptographic keys.					
	Communication Security					
CS-1	The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	✓	✓	✓	✗	✗
CS-2	The establishment of connections within the applicant's network is subject to specific security requirements.	✓	✓	✓	✗	✗
CS-3	The communication flows within the on premises systems, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	✓	✓	✓	✗	✓
CS-4	Cross-network access is restricted and only authorised based on specific security assessments.	✓	✓	✓	✗	✗
CS-5	The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CS-6	A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	✓	✓	✓	✗	✗
	Change and Configuration Management					
CCM-1	Policies and procedures are defined to control changes to information systems.	✓	✓	✓	✗	✓
CCM-2	Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	✓	✓	✓	✗	✗
CCM-3	Changes to the infrastructure are approved before being deployed in the production environment.	✓	✓	✓	✗	✓
CCM-4	Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	✓	✗	✗	✗	✓
	Development of Information Systems					
DIS-1	Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
DIS-2	The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	✓	✓	✓	✗	✗
DIS-3	The development environment takes information security in consideration.	✓	✓	✓	✗	✗
DIS-4	The development environment use logical or physical separation between production environments.	✓	✓	✓	✗	✗
DIS-5	Appropriate measures are taken to identify vulnerabilities introduced in the on premises service during the development process.	✓	✓	✓	✗	✗
DIS-6	Outsourced developments provide similar security guarantees than in-house developments.	✓	✓	✓	✗	✗
	Procurement Management					
PM-1	Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	✓	✓	✓	✗	✗
PM-2	Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PM-3	A centralized directory of suppliers is available to facilitate their control and monitoring.	✓	✗	✗	✓	✗
	Incident Management					
IM-1	A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✓	✗
IM-2	A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✗	✗
IM-3	Security incidents are documented to and reported in a timely manner to customers.	✓	✓	✓	✓	✗
IM-4	Measures are in place to continuously improve the service from experience learned in incidents.	✓	✓	✗	✗	✗
IM-5	Measures are in place to preserve information related to security incidents.	✓	✓	✗	✗	✓
	Business Continuity					
BC-1	Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	continuity-related activities are supported.					
BC-2	Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	✗	✗	✓	✗	✗
BC-3	A business continuity framework including a business continuity plan and associated contingency plans is available.	✗	✗	✓	✗	✗
	Compliance					
CMP-1	The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	✓	✗	✗	✓	✗
CMP-2	Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference of the infrastructure.	✗	✗	✗	✓	✗
CMP-3	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CMP-4	Provide customers with choices about the location of the data and of its processing.	✓	✓	✓	✓	✗
CMP-5	Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	✓	✗	✗	✓	✗
CMP-6	The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	✓	✗	✗	✓	✗
CMP-7	Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

4 Cloud Computing

Cloud Computing refers to the computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet (also defined as "the cloud").

***Note**: * denotes controls that apply only to Cloud Infrastructure Providers. Controls marked with asterisk (*) do not apply to an IDPS that merely uses cloud services.*

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	IDPS General Controls					
GEN-1	The applicant communicates information about the system design to the customers or users of the service.	✓	✓	✓	✓	✓
GEN-2	The applicant communicates the design documentation of the system to customers or users of the service.	✓	✓	✓	✓	✓
GEN-3	The applicant implements the system in line with the Blueprint submitted to the Authority.	✓	✓	✓	✓	✓
	Organisation of Information Security					
OIS-1-CLD	The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units,	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	locations and processes with respect to its infrastructure.					
OIS-2-CLD	Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	✓	✓	✓	✓	✓
OIS-3	The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	✓	✓	✓	✗	✗
OIS-4	Information security is considered in project management, regardless of the nature of the project.	✓	✓	✓	✓	✗
	Information Security Policies					
ISP-1	The top management of the applicant has adopted an information security policy and communicated it to internal	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	and external employees as well as customers.					
ISP-2	Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	✓	✓	✓	✓	✓
ISP-3	Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	✓	✓	✓	✓	✓
	Information Policies					
IP-1	Information handling policies and procedures are documented to ensure information protection.	✓	✗	✗	✓	✗
IP-2	Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	✓	✗	✗	✓	✗
IP-3	Information discovery capabilities are in place for both scanning internal unstructured and structured data.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IP-4	DLP technologies should be configured monitor and restrict external file transfers.	✓	✗	✗	✓	✗
IP-5	The organisation shall manage the inventory of its sensitive data and data owners.	✓	✗	✗	✓	✗
	Risk Management					
RM-1	Risk management policies and procedures are documented and communicated to stakeholders	✓	✓	✓	✓	✗
RM-2	Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	✓	✓	✓	✓	✗
RM-3	Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	✓	✓	✓	✓	✗
	Human Resources					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-1	The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	✓	✓	✓	✓	✓
HR-2	The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-3	The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant used to provide the service in the production environment.	✓	✓	✓	✓	✓
HR-4	The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-5	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	✓	✓	✓	✓	✓
HR-6	Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	✓	✗	✗	✓	✗
	Asset Management					
AM-1	The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent	✗	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	inventory throughout the asset lifecycle.					
