For Your Desk

Certified Information Systems Security Professional (CISSP)

(ISC)² Code of Ethics
Preamble
Canons

Security Concepts	
Authenticity	Verifying the identity of a person or process
Non-repudiation	Inability to refute responsibility

CIA Triad	
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Integrity	Guarding against improper information modification and ensuring information non-repudiation and authenticity
Availability	Ensuring timely and reliable access to and use of information by authorized users

GDPR Privacy Principles	
Lawfulness, fairness, and transparency	Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
Purpose limitation	Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimization	Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data must be accurate and, where necessary, kept up to date.
Storage limitations	Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary.
Integrity and confidentiality	Personal data must be processed to ensure appropriate security of the personal data.

Intellectual Property				
	Patent	**Trademark**	**Copyright**	**Trade secret**
Definition	Provides legal protection for rights over inventions	Identifies the brand owner of a particular product or service	Protects a wide range of creative, intellectual, or artistic works	Protects information that derives independent economic value from not being publicly known
Requirements	• Novelty • Usefulness • Nonobvious ness (US) • Inventive step (EU)	• To distinguish the goods or services of a party • To not confuse consumers about the relationship between one party and another • To not deceive consumers concerning the qualities	• Originality	• Information not generally known to the public • Confers economic benefits on its holder from not being publicly known
Symbol	N/A	™ (unregistered trademark) ℠ (unregistered service mark) ® (registered trademark)	© (copyright) ℗ (sound recording copyright)	N/A

Risk Terminology	
Asset	Anything of value to the company
Vulnerability	A weakness or the absence of a safeguard
Threat	The potential danger to systems or information
Threat agent	The entity which carries out the attack
Impact	The severity of the damage
Risk	The likelihood that damage or harm will be realized
Risk management	The process of identifying risks, analysing them, developing a response strategy for them, and mitigating their future impact
Risk appetite	The level of risk that an organization is prepared to accept in pursuit of its objectives
Residual risk	The risk remaining after risk treatment

Quantitative Risk Analysis	
Asset value (AV)	The value of the asset that might be affected or lost
Exposure factor (EF)	The percentage of the asset value that would be lost
Single loss expectancy (SLE)	The amount that would be lost in a single occurrence of the risk factor
SLE = AV x EF	
Annualized rate of occurrence (ARO)	The number of times per year a given threat is expected
Annualized loss expectancy (ALE)	The amount that would be lost over the course of a year
ALE = SLE x ARO	

Threat Model: STRIDE		
Threat	**Description**	**Violation**
Spoofing	Impersonating something or someone else	Authentication
Tampering	Modifying data or system	Integrity
Repudiation	Claiming to have not performed an action	Non-repudiation
Information disclosure	Exposing information to an unauthorized party	Confidentiality
Denial of service	Deny or degrade service to users	Availability
Elevation of privilege	Gain capabilities without proper authorization	Authorization

Security Control Functional Types
Preventive control
Detective control
Deterrent control
Corrective control
Compensating control
Recovery control

Security Control Categories
Administrative control
Technical control
Physical control

Investigation Types
Criminal
Civil
Administrative
Regulatory
Industry

Privacy Terms	
Personally identifiable information (PII)	Can be used to identify, locate, or contact an individual
Protected health information (PHI)	Can be used to identify an individual and to relate to that individual's past, present, or future physical or mental health care or health care payments
Classified information	Must protect the material that a government body deems to be sensitive information

Classified Information	
Top secret	Exceptionally grave damage to national security
Secret	Serious damage to national security
Confidential	Damage to national security
Restricted	Undesirable effects

EOL	EOS
The date where a vendor no longer manufactures a particular product and does not take orders for it	The date where the vendor no longer provides support for a particular product

Data Destruction methods	
Erasing	A simple deletion process that removes only the catalog reference and not the files
Clearing	A level of sanitization that renders media unreadable through normal means
Purging	An advanced level of sanitization that renders media unreadable even through an advanced laboratory attack
Sanitizing	A combination of processes that ensures data is removed
Degaussing	A method of destruction that generates heavy magnetic fields which realign the magnetic fields in magnetic media

Data Roles and Responsibilities	
Data Subject	A natural individual who is the subject of personal data.
Data Owner	Holds legal rights and complete control over data elements.
Data Custodian	Responsible for the safe custody, transport, and storage of the data and implementation of business rules.
Data Steward	Responsible for data content, context, and associated business rules.
Data Custodian	Determines the purposes for which and the means by which personal data is processed.
Data Processor	Processes personal data only on behalf of the controller.

