# Vocabulary

Reference: GMICT X 0003 Publication: 29 May 2021

Version: 12.0

## Purpose

Establishes standard vocabulary used across all GMICT Policy documents.

## Scope

Terms contained in GMICT Policy documents.

## Terms

All the Terms highlighted in bold text which are found in the Definitions of other Terms are themselves also defined.

All the Terms having a shaded background have an additional graphical representation in the Appendix.

### Government Structure

| Term | Definition |
|---|---|
| **Government** | The Government of Malta. |
| **Public Administration** | The Government of Malta including its ministries and departments, and the agencies, government entities, commissions and boards referred to in the Public Administration Act. |
| **Public Sector** | Same as **Public Administration**. |
| **Public Service** | All Ministries and **Departments**. |
| **Department** | An organisation in the **Public Service** other than a Ministry. |
| **Entity** | Authorities, Corporations, Agencies and commercial **Public Sector** entities:<br>• in which the Government has a majority shareholding<br>• that are not listed on the stock exchange<br>**Entities** also comprise Foundations and Local Councils. |
| **Government Employee** | Any **Public Sector** employee. |

| Term | Definition |
|---|---|
| **GMICT Policy** | All Government of Malta ICT Policies, Directives, Standards, Procedures and associated publications, which can be found at **http://ictpolicies.gov.mt**. |

## ICT Governance Roles

| Term | Definition |
|---|---|
| **Agent** | A trusted organisation that has the mandate by **Government** to provide Information and Communications Technology and related services.<br>This role is fulfilled by the Malta Information Technology Agency (MITA). |
| **Agent's Portal** | Refers to http://mita.gov.mt |
| **Assessor** | A trusted role that has the mandate by Government to enforce the provisions of established **GMICT Policy**. |
| **CIO** | Refers to Ministry CIO and to the equivalent role(s) responsible for ICT within a Public Sector entity. |
| **CIO Council** | A body set up for discussion, expression of general ideas or concerns relating to all operational ICT matters across **Government**. |
| **GMICT Compliance** | The goal that the Public Sector aspires to in its efforts to ensure that personnel are aware of, and take steps to comply to, relevant **GMICT Policy** requirements. |
| **GMICT Compliance function** | Refer to **Assessor**. |
| **InfoSec Authority** | Identifies security measures in order to protect classified information that is being processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional. |
| **InfoSec Council** | A body set up for discussion, expression of general ideas or concerns relating to information security matters across **Government**. |
| **Regulator** | A trusted role that has the mandate by **Government** to issue policies regarding Information and Communications Technology and related services.<br>This role is fulfilled by the Malta Information Technology Agency (MITA). |

## MAGNET (Malta Government Network)

| Term | Definition |
|---|---|
| **ICT device** | ICT hardware, software and/or their combination employed for processing, input and output and/or storage. The relevant GMICT Policies shall be applicable to a Government ICT device in both **trusted** and **untrusted networks**. |
| **Trusted ICT device** | **An ICT device** is considered by the Agent to be trusted if it is managed by the Agent in its entirety, in terms of, but not limited to:<br>• Device hardening<br>• Patches for Corporate Software<br>• Endpoint security, where applicable.<br>Other scenarios may be evaluated on a case by case basis. |
| **Untrusted ICT device** | **An ICT device** which is not trusted. |
| **Trusted Network** | A network of **ICT devices** that:<br>i) Are considered as **trusted** by the Agent<br>ii) Are not directly connected to an **untrusted network** |
| **Untrusted Network** | A network of **ICT devices** that:<br>i) are considered as **untrusted** by the Agent<br>ii) May require, subject to appropriate evaluation, a degree of autonomy, as agreed with the Agent. |
| **MAGNET (Malta Government Network)** | A Network connecting all Government **ICT devices**.<br>The MAGNET is logically made up of:<br>• Trusted Network<br>• Untrusted Network |

| Term | Definition |
|---|---|
| **Segregated Hosting Environment (SHE)** | An environment (physical, virtual or otherwise) enabling appropriate degrees of segregation, isolation and autonomy from adjacent constituents, within which a **Solution** is operated.<br><br>Access to any resources external to the SHE (including databases, directory services etc. etc), should be governed by **adapters**. No direct access from the SHE to a target resource is normally allowed, unless specific circumstances mandate otherwise.<br><br>Where applicable, SHEs will have a pre-defined set of controlled mechanisms, supported by accompanying policies, which allow and ensure the necessary level of auditing, logging, session recording, monitoring, change management, patch management, etc.<br><br>Failure to ensure any appropriate visibility and proof that these controls mechanism are in place and effective, as well as the non-adherence to any applicable policies will trigger a process where pre-established control and/or total service immobilisation procedures may be considered. |