AM-2	Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	✓	✓	✗	✗	✗
AM-3-CLDP	The applicant has an approval process for the use of hardware to be commissioned or decommissioned, which is used to provide the service in the production environment, depending on its intended use and based on the applicable policies and procedures. *	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
AM-4	The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	✓	✓	✗	✗	✗
AM-5	Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	✓	✓	✗	✓	✗
	Physical Security					
PS-1-CLDP	Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system. *	✗	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PS-2	There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	✗	✓	✓	✗	✗
PS-3	The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	✓	✓	✓	✗	✗
PS-5-CLDP	The buildings and premises related to the cloud service provided are divided into zones by security perimeters, depending on the level on information security risk associated to the activities performed and assets stored in these buildings and premises. *	✓	✓	✓	✗	✗
PS-6-CLDP	The premises from which the cloud service operates, and in particular its data centres, are protected against external and environmental threats. *	✗	✓	✓	✗	✗
	Operational Security					
OS-1-CLDP	The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks. *	✗	✗	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-2-CLDP	The capacities of critical resources such as personnel and IT resources are monitored. *	✗	✓	✓	✗	✗
OS-3-CLD	Policies are defined that ensure the protection against malware of IT equipment related to the infrastructure.	✓	✓	✓	✗	✗
OS-4	Malware protection is deployed and maintained on systems that provide in the infrastructure.	✓	✓	✓	✗	✗
OS-5	Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	✗	✓	✓	✗	✗
OS-6	The proper execution of data backups is monitored.	✗	✓	✓	✗	✗
OS-7	The proper restoration of data backups is regularly tested.	✗	✓	✓	✗	✗
OS-8	Policies are defined to govern logging and monitoring events on system components under the applicant's responsibility.	✓	✓	✓	✓	✓
OS-9	Policies are defined to govern the management of derived data by the applicant.	✗	✓	✗	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-10	The security of logging and monitoring data are protected with measures adapted to their specific use.	✓	✓	✓	✓	✓
OS-11-CLDP	Log data can be unambiguously attributed to a CSC. *	✗	✓	✗	✓	✓
OS-12	Access to the logging and monitoring system components and to their configuration is strictly restricted.	✗	✓	✗	✗	✓
OS-13	Systems for logging and monitoring are themselves monitored for availability.	✗	✗	✓	✗	✓
OS-14	Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	✓	✓	✓	✗	✗
OS-15-CLD	The applicant performs on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the service, in accordance with policies for handling vulnerabilities.	✓	✓	✓	✗	✗
OS-16-CLD	Incident handling measures are regularly evaluated and improved.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-17-CLD	System components are hardened to reduce their attack surface and eliminate potential attack vectors.	✓	✓	✓	✗	✗
	Identity, Authentication and Access Control Management					
IAM-1	Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓
IAM-2	Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓
IAM-3	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	✓	✓	✗	✗	✓
IAM-4	The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-5	Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	✓	✓	✗	✗	✓
IAM-6	Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	✓	✓	✗	✗	✓
IAM-7	Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	✓	✓	✗	✗	✓
IAM-8-CLDP	The assets in and around the cloud service are managed in a way that ensure that access restrictions are enforced between different categories of assets *	✓	✓	✗	✓	✓
	Cryptography and Key Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CKM-1	Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	✓	✓	✗	✓	✗
CKM-2-CLDP	The applicant has established procedures and technical safeguards to prevent the disclosure of cloud customers' data during storage *	✓	✗	✗	✓	✗
CKM-3	Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	✓	✓	✗	✗	✗
	Communication Security					
CS-1	The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CS-2	The establishment of connections within the applicant's network is subject to specific security requirements.	✓	✓	✓	✗	✗
CS-3-CLD	The communication flows within the cloud, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	✓	✓	✓	✗	✓
CS-4	Cross-network access is restricted and only authorised based on specific security assessments.	✓	✓	✓	✗	✗
CS-5-CLDP	The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.*	✓	✓	✗	✗	✗
CS-6-CLDP	A map of the information systems is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.*	✓	✓	✓	✗	✗
	Portability and Interoperability					
PI-1-CLDP	Inbound and outbound interfaces to/from the cloud service are	✓	✗	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	documented for access from other cloud services or IT systems *					