Secure Design Principles	
Threat modeling	A process by which developers can understand security threats to a system, determine risks from those threats, and establish appropriate mitigations
Least privilege	The practice of only granting a user the minimal permissions necessary to perform their explicit job function
Defence in depth	A design principle in which multiple layers of security controls are placed throughout an information technology system
Secure defaults	A secure design principle that ensures the default configuration settings of the system are the as secure as possible even if they are not necessarily the most user-friendly
Fail securely	A design feature that, in the event of a failure, should fail to a state that prevents further operations
Separation of duties (SoD)	The practice of ensuring that no organizational process can be completed by a single person; forces collusion as a means to reduce insider threats
Keep it simple	A design principle which states that most processes or systems work best if they are kept simple rather than made overly complicated
Trust but verify	A design principle that promotes the idea that system components should not blindly trust each other
Zero Trust	A security model based on the principle of trust nothing and verify everything
Privacy by design	A design-thinking approach to proactively embed into the design and operation of IT systems, networked infrastructure, and business practices by default
Shared responsibility	A cloud security framework that describes the security responsibilities of the cloud provider and the cloud customer

Security Models									
State machine	Multilevel lattice	Noninterference	Information flow	Bell-LaPadula	BIBA	Clark–Wilson integrity	Brewer and Nash	Graham-Denning	Take-grant

Block Ciphers			
	Key sizes	*Block size*	*Deprecated?*
DES	56 bits	64 bits	Yes
3DES	56 bits	64 bits	Yes
AES	128, 192, or 256 bits	128 bits	No

Water-Based Fire Suppression Systems			
Wet pipe	Dry pipe	Pre-action	Deluge

Classes of Fires		
Type of fire	***Elements of fire***	***Suppression method***
Class A: Ordinary combustibles	Paper and wood	Water and foam
Class B: Flammable liquids	Petroleum products	Dry chemical and foam
Class C: Electrical	Energized equipment	CO2 and dry powders
Class D: Flammable metals	Magnesium lithium	Dry powders
Class K: Commercial kitchens	Cooking oils and greases	Wet chemical

Cloud				
Software as a service (SaaS)	Platform as a service (PaaS)	Infrastructure as a service (IaaS)		*Service models*
Public	Private	Community	Hybrid	*Development models*

Block Ciphers			
	Key sizes	***Block size***	***Deprecated?***
DES	56 bits	64 bits	Yes
3DES	56 bits	64 bits	Yes
AES	128, 192, or 256 bits	128 bits	No

OSI Model		
SMTP, FTP	• Provides services or protocols to applications	**Application**
JPEG, ASCII	• Data formatting – compression or encryption	**Presentation**
RPC, AppleTalk	• Establish, maintain and manage sessions	**Session**
TCP, UDP	• End-to-end communication • Segmentation or sequencing of data	**Transport**
Router IP, ICMP	• Logical addressing • Routing	**Network**
Switch ARP	• Physical addressing • Error detection	**Data-link**
Hubs Ethernet	• Send bits and receive bits • Define standard interfaces	**Physical**

	TCP	UDP
	Establishes a connection between the computers before transmitting the data	Sends the data directly to the destination computer without checking whether the system is ready to receive or not
Connection	Connection-oriented protocol	Connectionless protocol
Acknowledgment	Takes acknowledgment of data and can retransmit if the user requests	Neither takes acknowledgment nor retransmits the lost data
Reliability	Highly reliable	Unreliable
Header Size	20 bytes	8 bytes
Speed	Slow	Fast

Encapsulation	TCP/IP Model
Data	**Application**
Segment	**Transport**
Packet (TCP) Datagram (UDP)	**Internet**
Frame	**Network interface**
Bits	

IPv6 vs. IPv4		
Address size	128 bits	32 bits
Range	340 undecillion possible addresses	4.3 billion possible addresses
Scalability	Improved by adding a scope field to the multicast address	No options for scalability
Anycast address	Used to send a packet to any one node in a group of nodes	Doesn't have an anycast address