## 1.1 General Definitions

| Term | Definition | Context |
|---|---|---|
| **Account** | The primary means of implementing a role-based assignment of permissions, rights and privileges in Systems. | *Information Security* |
| **Account Holder** | A person authorised to use electronic Services within the **Public Sector**.<br>Account Holders consist of all:<br>• **Public Sector** employees<br>• **Third Parties** that have access to or make use of **Government Assets** and/or Services | *All* |
| **Accredited Datasets** | Commonly used, sharable and/or reusable data sets that have been endorsed by the **Regulator** to support the delivery of **Public services**. | *Interoperability* |
| **Adapter** | A **technical** artefact that allows the interaction between two distinct systems, using standard and secure **protocols**, **specifically**:<br>• DNS<br>• HTTP(S)<br>• FTP(S)<br>• SSH<br>• RDP | *Interoperability*<br>*Connectivity to MAGNET*<br>*Open Source Software* |
| **Application** | See **Information System**. | *Applications* |
| **Application Code** | Code and mark-up for the purposes of generating **Dynamic Content**. | *Web Interface* |
| **Architecture** | The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. | *Enterprise Architecture* |
| **Architecture Assessment** | Refer to **Enterprise Architecture Review** | *Enterprise Architecture* |
| **Architecture Blueprint** | A document that describes the **Solution Architecture** through the documentation of decisions related to the planning and implementation of Business, Application, Data, Technology and Security. | *Enterprise Architecture* |
| **Architecture Roadmap** | A document or a part of a document that defines the transition strategy of an enterprise from the current baseline to the target architecture. It schedules multiple, concurrent, interdependent activities and incremental builds that will evolve the enterprise. | *Enterprise Architecture* |

| Term | Definition | Context |
|---|---|---|
| **Artefact** | Artefacts may consist of, but are not limited to:<br>• **Information System**<br>• Source Code<br>• Software Component, Module or Utility<br>• Database<br>• Hardware<br>• **Network**<br>• Middleware<br>• Operating System<br>• Documentation<br>• Policies and Procedures | *All* |
| **As-is Architecture** | Refer to **Baseline Architecture**. | *Enterprise Architecture* |
| **Asset** | Any **Artefact** that has an owner. | *All* |
| **Audit Data** | The minimum data that uniquely identify events in time, to enable the reconstruction and examination of their sequence. It is not data that is used for technical day-to-day troubleshooting purposes. | *Compliance Audit* |
| **Auditee** | Any individual, organisation, process, system, project and/or service being audited. | *Compliance Audit* |
| **Auditing** | A systematic process by which an **Auditor** objectively obtains and evaluates **Audit Data** regarding an **Auditee** for the purpose of forming an opinion about and reporting on the degree of compliance against established requirements.<br>Within the Public Sector, this shall be carried out with the **CIO** (or his/her representative). | *Compliance Audit* |
| **Auditor** | A competent, independent and objective person(s) responsible to execute an audit, document the findings in an audit report and follow up on the implementation of corrective actions according to agreed timeframes. | *Compliance Audit* |
| **Authentication** | A way to ascertain that a user is who claims to be.<br>*(Adapted from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods )* | *Information Security* |
| **Author** | The creator of work eligible for protection by Intellectual Property Rights. | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Availability** | Ability of an IT service or other configuration item to perform its agreed function when required. It is determined by reliability, maintainability, serviceability, performance and security.<br>*(Adapted from ITIL service Design, ITIL glossary and abbreviations, Crown Copyright 2011, www.itil-officialsite.com)* | *Information Security* |
| **Baseline Architecture** | The set of documented functional packages that portray the existing enterprise, the current business practices, and technical infrastructure. Commonly referred to as the **"as-is" architecture**. | *Enterprise Architecture* |
| **Baseline Profile** | A specification of Internet **Web Sites** which are not related to the Government's business requirements and updated by the **Assessor**. | *Web Filtering* |
| **Body** | The part of the **Content** that the originator explicitly communicates.<br>*(MSA ISO/IEC 2382-32:2002)* | *E-mail* |
| **Building Block** | A group of functional components defined to meet specific business needs. The way in which functionality, products, and custom developments are assembled into building blocks will vary between individual architectures. | *Enterprise Architecture, Interoperability* |
| **Business Role** | The generic business title that is used to identify the list of duties and responsibilities together with the authority required for the performance of such functions. Each **Business Role** will be clearly identified within an existing **Organisational Unit**. | *Data, Interoperability* |
| **Client-server Application** | An **Application** consisting of:<br>• a client program serving as the user interface, installed on each user's personal computer<br>• a server-side program and/or database | *Applications* |
| **Classified** | An aggregate term for **Security Marking**s *Restricted* and above. | |
| **Compliance Auditing** | Refer to **Auditing**. | *Compliance* |
| **Confidentiality** | A security principle that requires that data should only be accessed by authorised persons.<br>*Adapted from ITIL service Design, ITIL glossary and abbreviations, Crown Copyright 2011, www.itil-officialsite.com)* | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Configuration Item (CI)** | Any component that needs to be managed in order to deliver an IT service. Information about each **CI** is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its lifecycle by Configuration Management. **CIs** are under the control of Change Management. **CIs** typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and Service Level Agreements.<br>*(ITIL v3, Glossary of Terms, Definitions and Acronyms)* | |
| **Configuration Management Database (CMDB)** | A database used to store configuration records throughout their lifecycle. The Configuration Management System maintains one or more **CMDBs**, and each **CMDB** stores attributes of **Configuration Items**, and relationships with other **Configuration Items**.<br>*(ITIL v3, Glossary of Terms, Definitions and Acronyms)* | |
| **Content** | The **Body** of an **E-mail Message** and any **Attachments**. | *E-mail* |
| **Corporately approved** | Approved by an appropriate **Government** function, in line with documented procedures. | *Information Security* |
| **Corporately governed/managed** | Governed/managed by an appropriate **Government** function, in line with documented procedures. | *Information Security* |
| **Corporate Account** | An account that is governed/managed by the **Agent**. | |
| **Corporate Infrastructure** | The infrastructure that is governed/managed by the **Agent**. | *Information Security* |
| **Counterfeit E-mail** | An **E-mail Message** that makes use of or contains invalid or forged **Envelope Information**, invalid or non-existent domain names or other means of deceptive addressing. | *E-mail* |
| **Data Governance Council** | A forum for all data governance related issues, recommendations and decisions. | |
| **Data Owner** | The role that is accountable for the following aspects of data:<br>• Processing (collection, storage, transmission, retention, backup, archival and disposal)<br>• Security<br>• Access, data-sharing and reuse<br>• Quality | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Data that has a continuing value to Government** | This includes data that the Government produces, but also data that is not necessarily created or generated by the Government, but that may have come into the Government's possession in the execution of Government business, and that is still of value to Government. | *Information Security* |
| **Delegate** | An individual authorised by the **Account Holder** to access his/her E-mail account, using software permissions or a delegate password. The degree of access of the delegate must be under the control of the **Account Holder**. | *E-mail* |
| **Disaster** | Occurrence or the likely occurrence of one or more events which, either separately or cumulatively, mean that a Solution and/or services, or a material part of the services, are or will be unavailable resulting in material disruption to business continuity of an organisation. | *Server* |
| **Dynamic Web Page** | A Web Page that is constructed dynamically upon request by a browser and displays content in response to user or Application Code interaction. | *Web Interface* |
| **e-Government Platform** | A centralised platform that hosts a number of critical **e-Government Services**. | |
| **e-Government Service** | This includes any **Information System** through which the **Government** provides an online service to the public.<br>An **e-Government Service** may be:<br>• Informational<br>• Transactional<br>• a mix of both | |
| **Electronic mail for the Government of Malta**<br>**(EGM)** | The electronic mail service in use by the **Government**. | |
| **E-mail, Official** | E-mail that is created or received in the official conduct of **Government** business. | *E-mail* |
| **Enterprise** | A collection of functional units organised to achieve common goals.<br>Within the context of GMICT Policies, this refers to the **Public Sector**. | *Enterprise Architecture* |
| **Enterprise Agreement** | An agreement signed between the **Government** and Solution/Service Providers. | |