PI-2-CLDP	Contractual agreements define adequate information with regard to the migration of data following the termination of the contractual relationship. *	✓	✗	✓	✓	✗
PI-3-CLDP	Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems. *	✓	✗	✗	✓	✗
	Change and Configuration Management					
CCM-1	Policies and procedures are defined to control changes to information systems.	✓	✓	✓	✗	✓
CCM-2	Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	✓	✓	✓	✗	✗
CCM-3	Changes to the infrastructure are approved before being deployed in the production environment.	✓	✓	✓	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CCM-4	Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	✓	✗	✗	✗	✓
	Development of Information Systems					
DIS-1	Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	✓	✓	✓	✗	✗
DIS-2	The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	✓	✓	✓	✗	✗
DIS-3	The development environment takes information security in consideration.	✓	✓	✓	✗	✗
DIS-4	The development environment use logical or physical separation between production environments.	✓	✓	✓	✗	✗
DIS-5-CLDP	Appropriate measures are taken to identify vulnerabilities introduced in the cloud service during the development process. *	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
DIS-6	Outsourced developments provide similar security guarantees than in-house developments.	✓	✓	✓	✗	✗
	Procurement Management					
PM-1	Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	✓	✓	✓	✗	✗
PM-2	Vend+B100ors and third parties of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	✓	✓	✓	✓	✗
PM-3	A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	✓	✗	✗	✓	✗
	Incident Management					
IM-1	A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✓	✗
IM-2	A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IM-3	Security incidents are documented to and reported in a timely manner to customers.	✓	✓	✓	✓	✗
IM-4	Measures are in place to continuously improve the service from experience learned in incidents.	✓	✓	✗	✗	✗
IM-5	Measures are in place to preserve information related to security incidents.	✓	✓	✗	✗	✓
	Business Continuity					
BC-1	Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	✓	✓	✓	✗	✗
BC-2	Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	✗	✗	✓	✗	✗
BC-3	A business continuity framework including a business continuity plan and associated contingency plans is available.	✗	✗	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	Compliance					
CMP-1	The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	✓	✗	✗	✓	✗
CMP-2	Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference of the infrastructure.	✗	✗	✗	✓	✗
CMP-3	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	✓	✓	✓	✓	✗
CMP-4	Provide customers with choices about the location of the data and of its processing.	✓	✓	✓	✓	✗
CMP-5	Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CMP-6	The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	✓	✗	✗	✓	✗
CMP-7	Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	✓	✗	✗	✓	✗
	User Documentation					
UD-1-CLDP	Provide information to assist the customer in the secure configuration, installation and use of the cloud service. *	✓	✓	✓	✓	✗
UD-2-CLDP	Provide information to assist the customer in the secure configuration, installation and use of the cloud service *	✓	✓	✓	✗	✗
UD-3-CLDP	Provide transparent information about the location of the data and of its processing	✓	✓	✗	✓	✗
UD-4-CLDP	Provide a rationale for the assurance level target by the cloud service. *	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
UD-5-CLDP	Provide the information required by customers that want to use the applicant as subservice organization for the cloud infrastructure. *	✗	✗	✗	✓	✗
	Dealing with Investigation Requests from Government Agencies					
IRGA-1-CLDP	Cloud customers are kept informed of ongoing investigations if legally permitted. *	✗	✗	✗	✓	✓
IRGA-2-CLDP	Investigators only have access to the data required for their investigation after validation of the legality of their request. *	✗	✗	✗	✓	✓
	Product Safety and Security					
PSS-11-CLDP	Cloud customers have access to sufficient information about the cloud service through error handling and logging mechanisms *	✗	✓	✗	✗	✓
PSS-2-CLDP	A suitable session management is used to protect confidentiality, availability, integrity and authenticity during interactions with the cloud service. *	✓	✓	✓	✗	✗
PSS-3-CLDP	Software-defined networking is only used if the cloud user data is protected by appropriate measures. *	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PSS-4 -CLDP	Services for providing and managing virtual machines and containers to customers include appropriate protection measures. *	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

5 Artificial Intelligence

Artificial Intelligence (AI) refers to that technology that leverages computers and machines to mimics the problem-solving, decision-making, and cognitive capabilities of the human mind.

