Ron Sharon (www.ronsharon.com)

CISSP CHEATSHEET

These are just a few of the many terms and concepts covered in the CISSP certification. Remember to study and review all of the material thoroughly to prepare for the exam. Good luck!

Terminology	Explanation
Access control	Restricting access to resources or information to only authorized entities.
Authentication	The process of verifying the identity of a user or device.
Authorization	Granting access to a resource or information based on the user's identity and permissions.
Availability	Ensuring that resources or services are available when needed.
Backup	Creating copies of data to ensure its availability in case of loss or corruption.
Business continuity	Planning and implementing processes to ensure that critical business functions can continue in the event of a disruption.
Cryptography	The practice of secure communication using codes and ciphers.
Denial-of-service (DoS)	An attack that floods a network or system with traffic to disrupt its availability.
Disaster recovery	The process of restoring critical systems and data after a disaster.
Encryption	The process of encoding data to protect its confidentiality.
Firewall	A device or software that filters network traffic to prevent unauthorized access.
Incident response	The process of detecting, responding to, and mitigating security incidents.
Intrusion detection system (IDS)	A system that monitors network traffic for signs of unauthorized access or malicious activity.
Malware	Malicious software that can harm or disrupt systems and data.
Network segmentation	Dividing a network into smaller subnetworks to improve security and performance.
Password policy	Rules and guidelines for creating and managing passwords.
Penetration testing	Simulating an attack on a system or network to identify vulnerabilities and weaknesses.
Physical security	Measures to protect physical assets from unauthorized access or damage.
Risk assessment	Evaluating the likelihood and impact of potential risks to an organization.
Secure coding	Writing software code that is free from security vulnerabilities.
Security architecture	The design and implementation of security controls to protect an organization's assets.
Security controls	Technical or administrative measures that reduce the risk of security incidents.
Security policy	A set of rules and guidelines that define an organization's security posture.
Security testing	Assessing the effectiveness of security controls through testing and validation.
Social engineering	The use of deception to manipulate individuals into divulging sensitive information or performing actions that compromise security.
Spoofing	Faking or impersonating an identity or device to gain unauthorized access.
Threat	Any event or circumstance that has the potential to cause harm or loss.
Vulnerability	A weakness or flaw in a system or application that can be exploited by attackers.
Access control list (ACL)	A list of rules that govern access to network resources.
Biometric authentication	Using unique physical characteristics to verify a user's identity, such as fingerprints or facial recognition.
Botnet - A network of compromised	devices that can be used to launch attacks or carry out other malicious activities.
Chain of custody	The documentation and tracking of evidence to ensure its integrity and admissibility in legal proceedings.

Confidentiality	Ensuring that sensitive information is only accessible to authorized individuals.
Cross-site scripting (XSS)	A type of attack that injects malicious code into a website to steal user data or credentials.
Data classification	Categorizing data based on its sensitivity and value to an organization.
Digital signature	A cryptographic mechanism that provides authenticity and non-repudiation for electronic documents.
Disaster recovery plan (DRP)	A formal plan that outlines the steps to be taken in the event of a disaster.
Encryption key	A secret value used to encrypt and decrypt data.
Hashing	A cryptographic technique that produces a fixed-length, unique representation of data.
Incident management	The process of responding to and managing security incidents.
Information security	The protection of information from unauthorized access, use, disclosure, disruption, modification, or destruction.
Integrity	Ensuring that data is accurate and has not been tampered with.
Least privilege	Giving users only the minimum level of access necessary to perform their job functions.
Network security	The protection of network resources and information from unauthorized access or attacks.
Non-repudiation	The ability to prove the origin and integrity of data or messages.
Patch management	The process of keeping software and systems up-to-date with the latest security patches and updates.
Penetration testing report	A detailed report that outlines the findings and recommendations from a penetration testing engagement.
Phishing	A type of social engineering attack that tricks users into divulging sensitive information, often through email or fake websites.
Risk management	The process of identifying, assessing, and mitigating risks to an organization.
Security incident	An event or occurrence that violates an organization's security policies and procedures, or threatens the confidentiality, integrity, or availability of its information assets.
Security operations center (SOC)	A facility that is responsible for monitoring, detecting, and responding to security events and incidents in real-time.
Separation of duties	Dividing job responsibilities and access privileges among multiple individuals to prevent conflicts of interest or unauthorized actions.
Single sign-on (SSO)	A mechanism that allows users to authenticate once and access multiple applications or systems without having to re-enter their credentials.
System development life cycle (SDLC)	A framework for developing and managing software or systems that includes phases such as planning, design, development, testing, deployment, and maintenance.
Security incident	An event or occurrence that violates an organization's security policies and procedures, or threatens the confidentiality, integrity, or availability of its information assets.
Application security	The protection of software applications and their associated data from unauthorized access or attack.
Asset management	The process of identifying and classifying an organization's information assets and determining their value and risk.
Audit	A systematic review or examination of an organization's policies, procedures, controls, or operations to evaluate compliance, effectiveness, or risk.