| Term | Definition | Context |
|---|---|---|
| **Enterprise Architecture** | A process that comprises:<br>• Business<br>• Applications<br>• Data<br>• Technology<br>  o Hardware<br>  o Operating Software<br>  o Networks<br>• Security<br>and that:<br>• drives the continuous alignment of the adoption and use of technology with the enterprise's business objectives and strategic direction<br>• describes the current and future state of an enterprise's business processes and technology implementations<br>• provides an overall plan for designing, implementing and maintaining the underlying infrastructure to support the transition from the current to the future state | *Enterprise Architecture* |
| **Enterprise Architecture Review** | A review of the architecture of a system to ensure its correct fit within the overall **Enterprise Architecture**. | *Enterprise Architecture* |
| **Enterprise context** | Refers to **Public Sector** context | *Networking* |
| **Enterprise-grade Information and Communications Technology** | Information and Communications Technology that is:<br>1. Interoperable<br>2. Secure and able to allocate granular accessibility on a *least privilege* principle<br>3. Available<br>4. Supportable, Manageable and Serviceable | *Networking* |
| **Envelope Information** | A collection of attributes relating to an **E-mail Message**. Examples are:<br>• Sender<br>• Recipient<br>• Date and time sent<br>• Subject<br>• IP addresses of both Sender and Recipient<br>• Delivery report | *E-mail* |