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	IDPS General Controls					
GEN-1	The applicant communicates information about the system design to the customers or users of the service.	✓	✓	✓	✓	✓
GEN-2	The applicant communicates the design documentation of the system to customers or users of the service.	✓	✓	✓	✓	✓
GEN-3	The applicant implements the system in line with the Blueprint submitted to the Authority.	✓	✓	✓	✓	✓
GEN-4-AI	The applicant has a formalised plan to fulfil the requirements of the EU AI Act once it comes into force.	✓	✓	✓	✓	✓
	Asset Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
AM-1-AI	The applicant has established procedures for inventorying assets, including all AI assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	✗	✓	✓	✗	✗
AM-2	Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	✓	✓	✗	✗	✗
AM-3	The applicant has an approval process for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
AM-4	The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	✓	✓	✗	✗	✗
AM-5-AI	Assets are classified and, if possible, labelled. Classification and labelling of an AI asset reflect the protection needs of the information it processes, stores, or transmits.	✓	✓	✗	✓	✗
	Business Continuity					
BC-1	Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
BC-2-AI	Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the AI model.	✗	✗	✓	✗	✗
BC-3	A business continuity framework including a business continuity plan and associated contingency plans is available.	✗	✗	✓	✗	✗
	Change and Configuration Management					
CCM-1-AI	Policies and procedures are defined to control changes to AI systems.	✓	✓	✓	✗	✓
CCM-2-AI	Changes to the AI components are tested before deployment to minimize the risks of failure upon implementation.	✓	✓	✓	✗	✗
CCM-3-AI	Changes to the AI systems are approved before being deployed in the production environment.	✓	✓	✓	✗	✓
CCM-4-AI	Changes to the AI systems are performed through authorized accounts and traceable to the person or system component who initiated them.	✓	✗	✗	✗	✓
	Communication Security					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CS-1	The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	✓	✓	✓	✗	✗
CS-2	The establishment of connections within the internal network is subject to specific security requirements.	✓	✓	✓	✗	✗
CS-3-AI	The communication flows within the AI systems, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	✓	✓	✓	✗	✓
CS-4	Cross-network access is restricted and only authorised based on specific security assessments.	✓	✓	✓	✗	✗
CS-5	The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CS-6-AI	A map of the AI system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	✓	✓	✓	✗	✗
	Compliance					
CMP-2-AI	Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the AI systems' functionalities.	✗	✗	✗	✓	✗
CMP-3	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	✓	✓	✓	✓	✗
CMP-5	Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CMP-6	The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	✓	✗	✗	✓	✗
CMP-7	Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	✓	✗	✗	✓	✗
CMP-8-AI	Appropriate technical controls are implemented to ensure compliance with the Ethical & Trustworthy AI Framework.	✗	✗	✗	✗	✗
	Cryptography and Key Management					
CKM-1	Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	✓	✓	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CKM-2	The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	✓	✗	✗	✓	✗
CKM-3	Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	✓	✓	✗	✗	✗
	Development of Information Systems					
DIS-1-AI	Policies are defined to define technical and organisational measures for the development of AI systems throughout their lifecycle.	✓	✓	✓	✗	✗
DIS-3	The development environment takes information security in consideration.	✓	✓	✓	✗	✗
DIS-4-AI	The development environment use logical or physical separation between production of AI environments.	✓	✓	✓	✗	✗
DIS-5-AI	Appropriate measures are taken to identify vulnerabilities introduced in the AI service during the development process.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
DIS-6-AI	Outsourced developments provide similar security guarantees than in-house developments.	✓	✓	✓	✗	✗
	Human Resources					
HR-1	The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	✓	✓	✓	✓	✓
HR-2	The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-3	The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant used to provide the service in the production environment.	✓	✓	✓	✓	✓
HR-4	The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-5	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	✓	✓	✓	✓	✓
HR-6	Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-7-AI	The applicant operates an awareness and training programa in place that the appropriate teams and individuals are adequately empowered trained and accountable for managing the risks of AI systems.	✓	✓	✓	✓	✓
	Identity, Authentication and Access Control Management					
IAM-1-AI	Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized. AI applications shall comply with identity management, authentication, and access control policies.	✓	✓	✗	✗	✓
IAM-2	Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-3	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	✓	✓	✗	✗	✓
IAM-4	The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	✓	✓	✗	✗	✓
IAM-5	Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	✓	✓	✗	✗	✓
IAM-6	Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	✓	✓	✗	✗	✓
IAM-7	Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	✓	✓	✗	✗	✓
	Incident Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IM-1	A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✓	✗
IM-2-AI	A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner, including all AI components.	✓	✓	✓	✗	✗