Authorization matrix	A chart or document that outlines the access privileges of different roles or individuals in an organization.
Availability management	The process of ensuring that systems, services, or resources are available to meet business needs or service level agreements (SLAs).
Change management	The process of managing changes to systems, applications, or processes to minimize risk and ensure compliance.
Cloud computing	The delivery of computing services over the internet, including storage, processing, and software applications.
Code of ethics	A set of principles or standards that guide the professional conduct of individuals in a particular field or organization.
Compliance	The adherence to laws, regulations, standards, or policies that govern an organization's operations or practices.
Computer emergency response team (CERT)	A group of experts who are responsible for responding to and mitigating security incidents or threats.
Confidentiality agreement	A legal agreement that restricts the disclosure of confidential or sensitive information to third parties.
Cybersecurity	The protection of digital assets, networks, and information from cyber threats, attacks, or vulnerabilities.
Data backup and recovery	The process of creating copies of data and restoring it in the event of loss or corruption.
Data center	A facility that houses computer systems and equipment, including servers, storage devices, and networking infrastructure.
Data loss prevention (DLP)	A set of technologies and policies that prevent sensitive data from being transmitted, copied, or accessed without authorization.
Defense in depth	A security strategy that uses multiple layers of defense to protect systems and data, including physical, technical, and administrative controls.
Disaster recovery testing	The process of testing a disaster recovery plan to ensure that critical systems and data can be restored in the event of a disaster.
Due diligence	The process of conducting research, analysis, or investigation to assess risk or evaluate a business opportunity.
Endpoint security	The protection of devices, such as laptops, smartphones, and tablets, from cyber threats and attacks.
Governance	The set of processes, policies, and standards that guide the management and operation of an organization.
Incident response plan	A formal plan that outlines the steps to be taken in the event of a security incident, including detection, analysis, containment, and recovery.
Information assurance	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
Information security management system (ISMS)	A framework that includes policies, procedures, and controls for managing an organization's information security.
Insider threat	A security risk posed by individuals within an organization who have authorized access to systems or data.
Intellectual property	Legal rights that protect creative works, inventions, or other forms of intellectual property from unauthorized use or infringement.
Internet of Things (IoT)	A network of interconnected devices, objects, or machines that can communicate and exchange data over the internet.

Key performance indicator (KPI) - A	A metric or measure that is used to evaluate the performance or effectiveness of a process, function, or activity.
Least common mechanism	A security principle that states that components or functions should share the minimum amount of common resources or dependencies to reduce the risk of compromise or failure.
Mobile device management (MDM)	A set of policies, procedures, and technologies used to manage and secure mobile devices, such as smartphones, tablets, and laptops, that are used in a business or enterprise environment.
Network access control (NAC)	A security technology that controls access to a network based on user identity, device type, or other criteria.
Non-disclosure agreement (NDA)	A legal agreement that prohibits the disclosure of confidential information to third parties.
Open Web Application Security Project (OWASP)	An organization that provides guidance and resources for improving the security of web applications.
Personally identifiable information (PII)	Information that can be used to identify an individual, such as their name, address, social security number, or email address.
Physical access control	The use of physical barriers or security measures to prevent unauthorized access to buildings, rooms, or facilities.
Privacy	The protection of personal information from unauthorized disclosure or use.
Public key infrastructure (PKI)	A system that uses digital certificates and public and private key pairs to provide authentication and encryption for electronic communications.
Risk appetite	The level of risk that an organization is willing to accept or tolerate in pursuit of its objectives.
Security assessment	An evaluation of an organization's security posture or controls to identify vulnerabilities or weaknesses.
Security audit trail	A record of security-related events or actions that can be used for monitoring, analysis, or forensic investigation.
Security incident and event management (SIEM)	A system that aggregates and analyzes security-related data from multiple sources to identify threats and security incidents.
Security operations	The day-to-day management and monitoring of security controls and systems to ensure their effectiveness and compliance.
Security policy framework	A set of policies and guidelines that define an organization's security posture, responsibilities, and controls.
Separation of environments	The practice of isolating different environments or systems to prevent unauthorized access or data leakage.
Social media policy	Guidelines and rules that govern the use of social media by employees or representatives of an organization.