| Term | Definition | Context |
|---|---|---|
| **Erasure** | Process intended to render magnetically stored data irretrievable by normal means.<br>*(SANS Security Leadership Essentials for Managers with Knowledge Compression 512.1, Managing the Enterprise, Planning, Networks and Physical Plant, www.sans.org)* | *Information Security* |
| **Federated Authentication mechanism** | A centralised process through which system user **authentication** is delegated to various **trusted identity providers** and which would hence allow the system user to authenticate for access to systems using a wider range of trusted identity providers. | *Information Security* |
| **Formalised Specifications** | Either a standard pursuant to EU Directive 98/34 or a specification established by ICT industry fora or consortia.<br>*(EIF for European Public Services, http://ec.europa.eu/isa/strategy/index_en.htm)* | *Interoperability* |
| **Functional Unit** | A hardware or software component or system that performs a specific function or provides a particular service. | |
| **Functional Risk** | The risk of performance degradation of Government ICT infrastructure due to the running of particular Web-related activities, e.g. download of very large files, continuous streaming, etc. | |
| **Gateway to Internet** | A functional unit that is that node on the network that lies between the **Malta Government Network** and the Internet. | *Internet* |
| **GMICT Compliance** | Conformance to any established GMICT Policy requirement. | *Compliance* |
| **Government ICT Shared Service** | Refer to **Shared Service**. | *Enterprise Architecture* |
| **Head of Department / Entity** | The person to whom the **Account Holder** reports. | *E-mail* |
| **Information Security Event** | An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.<br>*(ISO/IEC TR 18044:2004)* | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Information Security Incident** | Indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.<br>*(ISO/IEC TR 18044:2004)* | *Information Security* |
| **Information System** | An aggregate of interrelated components that work together to collect, process, store, transmit and disseminate data and produce information to support analysis, coordination, control and decision making in an organisation. | *Applications* |
| **Inherent Risk** | Risk status before management actions are taken to control / mitigate the risk.<br>*(Risk management – Vocabulary ISO Guide 73:2009(E/F))* | *Risk Management* |
| **Integrity** | A security principle that ensures data and configuration items are modified only by authorised persons and activities. It considers all possible causes of modification, including hardware and software failure, environmental events and human intervention.<br>*(Adapted from ITIL service Design, ITIL glossary and abbreviations, Crown Copyright 2011, www.itil-officialsite.com)* | *Information Security* |
| **Integrity Risk** | The risk of damage to the corporate image of Government through unethical behaviour, e.g. viewing of pornography. | |
| **Intellectual Property** | Intangible property, having a commercial value that is protected by Intellectual Property Rights. | *Information Security* |
| **Intellectual Property Rights** | Includes without limitation, patents, trademarks, registered designs, copyright, design rights and any other intellectual or industrial property rights. | *Information Security* |
| **Interactive Account** | An account that requires human interaction to access a system or service. | *Information Security* |
| **Internationalisation** | Refers to the design and development of a product, application or document content that enables easy localisation for target audiences that vary in culture, region, or language. | *Open Source Software* |

| Term | Definition | Context |
|---|---|---|
| **Interoperability** | Interoperability, within the context of **Public services** delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.<br>(*Adapted from the* European Interoperability Strategy - *http://ec.europa.eu/idabc/servlets/Doca74c.pdf?id=32768)* | *Open Standards, Interoperability* |
| **Interoperability Profile** | Guideline, template, pattern, profile or other forms of reference material that contextualises and standardises the use of **formalised specifications** within the Public Sector. | *Interoperability* |
| **Least Privilege** | Granting only the **minimum** permissions or access rights required by a **user**, **account** or **computing process** to perform **authorised** activities. | *Information Security* |
| **Line of Business (LoB) Software** | A software product that is not Corporate. | *Software – Desktop* |
| **Mapping** | A specific, fixed and explicit assignment of elements between two or more static data structures, which is aimed at establishing correlations and relationships between the involved data structures. A mapping may be unidirectional (injective) or bidirectional (bijective).<br>*(European Commission's Joinup collaborative platform, http://joinup.ec.europa.eu)* | *Interoperability* |
| **Metadata** | Data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths and data volatility.<br>*(MSA ISO/I EC 2382-17:2002)* | *Data, Interoperability* |
| **m-Government Service** | An **e-Government Service** that sends SMS messages to and/or receives SMS messages from citizens or an Application.<br>An **m-Government Service** may be provided either by automated means through an **Application** or through a mechanism requiring human intervention. | |

| Term | Definition | Context |
|---|---|---|
| **Need to know** | A determination made by the possessor of **Classified** information that a prospective recipient has a requirement for access to, knowledge of, or possession of the **Classified** information to perform tasks or services essential to the fulfilment of a **Classified** contract or programme. | *Information Security* |
| **Network** | A number of interconnected ICT devices, networks or operations.<br>*(Adapted from http://oxforddictionaries.com)* | *Network* |
| **Non-Enterprise-grade Information and Communications Technology** | Information and Communications Technology that is not **enterprise-grade**. | *Networking* |
| **Non-interactive account** | An account that is not an **interactive** one and that enables access programmatically. | *Information Security* |
| **Non-repudiation** | Ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. | *Information Security* |
| **Official E-mail** | See **E-mail, Official**. | *E-mail* |
| **One-time Password (OTP)** | A **password** that authenticates a user for a single transaction or session.<br>*(Adapted from: http://whatis.techtarget.com).* | *Information Security* |
| **Ontology** | Usually referred to as a data model, which features a set of concepts within one knowledge domain, a standardised terminology (Refer to **Taxonomy**) for all required and involved terms, and the specific relationships between the involved concepts.<br>*(European Commission's Joinup collaborative platform, http://joinup.ec.europa.eu)* | *Interoperability* |