IM-3	Security incidents are documented to and reported in a timely manner to customers.	✓	✓	✓	✓	✗
IM-4	Measures are in place to continuously improve the service from experience learned in incidents.	✓	✓	✗	✗	✗
IM-5	Measures are in place to preserve information related to security incidents.	✓	✓	✗	✗	✓
	Information Protection					
IP-1	Information handling policies and procedures are documented to ensure information protection.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IP-2	Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	✓	✗	✗	✓	✗
IP-3	Information discovery capabilities are in place for both scanning internal unstructured and structured data.	✓	✗	✗	✓	✗
IP-4	DLP technologies should be configured monitor and restrict external file transfers.	✓	✗	✗	✓	✗
IP-5	The organisation shall manage the inventory of its sensitive data and data owners	✓	✗	✗	✓	✗
IP-6-AI	Controls are in place to ensure the quality of AI data.	✓	✓	✗	✗	✗
	Information Security Policies					
ISP-1	The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
ISP-2-AI	Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner. AI applications shall comply with information security policies and are integrated to security operations processes.	✓	✓	✓	✓	✓
ISP-3	Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	✓	✓	✓	✓	✓
	Operational Security					
OS-1	The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	✗	✗	✓	✗	✗
OS-2	The capacities of critical resources such as personnel and IT resources are monitored.	✗	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-3-AI	Policies are defined that ensure the protection against malware of IT equipment related to the AI service.	✓	✓	✓	✗	✗
OS-4	Malware protection is deployed and maintained on systems that provide in the infrastructure.	✓	✓	✓	✗	✗
OS-5	Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	✗	✓	✓	✗	✗
OS-6	The proper execution of data backups is monitored.	✗	✓	✓	✗	✗
OS-7	The proper restoration of data backups is regularly tested.	✗	✓	✓	✗	✗
OS-8-AI	Policies are defined to govern logging and monitoring events on AI components.	✓	✓	✓	✓	✓
OS-9-AI	Policies are defined to govern the management of data in the machine learning algorithms.	✗	✓	✗	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-10-AI	The security of logging and monitoring of AI data are protected with measures adapted to their specific use.	✓	✓	✓	✓	✓
OS-11-AI	Log data can be unambiguously attributed to a customer.	✗	✓	✗	✓	✓
OS-12	Access to the logging and monitoring system components and to their configuration is strictly restricted.	✗	✓	✗	✗	✓
OS-14-AI	Vulnerabilities in the system components used in the AI components are identified and addressed in a timely manner.	✓	✓	✓	✗	✗
OS-15-AI	The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the AI service, in accordance with policies for handling vulnerabilities.	✓	✓	✓	✗	✗
OS-16	Incident handling measures are regularly evaluated and improved.	✓	✓	✓	✗	✗
OS-17-AI	AI system components are hardened to reduce their attack surface and eliminate potential attack vectors.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-18-AI	Documentation of AI core functionalities in Technical Blueprint	✓	✓	✓	✗	✗
	Organisation of Information Security					
OIS-1	The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	✓	✓	✓	✓	✓
OIS-2-AI	Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the AI infrastructure.	✓	✓	✓	✓	✓
OIS-3-AI	The applicant stays informed about current threats, including AI specific threats, and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OIS-4-AI	Information security, including AI-specific information security is considered in project management, regardless of the nature of the project.	✓	✓	✓	✓	✗
	Physical Security					
PS-1	Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	✗	✓	✗	✗	✓
PS-2	There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	✗	✓	✗	✗	✗
PS-3	The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PS-4-AI	Data centres related to the AI service, are protected against external and environmental threats.	✗	✓	✓	✗	✗
	Procurement Management					
PM-1	Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	✓	✓	✓	✗	✗
PM-2-AI	Vendors and third parties of the applicant undergo a risk assessment to determine the security needs related to the AI service.	✓	✓	✓	✓	✗
PM-3	A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	✓	✗	✗	✓	✗
	Risk Management					
RM-1	Risk management policies and procedures are documented and communicated to stakeholders	✓	✓	✓	✓	✗
RM-2-AI	Risk assessment-related policies and procedures are implemented on the AI service.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
RM-3	Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	✓	✓	✓	✓	✗
RM-4-AI	The applicant should regularly receive feedback from appropriate subject matter experts with respect to the performance, interended use and trustworthiness of the AI systems.	✗	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

6 Internet of Things

The Internet of Things (IoT) refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	IDPS General Controls					
GEN-1	The applicant communicates information about the system design to the customers or users of the service.	✓	✓	✓	✓	✓
GEN-2	The applicant communicates the design documentation of the system to customers or users of the service.	✓	✓	✓	✓	✓
GEN-3	The applicant imlemenents the system in line with the Blueprint submitted to the Authority.	✓	✓	✓	✓	✓
	Organisation of Information Security					
OIS-1	The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OIS-2-IOT	Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the IoT devices.	✓	✓	✓	✓	✓
OIS-3	The applicant stays informed about current threats and vulnerabilities, including IoT specific vulnerabilities, by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	✓	✓	✓	✗	✗
