EXAM/CRAM

The CISSP Cram Sheet

This Cram Sheet contains the distilled, key facts about the exam. Review this information as the last thing you do before you enter the testing center, paying special attention to those areas where you feel that you need the most review.

Physical Security

1. Facility controls include:

   Lighting—Used to discourage crime and protect employees, the NIST standard states that the area should be illuminated at 2 feet wide by 8 feet high.

   Fencing—A 3- to 4-foot fence is deterrent; a 6- to 7-foot is hard to climb; 8 foot with three strands of barb wire acts as a serious deterrent.

   Perimeter controls include gates, guards, dogs, CCTV, turnstiles, mantraps, and alarms.

2. Locks can be:

   Cipher locks—Programmable

   Preset locks—Warded or pin and tumbler

   Device locks—Used to prevent the theft of equipment

3. Facility management requires review of the facility:

   Proper construction and design should give attention to walls, doors, ceilings, windows, flooring, HVAC, and fire detection and suppression. Must know where cut-off valves and switches are located.

   The computing area should be neither on the top floor nor in the basement. It should be near the core of the building and offer protection on all six sides.

   HVAC should be separate for the data center and have positive pressurization to keep contaminants and smoke out of the facility.

4. The following are common power anomalies:

   Blackout—Prolonged loss of power

   Brownout—Power degradation that is low and less than normal

   Sag—Momentary low voltage

   Fault—Momentary loss of power

   Spike—Momentary high voltage

   Surge—Prolonged high voltage

   Noise—Interference superimposed onto the power line

   Transient—Noise disturbances of a short duration

   Inrush—Initial surge of power at startup

5. Hardware-protection mechanisms and expected life controls include:

   SLAs—Ensure that vendors will provide the necessary maintenance and uptime

   MTBF—Used to calculate the expected lifetime of the device

   MTTR—Used to estimate the amount of time between repairs

6. Fire-suppression methods include:

   Class A—Paper or wood; suppressed with water or soda acid

   Class B—Gasoline or oil fires; suppressed by using CO_2, soda acid, or halon

   Class C—Electronic or computer fires; suppressed by using CO_2, FM200, or halon

   Class D—Fires caused by combustible metals; suppressed by applying dry powder or using special techniques

7. Halon, an effective fire suppressant, is a banned substance because it depletes ozone.

   Halon 1211—This type is found in portable extinguishers and is stored as a liquid.

   Halon 1301—This version is used in fixed flooding systems and is stored as a gaseous agent.

8. Halon fire-suppression systems can be left in place, but there are strict regulations on reporting discharges. EPA-approved replacements include FM-200, CEA-410, NAF-S-III, and FE-13. FE-13 is one of the newest and safest up to 30% saturation tolerable.

9. Water sprinklers are an effective means of extinguishing Class A fires. Four variations are available:

   Dry pipe—Maintains no standing water. It reduces the risk of accidental flooding and gives some time to cover or turn off electrical equipment.

   Wet pipe—Widely used and ready for activation. This system is charged and full of water.

   Preaction—A combination system. Pipes are initially dry and filled with compressed air.

   Deluge—Not suitable for data centers, a large volume of water capable of covering a large area quickly.

Access Control Systems

10. Subject, an active entity. Object, a passive entity. Mode of access, read, write, or execute.

11. Granularity, the ability to which an access control system can be regulated.

12. Biometric systems include:

    FRR—The false rejection rate or Type I error is the percentage of valid users who are falsely rejected.

    FAR—The false acceptance rate or Type II error is the percentage of invalid users who are falsely accepted.

    CER—The crossover error rate is the point at which the False Rejection Rate equals the False Acceptance Rate.

13. Cognitive passwords are facts used to verify identity such as maiden name, pet, high school, and so on.

14. Zephyr charts compare different types of biometric systems.

15. Centralized access control, such as RADIUS, TACACS, TACACS+, and Diameter, can be used to maintain user IDs, rights, and permissions in one central location.

16. Diameter is unique because it provides services for tablets, handheld devices, and mobile devices.

17. Access control categories:

    Technical—Examples include encryption, authentication, network segmentation, and anti-virus.

    Physical—Examples include locks, fences, guards, lights, video, and physical IDs.

    Administrative—Examples include policies, procedures, training, and pre-employment checks.

    Controls—Each can be applied as preventive, detective, deterrent, corrective, compensating, or recovery.

18. Access control models are established to control how subjects can access data and what the user's level of authorization is. The three primary models include:

    The DAC model is so titled because the user controls who has access to the system he maintains; uses ACLs.

    The MAC model bases looks to the system to determine access. The MAC model is typically used by organizations that handle highly sensitive data and is based on labels.

    The role-based access control model is considered nondiscretionary. RBAC place users into groups and implicitly assigns access. Used by companies with high turnover.

19. Intrusion detection can be signature, statistical, or anomaly based, and is host or network based.

Cryptography

20. Cryptography can be used for confidentiality, integrity, authentication, or nonrepudiation.

21. Internet security applications include SET, developed by MasterCard and Visa; SSH, a secure replacement for Telnet; TLS/SSL, both used to protect web communications; IPSec, the standard for VPNs and secure communication.

22. Symmetric cryptography works by providing both parties with the same key for encryption and decryption. It provides confidentiality and is hard to break. Its weakness is that the keys are subject to exposure and must be transmitted through a channel other than the message.

23. Data Encryption Standard (DES) is a block encryption algorithm based on IBM's 128-bit algorithm; 56 bits make up the key and 8 bits are used for parity. The four primary modes of DES include

    Electronic Code Book (ECB)—Native encryption mode used for small amounts of data. ECB is the weakest form of DES.

    Cipher Block Chaining (CBC)—Works by taking each datum from the previous and applying it to the next.

    Cipher Feedback Mode (CFB)—Emulates a stream cipher and can be used when the encryption of individual characters is required.

    Output Feedback Mode (OFB)—Also emulates a stream cipher and generates random binary bits that are combined with the plain text to create cipher text and does not propagate errors. OFB can also emulate a stream cipher.

24. Asymmetric algorithms use two different keys. The advantage is that key distribution is easier. Asymmetric algorithms are not as fast as symmetric systems.

25. Asymmetric algorithms include Diffie-Hellman, El Gamal, and Elliptic Curve Cryptosystem algorithms.
26. Hashing algorithms work well for integrity verification and include the MD series, HAVAL, Tiger, and SHA.
27. A public key infrastructure (PKI) allows individuals using the Internet to obtain and share cryptographic keys from a trusted authority. The PKI consists of four basic components and is governed by the X.509 standards:

    Certificate Authority (CA)—Used to verify and issue digital certificates. The certificate includes the public key and information about it.

    Registration Authority (RA)—Verifies authenticity for the CA. Cannot issue certificates.

    Repository—Accepts certificates and distributes them to authorized parties.

    Archive—Responsible for the long-term storage of archived information distributed from the CA.
28. Terms to know: one-time pad, Vigenére cipher, block cipher, stream cipher, key escrow, and Kerckhoff's principle.

Security Architecture and Design

29. The Trusted Computing Base (TCB) is the combination of protection mechanisms, including hardware, software, and firmware, that maintain security within a computer system.
30. The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects.
31. The security kernel implements the reference monitor concept. The reference monitor concept has the following properties:
    - Provides isolation
    - Is invoked for every access attempt
    - Is impossible to circumvent and be foolproof
    - Is complete, verified, and tested
32. Resource isolation is the process of segmentation so that memory is separated physically, not just logically.
33. Rings of protection are used to isolate processes. Ring 0: OS, ring 1: remaining parts of the OS, ring 2: utilities and I/O, ring 3 applications and programs. Lower numbers have higher levels of privileges.
34. Security models define the structure by which data structures and systems are designed to enforce security policy. Well-known security models include:

    Bell-LaPadula—Enforces confidentiality and uses rules: the simple security rule (no read up) and the * property (no write down).

    Biba—Integrity model that has two basic rules: the star property (no write up) and simple integrity (no read down). The only addresses model one goal of integrity.

    Clark-Wilson—Integrity model with three goals: maintaining consistency, preventing unauthorized access, and preventing improper modification. Properties include tamperproof, logged, and consistent.

    Brewer Nash—Prevents conflicts of interest also known as the Chinese Wall.

    State machine—Basis of the Bell-LaPadula and Biba model. Concerned with state transaction and modes of operation.
35. Security evaluation models—TCSEC (Orange Book) is used for system ratings, includes A1, B3, B2, B1, C1, C2, and D. Other models include ITSEC and Common Criteria.

Telecommunications and Network Security

36. Authentication protocols: PAP is clear text; CHAP, challenge response with periodic reauthentication; EAP is advanced authentication techniques such as smart cards.
37. ARP poisoning sends fake ARP packets to change ARP cache tables and redirect traffic.
38. DNS spoofing is much like ARP poisoning, except the attack attempts to poison the DNS cache. Victims can be redirected to wrong Internet sites.
39. Sniffing is a passive attack that requires the attacker to gain some type of access to the network. Any clear-text information is at risk. FTP, Telnet, SMTP, and SNMP can be targets. MITM attacks can undermine crypto such as SSL and SSHv1.
40. POTS is a voice-grade analog telephone service used for voice calls and for connecting to the Internet and other locations via modem.
41. ISDN is a communication protocol that operates similar to POTS, except all digital signaling is used. ISDN uses separate frequencies called *channels*. It is configured as follows:

    ISDN BRI—Two 64Kbps B channels and one 16-kbps D channel

    ISDN PRI—Twenty-three 64Kbps B channels (US) and one 16-kbps D channel
42. The seven layers of the Open Systems Interconnect models are application, presentation, session, transport, network, data link, and physical.
43. TCP/IP is the foundation of the Internet as we know it today. TCP/IP is similar to the OSI model but consists of only four layers. TCP/IP includes:

    TCP—A reliable, slow, and connection-oriented protocol that ensures that packets are delivered to the destination computer

    UDP—A fast, best-effort, non-connection-oriented protocol
44. Internal routing protocols can be divided into two broad categories:

    Distance-vector protocols—RIP

    Link-state protocols—OSPF
45. TCP/IP data can be addressed as a unicast to one particular system; a multicast, which targets a group; or a broadcast, which goes to all systems.
46. Data can be transmitted in two fundamental methods: analog and digital. Each converts the signal to a binary value.
47. Information can move in two ways:

    Asynchronous communication—Two devices are not synchronized in any way.