| Term | Definition | Context |
|---|---|---|
| **Open Source**<br>**or**<br>**Open Source Software (OSS)** | Software, having distribution terms that must comply with the following criteria:<br>1. Free Redistribution<br>2. Source Code availability<br>3. Derived Works<br>4. Integrity of the Authors Source Code<br>5. No Discrimination against persons or groups<br>6. No Discrimination against Fields of Endeavour<br>7. Distribution of License<br>8. License must not be Specific to a Product<br>9. License must not Restrict Other Software<br>10. License must be Technology Neutral<br>*(http://opensource.org/docs/osd)* | *Open Source Software* |
| **Open Source Business Model** | A business model building upon the paradigm of community based workforce producing software which is freely available. | *Open Source Software* |
| **Open Specification**<br>**(Open Standard)** | Open specifications (informally referred to as Open Standards) are formalised specifications which within the context of Public services delivery, are characterised by the following features:<br>• All stakeholders have the same possibility of contributing to the development of the specification and public review is part of the decision-making process<br>• The specification is available for everybody to study<br>• Intellectual property rights related to the specification are licensed on FRAND terms or on a royalty-free basis in a way that allows implementation in both proprietary and open source software. | *Open Standards, Interoperability* |
| **Organisation** | Any structured body of persons performing activities or rendering services and that can be represented for legal or business continuity purposes. | *Data* |
| **Organisational Unit** | Any unit within an **Organisation** that can be identified and that has specific functions that are relevant to the services provided. | *Data* |
| **Owner** | The **Business Role** or **Person** responsible for the maintenance of an object of information. | *Data, Interoperability* |

| Term | Definition | Context |
|---|---|---|
| **Password** | A string of characters that serve as an authenticator of the user.<br>*(Adopted from PCI Data Security Standard and Payment Application Data Security Standard, PCI Security Standards Council, Ver 2.0).* | *Information Security* |
| **Perceived Risk** | An indication of a potential undesirable event (threat) which may exploit a weakness (vulnerability) and potentially impact MITA.<br><br>**Risk perception:** Stakeholder's view on a risk.<br>*(Risk management – Vocabulary ISO Guide 73:2009(E/F))* | *Risk Management* |
| **Person** | Any individual whose birth, adoption, marriage or death is registered at the Public Registry in Malta or Gozo; or any naturalised Maltese; or persons acquiring permits for work or residence; or persons otherwise known to public sector organisations. | *Data, Interoperability* |
| **Personal Data** | Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.<br>*(Data Protection Act - Chapter 440 of the Laws of Malta)* | *Data* |
| **Personal Identification Number** | A secret numeric **password** known only to the user and a system to authenticate the user to the system.<br>*Adopted from PCI Data Security Standard and Payment Application Data Security Standard, PCI Security Standards Council, Ver 2.0).* | *Information Security* |
| **Privileged Credential Management Solution** | A solution which manages accounts with elevated privileges and non-interactive accounts. | *Information Security* |
| **Processor** | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.<br>*(General Data Protection Regulation, (EU) 2016/679)* | *Electronic Communications*<br>*Email*<br>*Internet*<br>*Data Protection* |