OIS-4	Information security is considered in project management, regardless of the nature of the project.	✓	✓	✓	✓	✗
	Information Security Policies					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
ISP-1	The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	✓	✓	✓	✓	✓
ISP-2	Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	✓	✓	✓	✓	✓
ISP-3	Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	✓	✓	✓	✓	✓
	Information Protection					
IP-1	Information handling policies and procedures are documented to ensure information protection.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IP-2	Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	✓	✗	✗	✓	✗
IP-3	Information discovery capabilities are in place for both scanning internal unstructured and structured data.	✓	✗	✗	✓	✗
IP-4	DLP technologies should be configured monitor and restrict external file transfers.	✓	✗	✗	✓	✗
IP-5	The organisation shall manage the inventory of its sensitive data and data owners	✓	✗	✗	✓	✗
	Risk Management					
RM-1	Risk management policies and procedures are documented and communicated to stakeholders	✓	✓	✓	✓	✗
RM-2-IOT	Risk assessment-related policies and procedures are implemented on the entire perimeter of the service, including IoT devices.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
RM-3	Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	✓	✓	✓	✓	✗
	Human Resources					
HR-1	The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-2	The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	✓	✓	✓	✓	✓
HR-3	The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant used to provide the service in the production environment.	✓	✓	✓	✓	✓
HR-4	The applicant operates an IoT security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-5	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	✓	✓	✓	✓	✓
HR-6	Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	✓	✗	✗	✓	✗
	Asset Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
AM-1	The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	✗	✓	✓	✗	✗
AM-2	Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	✓	✓	✗	✗	✗
AM-3	The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	✓	✓	✗	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
AM-4	The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	✓	✓	✗	✗	✗
AM-5-IOT	IoT assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	✓	✓	✗	✓	✗
AM-6-IOT	End-of-Life handling process is established for the IOT devices.	✓	✓	✗	✓	✗
	Physical Security					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PS-1	Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	✗	✓	✗	✗	✓
PS-2	There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	✗	✓	✗	✗	✗
PS-3	The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	✓	✓	✓	✗	✗
PS-4	Data centres, are protected against external and environmental threats.	✗	✓	✓	✗	✗
	Operational Security					
OS-1-IOT	The capacities of critical resources such as personnel and IoT devices and resources are planned in order to avoid possible capacity bottlenecks.	✗	✗	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-2-IOT	The capacities of critical resources such as personnel and IoT devices and resources are monitored.	✗	✓	✓	✗	✗
OS-3-IOT	Policies are defined that ensure the protection against malware of IoT devices and resources related.	✓	✓	✓	✗	✗
OS-4-IOT	Malware protection is deployed and maintained on IoT devices.	✓	✓	✓	✗	✗
OS-5	Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	✗	✓	✓	✗	✗
OS-6	The proper execution of data backups is monitored.	✗	✓	✓	✗	✗
OS-7	The proper restoration of data backups is regularly tested.	✗	✓	✓	✗	✗
OS-8-IOT	Policies are defined to govern logging and monitoring events on IoT components.	✓	✓	✓	✓	✓
OS-9	Policies are defined to govern the management of derived data by the applicant.	✗	✓	✗	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-10	The security of logging and monitoring data are protected with measures adapted to their specific use.	✓	✓	✓	✓	✓
OS-11	Log data can be unambiguously attributed to a customer.	✗	✓	✗	✓	✓
OS-12	Access to the logging and monitoring system components and to their configuration is strictly restricted.	✗	✓	✗	✗	✓
OS-13	Systems for logging and monitoring are themselves monitored for availability.	✗	✗	✓	✗	✓
OS-14-IOT	Vulnerabilities in the IoT devices and resources are identified and addressed in a timely manner.	✓	✓	✓	✗	✗
OS-15-IOT	The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the IoT devices and resources in accordance with policies for handling vulnerabilities.	✓	✓	✓	✗	✗
OS-16	Incident handling measures are regularly evaluated and improved.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-17-IOT	IoT devices and resources are hardened to reduce their attack surface and eliminate potential attack vectors.	✓	✓	✓	✗	✗
OS-19-IOT	The configuration of the IoT devices' software can be changed, and such changes can be performed by authorized entities only.	✓	✓	✓	✗	✗
OS-20-IOT	The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	✓	✓	✓	✗	✗
OS-21-IOT	A security update policy for IoT devices with a constrained power source is in place.	✗	✓	✓	✗	✗
OS-22-IOT	A Security by Design approach has been estabilshed for the IoT devices.	✓	✓	✓	✓	✗
	Identity, Authentication and Access Control Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-1	Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓
IAM-2	Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓
IAM-3	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	✓	✓	✗	✗	✓
IAM-4	The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-5	Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	✓	✓	✗	✗	✓
IAM-6	Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	✓	✓	✗	✗	✓
IAM-7	Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	✓	✓	✗	✗	✓
