Student ID (Matricola):

Security Category	Definition	Weights
Access Control	Access Control ensures that resources are only granted to those users who are entitled to them.	
Key Management	Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys.	
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.	
User Access Revocation	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer).	
Intrusion Detection	An Intrusion Detection System (IDS) gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).	
Penetration Testing	Penetration testing is used to test the external perimeter security of a network or facility.	
Multi-factor Authentication	Multi-factor authentication (MFA) is an authentication mechanism where a user is only successfully authenticated after presenting several separate pieces of evidence typically at least two of the following categories: knowledge (something they know); possession (something they have), and inherence (something they are).	
Asset Management	Asset management refers to the process of maintaining a complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership, defined roles and responsibilities.	
Disaster Recovery	It is the process of recovery of IT systems in the event of a disruption or disaster.	
Anti-Malware	Anti-malware is a software program designed to prevent, detect and remediate malicious programming on individual computing devices and IT systems.	
Segregation of Duties	Segregation of duties is the principle of splitting privileges among multiple individuals or systems.	
Auditing	Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.	
Intellectual Property	Intellectual Property protects the programs and systems that support what makes a company successful and unique.	
Personnel Security	Personnel security is a system of policies and procedures which seek to manage the risk of staff (permanent, temporary or contract staff) exploiting, or intending to exploit, their legitimate access to an organisation's assets or premises for unauthorised purposes.	
Production Changes	Policies and procedures established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components.	
Physical and Environment Protection	Security measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment	
Non Disclosure Agreements	A non-disclosure agreement (NDA) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties.	
Awareness and Training	Activities which seek to focus an employees’ attention on an (information security) issue or set of issues.	
Vulnerability Management	Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities", especially in software and firmware.	
Source Code Analysis	Source code analysis analyses source code and/or compiled version of code in order to help find security flaws.	
		0

Weight	Definition
1	Not important
3	Slightly important
5	Neutral
7	Moderately important
9	Very important