| Term | Definition | Context |
|---|---|---|
| **Production Data** | Data that supports **Public Services**. It includes:<br>• any exact copies or subsets of it<br>• backups of it<br>• parallel runs<br>• audit data | *Information Security* |
| **Public Domain Data** | Data that is legally available and accessible to any individual or corporate entity and relates to:<br>• Civil Status information available at the Public Registry as regulated by the Civil Code<br>• **Person** and Address information that is made public by means of the publication of the Electoral Register<br>• Companies information that is published in the Companies Register<br>• Information that is published in the Government Gazette, or any other Government publication<br>• Name and address details of business enterprises other than companies that are made public through the issue of fiscal receipts. | *Data, Interoperability* |
| **Public services** | Services supplied by the Public Sector. | *Interoperability* |
| **Purging** | Process to remove stored data such that its recovery is not possible.<br>*(Adapted from: SANS Security Leadership Essentials for Managers with Knowledge Compression 512.1, Managing the Enterprise, Planning, Networks and Physical Plant, www.sans.org)* | *Information Security* |
| **Record** | Recorded information – regardless of form or medium – created, received and maintained by any public office in pursuance of its legal obligations or in the transaction of its business and providing evidence of the performance of those obligations or that business.<br>A record may include paper, book, photograph, microfilm, map, drawing, chart, magnetic tape, disk or optical disk, electronic storage medium or any copy thereof which provides evidence of the organisation functions, activities and transaction. A record may be created, received, maintained and destroyed.<br>*(Malta National Archives Act, Chapter 477 of the Laws of Malta.)* | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Recovery point objective** | The maximum acceptable level of data loss (in terms of time), from the occurrence of a Disaster. | *Server* |
| **Recovery time objective** | Maximum acceptable length of time from occurrence of a disaster, that may elapse before the lack of a business function severely impacts its beneficiary/ies. | *Server* |
| **Residual Risk** | Risk status after management actions have been implemented.<br>Risk remaining after risk treatment.<br>*(Risk management – Vocabulary ISO Guide 73:2009(E/F))* | *Risk Management* |
| **Risk** | Impact and Likelihood of a threat (event) exploiting a vulnerability (weakness) which may affect the Government.<br>Effect of uncertainty on objectives.<br>*(Risk management – Vocabulary ISO Guide 73:2009(E/F))* | *Risk Management* |
| **Risk Appetite** | The amount and type of risk that an organisation is prepared to seek, accept or tolerate.<br>*(British Standard on Risk Management BS31100 2008).*<br>Amount and type of risk that an organisation is willing to pursue or retain.<br>*(Risk management – Vocabulary ISO Guide 73:2009(E/F))* | *Information Security*<br>*Risk Management* |
| **Risk Register** | This is a register containing all the risks identified by the Agency and controls to mitigate them. | *Risk Management* |
| **Risk Treatment** | Process to modify risk. May involve:<br>• Avoiding the risk<br>• Taking or increasing the risk in order to pursue an opportunity<br>*(Risk management – Vocabulary ISO Guide 73:2009(E/F))* | |
| **Sanitised Data** | Data that is modified so as to hinder the possibility of it being identifiable (to an individual or organisation that it refers to). It is not **production data**. | *Information Security* |
| **Security Baseline** | A documented set of security requirements established for a **System.** | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Security Control** | A control that may include, but not be limited to:<br>• software including patches and updates<br>• anti-virus software<br>• virus definition files<br>• updating of the virus signature file before each login and at least once a week<br>• regular scanning of a Solution<br>• detection and cleaning of malicious code<br>• hardware<br>• specialised devices/environments<br>• operational procedures<br>• contractual agreements | *Information Security* |
| **Security Information and Event Management** | The centralised collection, normalisation and storage of disparate events across interconnected heterogeneous systems, by means of a segregated tool. | *Information Security* |
| **Security Marking** | An indication of the relative importance of an **asset** to **enterprise** security which thereby determines specific protection requirements applicable to that **asset**.<br>*(Adapted from http://www.fas.org/sgp/library/quist2/chap_7.html)* | *Information Security* |
| **Security Tenets** | Refers to Confidentiality, Integrity and Availability. | *Information Security* |

| Term | Definition | Context |
|---|---|---|
| **Semantic Interoperability** | The ability for organisations to process information from external sources in a meaningful manner. It ensures that the precise meaning of exchanged information is understood and preserved throughout exchanges between parties.<br>In the context of the EIF, semantic interoperability encompasses the following aspects:<br>• Semantic interoperability is about the meaning of data elements and the relationship between them. It includes developing vocabulary to describe data exchanges, and ensures that data elements are understood in the same way by communicating parties.<br>• Syntactic interoperability is about describing the exact format of the information to be exchanged in terms of grammar, format and schemas.<br>*(European Interoperability Framework for European public services v2.0 – http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf)* | *Interoperability* |
| **Semantic assets** | Commonly referred terminologies that ensure that data elements are interpreted in the same way by communicating parties. They usually include dictionaries, thesauri, nomenclatures, taxonomies, mapping tables, ontologies and service registers. | *Interoperability* |
| **Server** | Any physical - irrespective of form factor - or virtual **ICT device** having intelligence to provide one or more services to ICT devices. | *Server* |
| **Server Operator** | Individual or group of individuals who are responsible for the operation (day to day administration) of a **Server**. | *Server* |
| **Service Centre** | A trusted organisation that has the mandate by **Government** to monitor and action calls received from **Public Sector** employees as well as **Third Parties** rendering services to the **Government**.<br>This role is fulfilled by the Service Call Centre (SCC) of Malta Information Technology Agency (MITA). | |
| **Service orientation** | Creating and using business processes packaged as services.<br>*(European Interoperability Framework for European public services v2.0 –*<br>*https://ec.europa.eu/isa2/sites/isa/files/isa_annex_ii_eif_en.pdf*<br>*)* | *Interoperability* |