IAM-8-IOT	The assets in and around the IoT devices and resources are managed in a way that ensure that access restrictions are enforced between different categories of assets	✓	✓	✗	✓	✓
IAM-9-IOT	A password policy with minimum security requirements is established for the IoT devices.	✓	✓	✗	✓	✗
	Cryptography and Key Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CKM-1	Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	✓	✓	✗	✓	✗
CKM-2-IOT	The applicant has established procedures and technical safeguards to prevent the disclosure of IoT devices' customers' data during storage.	✓	✗	✗	✓	✗
CKM-3	Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	✓	✓	✗	✗	✗
	Communication Security					
CS-1	The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CS-2	The establishment of connections within the applicant's network is subject to specific security requirements.	✓	✓	✓	✗	✗
CS-3-IOT	The communication flows within the IoT devices and resources, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	✓	✓	✓	✗	✓
CS-4	Cross-network access is restricted and only authorised based on specific security assessments.	✓	✓	✓	✗	✗
CS-5	The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	✓	✓	✗	✗	✗
CS-6	A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	✓	✓	✓	✗	✗
	Change and Configuration Management					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CCM-1-IOT	Policies and procedures are defined to control changes to IoT devices.	✓	✓	✓	✗	✓
CCM-2	Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	✓	✓	✓	✗	✗
CCM-3	Changes to the infrastructure are approved before being deployed in the production environment.	✓	✓	✓	✗	✓
CCM-4	Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	✓	✗	✗	✗	✓
	Development of Information Systems					
DIS-1	Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	✓	✓	✓	✗	✗
DIS-2	The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
DIS-3	The development environment takes information security in consideration.	✓	✓	✓	✗	✗
DIS-4	The development environment use logical or physical separation between production environments.	✓	✓	✓	✗	✗
DIS-5-IOT	Appropriate measures are taken to identify vulnerabilities introduced in the IoT device during the development process.	✓	✓	✓	✗	✗
DIS-6	Outsourced developments provide similar security guarantees than in-house developments.	✓	✓	✓	✗	✗
DIS-7-IOT	A comprehensive test plan for the IoT devices software is established.	✓	✓	✗	✓	✗
DIS-8-IOT	IoT application protocols should be configured securely and update default configurations.	✓	✓	✗	✗	✗
	Procurement Management					
PM-1	Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PM-2	Vendors and third parties of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	✓	✓	✓	✓	✗
PM-3	A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	✓	✗	✗	✓	✗
	Incident Management					
IM-1	A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✓	✗
IM-2	A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✗	✗
IM-3	Security incidents are documented to and reported in a timely manner to customers.	✓	✓	✓	✓	✗
IM-4	Measures are in place to continuously improve the service from experience learned in incidents.	✓	✓	✗	✗	✗
IM-5	Measures are in place to preserve information related to security incidents.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IM-6-IOT	Threat modeling is performance for the whole IoT supply chain.	✓	✓	✗	✗	✗
	Business Continuity					
BC-1	Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	✓	✓	✓	✗	✗
BC-2	Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	✗	✗	✓	✗	✗
BC-3	A business continuity framework including a business continuity plan and associated contingency plans is available.	✗	✗	✓	✗	✗
	Compliance					
CMP-1	The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CMP-2-IOT	Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the IoT devices software.	✗	✗	✗	✓	✗
CMP-3	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	✓	✓	✓	✓	✗
CMP-4	Provide customers with choices about the location of the data and of its processing.	✓	✓	✓	✓	✗
CMP-5	Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CMP-6	The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	✓	✗	✗	✓	✗
CMP-7	Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	✓	✗	✗	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

7 Distributed Ledger Technology

Distributed Ledger Technology (or Blockchain) refers to a distributed technology that maintains a continuously growing list of ordered records, called blocks, including blockchain and smart contracts. A DLT is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
	IDPS General Controls					
GEN-1	The applicant communicates information about the system design to the customers or users of the service.	✓	✓	✓	✓	✓
GEN-2	The applicant communicates the design documentation of the system to customers or users of the service.	✓	✓	✓	✓	✓
GEN-3	The applicant implements the system in line with the Blueprint submitted to the Authority.	✓	✓	✓	✓	✓
	Identity, Authentication and Access Control Management					
IAM-1	Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-2	Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	✓	✓	✗	✗	✓
IAM-3	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	✓	✓	✗	✗	✓
IAM-4	The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	✓	✓	✗	✗	✓
IAM-5	Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	✓	✓	✗	✗	✓
IAM-6	Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	✓	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IAM-7	Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	✓	✓	✗	✗	✓
	Compliance					
CMP-1-DLT	The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the blockchain service are defined and documented.	✓	✗	✗	✓	✗
CMP-2-DLT	Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the blockchain service.	✗	✗	✗	✓	✗