TCP and UDP Ports		
Well-known ports	0 - 1023	Reserved for privileged applications
Registered ports	1024 - 49151	Assigned by IANA for specific service upon application by a requesting entity
Dynamic ports	49152 - 65535	Used by any application for temporary purposes and cannot be registered

Access Control	
Subject	An active component that needs access to an object or the data within it
Object	A passive component that contains data or information
Access	The flow of information between a subject and an object

AAA	
Identification	Claiming identity
Authentication	Verifying identity
Authorization	Granting access
Accounting	Tracking activity

Multi-Factor Authentication		
Something you know	Authentication by knowledge	Password or PIN
Something you have	Authentication by ownership	A token device or passport
Something you are	Authentication by characteristic	Biometrics

Access Control Models		
	Access control based on	***Used in***
Discretionary access control (DAC)	Owner's discretion	Operating systems
Mandatory access controls (MAC)	Subject's security clearance level	Military and government sectors
Role-based access control (RBAC)	Subject's roles	Organizations
Rule-based access control (RuBAC)	Predefined rules	ACL in routers and firewalls
Attribute-based access control (ABAC)	Attributes of the subject, object, and environment and set of policies	Complex environment
Risk-based access control	Security risk value related to each access request	Retail banking

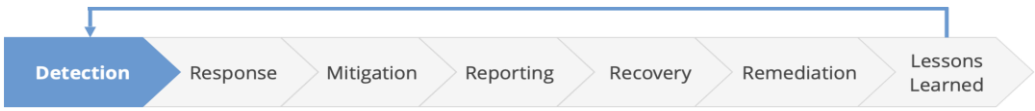
Testing Levels	Testing Methods
Unit test	Static testing
Integration test	Dynamic testing
System test	Use case testing
User acceptance test	Abuse case testing

SOC Reports			
	Scope	**Purpose**	**Users**
SOC 1	Financial reporting controls	Audit the financial statements of customers	Restricted to customers and their auditors
SOC 2	Managing regulations and four optional criteria: • Confidentiality • Availability • Processing integrity • Privacy	GRC programs, oversight, and due diligence	Restricted to management, regulators, and auditors
SOC 3		Marketing purposes	Freely available to anyone who needs confidence in the controls of the service organization

IPS	IDS
Detects and prevents any malicious traffic or activity to gain access to the target	Detects any unauthorized intrusion in a network, server, or system

	IDS Detected It	IDS Didn't Detect It
Malicious traffic	**True positive** (attack and alert)	**False negative** (attack and no alert)
Normal traffic	**False positive** (no attack and alert)	**True negative** (no attack and no alert)

Incident Response Life Cycle



Alternate Location Sites

	Mirror	Hot	Warm	Cold
RTO	0	0 to 24 hours	1 to 7 days	1 to 2 weeks
Cost	$$$$	$$$	$$	$
Equipment available	Yes	Yes	Not fully	No
Connectivity available	Yes	Yes	Yes	No
Active before failover	Yes	Yes	Yes	No

Backups

	Data backed up	***Back up speed***	***Restoration speed***	***Storage space***	***Archive bit set to 0***
Full backup	All data	Slowest	Fastest	Maximum	Yes
Differential backup	All data since last full backup	Moderate	Moderate	Moderate	No
Incremental backup	Only new or modified data	Fastest	Slowest	Minimum	Yes

Software Capability Maturity Model	
Level 1: Initial	Process is unpredictable, poorly controlled, and reactive
Level 2: Repeatable	Processes are more organized and are often reactive
Level 3: Defined	Processes are well-characterized, understood, and proactive
Level 4: Managed	Processes are controlled using quantitative techniques
Level 5: Optimizing	Processes are continually improved, and optimized

Systems Development Life Cycle
Prepare a security plan
Development or acquisition
Implementation
Operation or maintenance
Disposal

Software Development Models
Waterfall model
Spiral model
Rapid-application development
Extreme programming
Prototyping
Modified prototyping model
Joint analysis development

Certification	Accreditation
A technical evaluation of a system's security capabilities against a predetermined set of security standards or policies	The formal management authorization to move the system into production