| Term | Definition | Context |
|---|---|---|
| **Service oriented architecture** | A paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.<br>*(European Interoperability Framework for European public services v2.0 – http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf)* | *Interoperability* |
| **Shared Service** | A singular instance of a set of resources which service **multiple consumers** concurrently. A shared service can provide the ability to be used both interactively (via an appropriate interface) as well as in a machine-to-machine context. | *Enterprise Architecture* |
| **Signature** | At the end of the **Body**, a specific piece of text designed by the originator for individual identification.<br>*(MSA ISO/IEC 2382-32:2002)* | *E-mail* |
| **Simulated Data** | Fictitious data. It is not **production data**. | *Information Security* |
| **Solution** | A **System** or number of **Systems** delivered by a **Solution Provider**. | |
| **Solution Architecture** | A single or aggregated set of **architectures** that are intended to address a particular technology and/or business need. | *Enterprise Architecture, Interoperability* |
| **Solution Owner** | A role that has the responsibility and decision making authority for a **Solution** throughout its lifecycle. | Information Security |
| **Solution Provider** | A person or organisation that has the mandate by **Government** to design and/or develop a **Solution** for the **Government**. | |
| **Spam** | Unsolicited junk or bulk E-mail that is not related to work or personal interest. | *E-mail* |

| Term | Definition | Context |
|---|---|---|
| **Standard** | A technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory and which is one of the following:<br>• international standard: a standard adopted by an international standardisation organisation and made available to the public,<br>• European standard: a standard adopted by a European standardisation body and made available to the public,<br>• national standard: a standard adopted by a national standardisation body and made available to the public.<br>*Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, Article 1, paragraph 6, as referenced by the European Interoperability Framework for European public services v2.0* | *Open Standards* |
| **Standards developing organisation** | A chartered organisation tasked with producing standards and specifications, according to specific, strictly defined requirements, procedures and rules. Standards developing organisations include:<br>• recognised standardisation bodies such as international standardisation committees such as the International Organisation for Standardisation (ISO), the three European Standard Organisations: the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) or the European Telecommunications Standards Institute (ETSI)<br>• fora and consortia initiatives for standardisation such as the Organisation for the Advancement of Structured Information Standards (OASIS), the World Wide Web Consortium (W3C) or the Internet Engineering Task Force (IETF).<br>*European Interoperability Framework for European public services v2.0* | *Open Standards* |
| **Syntactic assets** | Definitions of common data structures, such as XML and metadata schemas, to support the exchange of data in distributed information systems. | *Interoperability* |
| **System** | Consists of any number of **Artefacts**. | |

| Term | Definition | Context |
|---|---|---|
| **System Security Baseline** | A variation from a **Corporate Security Baseline**. This is documented by the **Data Owner.** | |
| **Target Architecture** | The state of an **Architecture** at the end of a specified timeframe, generally captured in the organization's strategic objectives and plans. Commonly referred to as the "to-be" architecture. | *Enterprise Architecture* |
| **Taxonomy** | A classification of the standardised terminology for all terms used within a knowledge domain. In a taxonomy, all elements are grouped and categorised in a strict hierarchical way and are usually represented by a tree structure. In a taxonomy, the individual elements are required to reside in the same semantic scope, so all elements are semantically related with one another to one degree or another.<br>*European Interoperability Framework for European public services v2.0* | *Interoperability* |
| **Third Party** | Any person who is not employed with, or any organisation that does not form part of, the **Public Sector**. Third Parties include, but are not limited to:<br>• Suppliers<br>• Sub-contractors<br>• Service providers<br>• Sponsored students | |
| **Trusted Identity Providers** | Include corporate directories (e.g. CORP in Government's case), eID for Maltese citizens, other security token services (STS) provided by business partners, or social identity providers who can authenticate users having social media accounts. | *Information Security* |
| **Unclassified** | Not **Classified.** | |
| **User Account** | An **authentication** method that determines whether a user is authorised to access electronic resources including, but not limited to, a computer, network or information service. | *Information Security* |

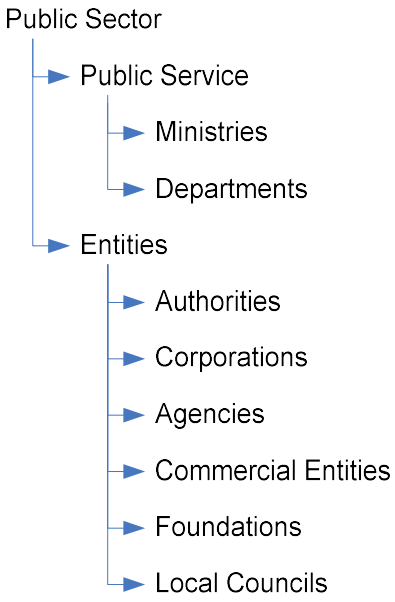
| Term | Definition | Context |
|---|---|---|
| **Website** | An **Information System** deployed on the Web comprised of a collection of any number of Web pages consisting of either:<br>• **Static Content**, and/or<br>• **Dynamic Content**<br>**Note:**<br>A **website** is defined as **new** if it does not make use of any of the following items of an existing **website**:<br>• **Static Content**<br>• **Application Code**<br>• Components | |
| **Works Order** | A works order should include:<br>• A description of the work required<br>• Response time<br>• Time to fix | *Hardware - Desktop* |
| **Workstation** | A PC and any Peripherals connected directly to the PC or shared by a workgroup.<br>Peripherals connected to the PC **exclude** heavy duty, high volume and combo printers.<br>For PCs in schools, the peripherals forming part of a Workstation **include** audio-visual and ancillary equipment. | *Hardware – Desktop* |