CMP-3	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CMP-4-DLT	Provide vendors, third parties or customers with choices about the location of the data and of its processing.	✓	✓	✓	✓	✗
CMP-5	Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	✓	✗	✗	✓	✗
CMP-6	The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	✓	✗	✗	✓	✗
CMP-7	Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	✓	✗	✗	✓	✗
	Operational Security					
OS-3-DLT	Policies are defined that ensure the protection against malware attacks in the DLT infrastructure.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OS-5	Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	✗	✓	✓	✗	✗
OS-6	The proper execution of data backups is monitored.	✗	✓	✓	✗	✗
OS-7	The proper restoration of data backups is regularly tested.	✗	✓	✓	✗	✗
OS-8-DLT	Policies are defined to govern logging and monitoring events on DLT components.	✓	✓	✓	✓	✓
OS-14	Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	✓	✓	✓	✗	✗
OS-23-DLT	Appropriate safeguards to ensure processing integrity are in place.	✗	✗	✗	✗	✗
	Physical Security					
PS-1	Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	✗	✓	✗	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PS-2	There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	✗	✓	✗	✗	✗
PS-3	The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	✓	✓	✓	✗	✗
PS-4	On premises data centres, are protected against external and environmental threats.	✗	✓	✓	✗	✗
	Human Resources					
HR-2	The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	✓	✓	✓	✓	✓
HR-4	The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
HR-5	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	✓	✓	✓	✓	✓
	Change and Configuration Management					
CCM-1-DLT	Policies and procedures are defined to control changes to blockchain services and nodes.	✓	✓	✓	✗	✓
CCM-2-DLT	Changes to the DLT infrastructure are tested before deployment to minimize the risks of failure upon implementation.	✓	✓	✓	✗	✗
CCM-3-DLT	Changes to the DLT infrastructure are approved before being deployed in the production environment.	✓	✓	✓	✗	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CCM-4-DLT	Changes to the blockchain infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	✓	✗	✗	✗	✓
	Information Protection					
IP-1	Information handling policies and procedures are documented to ensure information protection.	✓	✗	✗	✓	✗
IP-2	Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	✓	✗	✗	✓	✗
IP-3	Information discovery capabilities are in place for both scanning internal unstructured and structured data.	✓	✗	✗	✓	✗
IP-5	The organisation shall manage the inventory of its sensitive data and data owners	✓	✗	✗	✓	✗
	Business Continuity					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
BC-1	Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	✓	✓	✓	✗	✗
BC-2-DLT	Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the blockchain infrastructure.	✗	✗	✓	✗	✗
	Incident Management					
IM-1	A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✓	✗
IM-2	A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	✓	✓	✓	✗	✗
IM-3	Security incidents are documented to and reported in a timely manner to customers.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
IM-4-DLT	Measures are in place to continuously improve the DLT service from experience learned in incidents.	✓	✓	✗	✗	✗
IM-5	Measures are in place to preserve information related to security incidents.	✓	✓	✗	✗	✓
	Organisation of Information Security					
OIS-1	The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	✓	✓	✓	✓	✓
OIS-2-DLT	Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of vendor, third party or customer data processed, stored or transmitted in the DLT infrastructure.	✓	✓	✓	✓	✓

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
OIS-3	The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	✓	✓	✓	✗	✗
OIS-4	Information security is considered in project management, regardless of the nature of the project.	✓	✓	✓	✓	✗
	Risk Management					
RM-1	Risk management policies and procedures are documented and communicated to stakeholders	✓	✓	✓	✓	✗
RM-2	Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	✓	✓	✓	✓	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
RM-3	Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	✓	✓	✓	✓	✗
	Development of Information Systems					
DIS-1-DLT	Policies are defined to define technical and organisational measures for the development of DLT infrastructure throughout its lifecycle.	✓	✓	✓	✗	✗
DIS-3	The development environment takes information security in consideration.	✓	✓	✓	✗	✗
DIS-5-DLT	Appropriate measures are taken to identify vulnerabilities introduced in the DLT service during the development process.	✓	✓	✓	✗	✗
	Communication Security					

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
CS-1-DLT	The applicant has implemented appropriate technical safeguards in order to detect and respond to DLT network based attacks as well as to ensure the protection of information and information processing systems.	✓	✓	✓	✗	✗
	Cryptography and Key Management					
CKM-1	Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	✓	✓	✗	✓	✗
CKM-3	Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	✓	✓	✗	✗	✗
	Procurement Management					
PM-1-DLT	Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	✓	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	Control Objective	Confidentiality	Integrity	Availability	Privacy	Accountability
PM-2-DLT	Vendors and third parties of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	✓	✓	✓	✓	✗
PM-3-DLT	A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	✓	✗	✗	✓	✗
	Asset Management					
AM-1	The applicant has established processes for inventorying assets, including all DLT infrastructure components to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	✗	✓	✓	✗	✗

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt