Definitions

Word/Term	Definition
Access control	Controlling who has access to a computer or online service and the information it stores.
Asset	Something of value to a person, business or organization.
Authentication	The process to verify that someone is who they claim to be when they try to access a computer or online service.
Authenticity	Property that an entity is what it claims to be (ISO 27000)
Cloud computing	Delivery of storage or computing services from remote servers online (ie via the internet).
Cybersecurity program	It is defined as a set of projects to provide secure and resilient digital services, including prevention, risk management, and response and recovery activities.
Encryption	The transformation of data to hide its information content.
Firewall	Hardware or software designed to prevent unauthorised access to a computer or network from another computer or network.
Guideline	A guideline is not a mandatory action, and no disciplinary action should result from non-adoption. However, Cybersecurity Guidelines are considered Best Practice and should be implemented whenever possible. A guideline typically uses works like "should" or "may" in the definition.
Hacker	Someone who violates computer security for malicious reasons, kudos or personal gain.
Hard disk	The permanent storage medium within a computer used to store programs and data.
Integrity	Property of accuracy and completeness (ISO 27000)
Interactive logon	An interactive logon to a computer can be performed either locally, when the user has direct physical access, or remotely, through Terminal Services, in which case the logon is further qualified as remote interactive. After an interactive logon, Windows/IOS runs applications on the user's behalf and the user can interact with those applications.

Identification	The process of recognising a user of a computer or online service.
Infrastructure-as-a-service (IaaS)	Provision of computing infrastructure (such as server or storage capacity) as a remotely provided service accessed online (ie via the internet).
Instant messaging	Chat conversations between two or more people via typing on computers or portable devices.
Internet service provider (ISP)	Company that provides access to the internet and related services.
Intrusion detection system (IDS)	Program or device used to detect that an attacker is or has attempted unauthorised access to computer resources.
Intrusion prevention system (IPS)	Intrusion detection system that also blocks unauthorised access when detected.
Keyboard logger	A virus or physical device that logs keystrokes to secretly capture private information such as passwords or credit card details.
Least Privilege	A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.
Local area network (LAN)	Communications network linking multiple computers within a defined location such as an office building.
Malware	Software intended to infiltrate and damage or disable computers. Shortened form of malicious software.
Management system	A set of processes used by an organisation to meet policies and objectives for that organisation.
Network firewall	Device that controls traffic to and from a network.
Password	A secret series of characters used to authenticate a person's identity.
Passphrase	A passphrase is a string containing multiple words that is used to authenticate a user on a computer system. It may be used in combination with a username to create a login or may be required separately for additional authentication. By definition, a passphrase must contain a phrase that includes multiple words, while a password may only have a minimum length of six or eight characters. There is no universal required length for a passphrase, but a typical passphrase is 20 to 30 characters in length.

Personal firewall	Software running on a PC that controls network traffic to and from that computer.
Personal information	Personal data relating to an identifiable living individual.
Phishing	Method used by criminals to try to obtain financial or other confidential information (including user names and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organization (often a bank). The email usually contains a link to a fake website that looks authentic.
Public Key Infrastructure (PKI)	A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued
Platform-as-a-service (PaaS)	The provision of remote infrastructure allowing the development and deployment of new software applications over the internet.
Principles	Principles provide mandatory considerations. Whereas, standards identify an exhaustive set of considerations for adjudication or policy making, a principle identifies a nonexhaustive set, leaving open the possibility that other considerations may be relevant to the decision.
Privileged access	Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network.
Qualified Certificate for Electronic Seal	Information on the party or provider, such as the Member State, to potentially include the registration number of the legal entities or name of the natural persons; the name of the creator of the seal; and/or electronic seal validation data.
Risk	Something that could cause an organization not to meet one of its objectives.
Risk assessment	The process of identifying, analysing and evaluating risk. Risk assessments focus on identifying risks to the confidentiality, integrity and availability of WHO information in computing solutions being proposed to use or store WHO information. The assessment will give due consideration to the following non-exhaustive list of topics: 1. the classification of information and data to be stored or processed, their confidentiality and sensitivity (e.g. e-mails, old archival records, correspondence with third parties, HR or medical information, financial information, meeting records, etc.); 2. the Information Technology priority needs of the Organization and the related business case; 3. the countries where the service provider or the cloud servers are

	located; 4. the type of solution(s), including on premises and cloud solutions; 5. the Cybersecurity features and configurations of the computing solution; 6. the cost and efficiency of the computing solution; 7. the available risk mitigation measures and mitigation costs for external, public and hybrid clouds, including (but not limited to) through encryption of data, segregation of data, access and authentication to the solution and appropriate contractual clauses; and Whether storage of the information and data in question requires the agreement of, or at least consultation with, staff and/or third parties.
Rule	Rules are the most constraining and rigid. Once a rule has been interpreted and the facts have been found, then the application of the rule to the facts decides the issue to which it is relevant.
Security control	Something that modifies or reduces one or more security risks.
Security information and event management (SIEM)	Process in which network information is aggregated, sorted and correlated to detect suspicious activities.
Security perimeter	A well-defined boundary within which security controls are enforced.
Segregation of duties	Separation of duties (SoD; also known as Segregation of Duties) is the concept of having more than one person required to complete a task.
Server	Computer that provides data or services to other computers over a network.
Service Owner	The Service Owner is accountable for a specific service (Infrastructure, Application or Professional Service) within an organization regardless of where the technology components or professional capabilities reside. To ensure that a service is managed with a business focus, the definition of a single point of accountability is absolutely essential to provide the level of attention and focus required for its delivery. The Service Owner is a primary stakeholder in all of the IT processes which enable or support it.
Software-as-a-service (SaaS)	The delivery of software applications remotely by a provider over the internet; perhaps through a web interface.

Standard	Standards provide an intermediate level of constraint. Standards guide decisions but provide a greater range of choice or discretion; for example, a standard may provide a framework for balancing several factors.
Technology Standard	The technology standard is defined as a list of approved technologies that have been assessed. Each project team must consult the Technology Architect for the target development, desktop, testing and/or production environments to ensure that the intended use of the technologies is included in the approved technology standard list.
Threat	Something that could cause harm to a system or organization.
Two-factor authentication	Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.
User	User is defined as unique account created in the WHO authorized user directory (WIMS).
Username	The short name, usually meaningful in some way, associated with a particular computer user.
User account	The record of a user kept by a computer to control their access to files and programs.
Verifiability of Certificates	Requirements shall be objectively verifiable. Only those requirements that can be verified shall be included. (ISO 27000)
Virtual private network (VPN)	Link(s) between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network.
Virus	Malware that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.
Vulnerability	A flaw or weakness that can be used to attack a system or organization.
Wide area network (WAN)	Communications network linking computers or local area networks across different locations.