# Acronyms

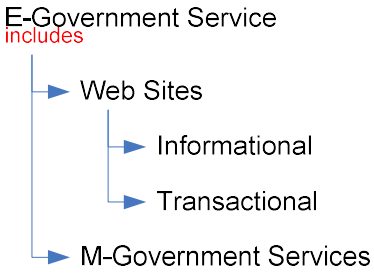
| Acronym | Term |
|---|---|
| **CI** | Configuration Item |
| **CIO** | Chief Information Officer |
| **CMDB** | Configuration Management Database |
| **EGM** | Electronic Mail for the Government of Malta |
| **EIF** | European Interoperability Framework |
| **EMA** | Enterprise Management Architecture |
| **FITA** | Foundation for Information Technology Accessibility |
| **FRAND** | Fair, reasonable and non-discriminatory |
| **ICT** | Information and Communications Technology |
| **IP** | Internet Protocol |
| **LAN** | Local Area Network |
| **MAGNET** | Malta Government Network |
| **OSS** | Open Source Software |
| **PC** | Personal Computer |
| **RPO** | Recovery Point Objectives |
| **SIEM** | Security Information and Event Management |

# Appendix

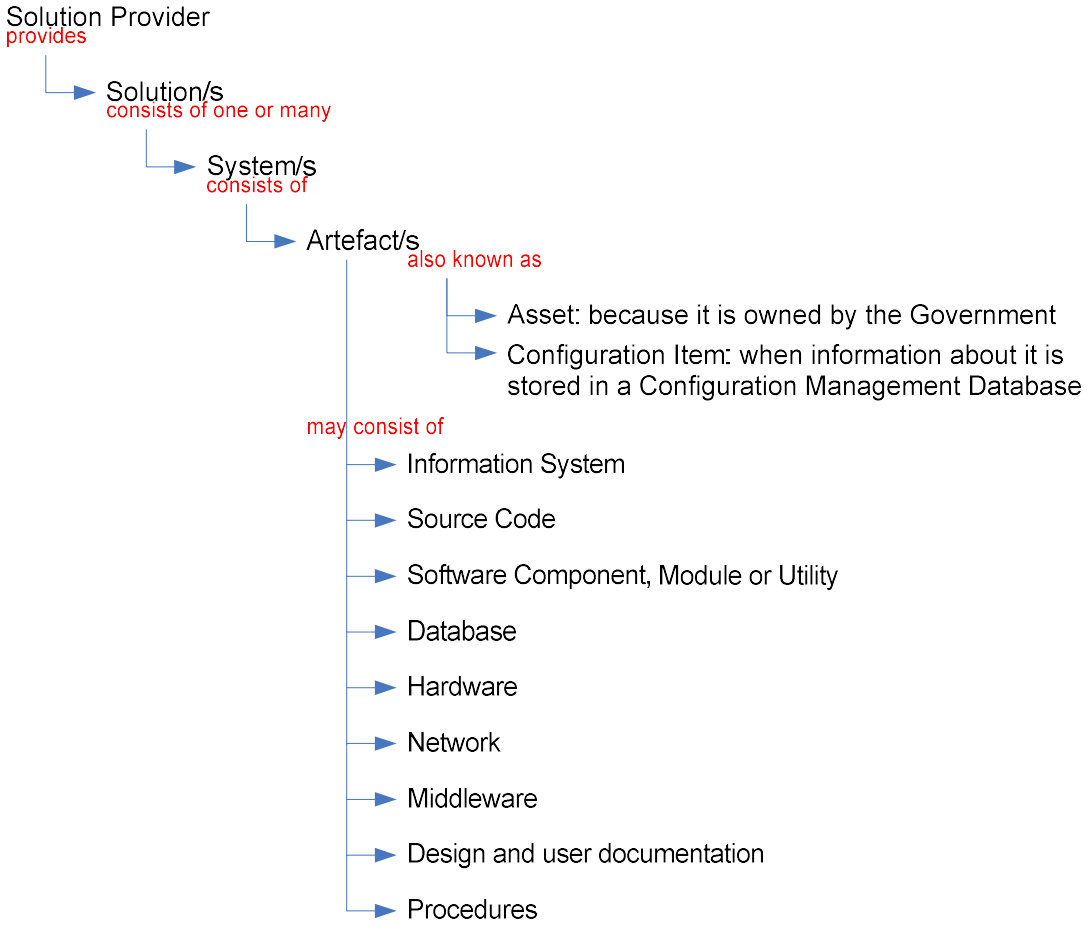
## Public Sector




## E-Government Service



## Solutions, Systems and Artefacts



## Issuing Authority

This document has been issued by the **Malta Information Technology Agency**.

## Contact Information

Government ICT Policies may be found at **http://ictpolicies.gov.mt**.

Any suggestions, queries or requests for clarification regarding Government ICT Policies may be forwarded to **ictpolicies@gov.mt**.