    Synchronous communication—Two devices are synchronized and usually controlled by a clocking mechanism.
48. Baseband transmission means the entire cable is used for the transmission of data so that only one thing can happen at a time.
49. Broadband transmission means the cable is divided into channels so that different types of data can be transmitted all at the same time.
50. Firewalls focus security to one point and don't protect against insiders behind the firewall.
51. Common firewall terms include:

    Demilitarized zone (DMZ)—A network segment that is located between the protected and the unprotected networks.

    Bastion host—A device that has been hardened and is to be deployed in the DMZ to run specific services.

    Packet filtering—Considered a first level of defense. Access is based on rules.

    Stateful packet filtering—Method of control that keeps a state table to keep track of activity and control access.

    Proxy—Stands between the trusted and untrusted network.
52. WAP gap—If an attacker can compromise the gateway, he would be able to access all the secure communications traversing the network juncture.

Business Continuity and Disaster Recovery Planning

53. No demonstrated recovery exists until the BCP plan has been tested.
54. Backup types—Incremental backup copies only on files that have changed since the last backup. Differential backup copies any files that have changed since the last full backup. Full backups copy everything.
55. BCP testing includes:

    Checklist—Copies of the plan are sent to different department managers and business unit managers for review.

    Tabletop—Members of the emergency management team and business unit managers meet in conference to discuss the plan.

    Walkthrough—Simulation of the real event using only what would be available in a disaster.

    Functional—Operations of the new and old site can be run in parallel.

    Full interruption—A complete a test of the BCP plan is performed.
56. Subscription services include:

    Cold site—An empty room with only rudimentary electrical, power, and computing capability

    Warm site—Partially configured

    Hot site—Ready to go; an expensive option

Legal, Regulations, Investigations, and Compliance

57. The ISC² code of ethics states that CISSPs will:

    Protect society, the commonwealth, and the infrastructure

    Act honorably, honestly, justly, responsibly, and legally

    Provide diligent and competent service to principles

    Advance and protect the profession

58. RFC 1087 states that the following activities are unethical:

    Seeking to gain unauthorized access to the resources of the Internet

    Disrupting the intended use of the Internet

    Wasting resources (people, capacity, computer) through such actions

    Destroying the integrity of computer-based information

    Compromising the privacy of users

59. The chain of custody examines who collected, transported, stored, controlled, and accessed the evidence.

Software Development Security

60. Polyinstantiation allows different records to exist in the same table at various security levels.
61. Database models can be relational, using attributes (columns) and tuples; hierarchical, combining records and fields in a logical tree structure; or distributed, storing information in more than one database.
62. The software development life cycle includes the following stages: project initiation, functional design and planning, system design, functional review, software development, product installation, operation and maintenance, and disposal and replacement.
63. Software development models include waterfall, spiral RAD, JAD, CASE, and prototyping.

Security Operations

64. Operational security can be enhanced by implementing good employee controls, such as new hire orientation, background checks, separation of duties, job rotation, least privilege, and mandatory vacations.
65. Penetration testing is the process of evaluating the organization's security measures. These tests can be performed in a number of ways, including internal, external, white box testing, and black box testing.
66. Clipping levels are the thresholds implemented for certain types of errors or mistakes that are allowed without alarm.
67. Clustering is suitable for high security projects, whereas distributed computing is not.
68. RAID can be used for fault tolerance and speed. The most used levels are 0, 1, and 5.

Risk Management Practices

69. Three goals of risk management are to identify risks, quantify the impact of potential threats, and find an economic balance between the impact of the risk and the cost of the countermeasure.
70. A threat is a natural or manmade event that could have a negative impact on the organization. A vulnerability is a flaw, loophole, oversight, or error that makes the organization susceptible to attack or damage.
71. There are two approaches to dealing with risk:

    Quantitative analysis—Assigns real numbers or dollar amounts to the costs of countermeasures and the amount of damage that can occur. Pure quantitative risk analysis is not possible.

    Qualitative analysis—Looks at different scenarios of risk possibilities and ranks the seriousness of the threats and the sensitivity of the assets.

72. Formulas used for quantitative analysis include:

    EF (exposure factor) = Percentage of an asset loss caused by an identified threat

    SLE (single loss expectancy) = Asset value ? Exposure factor

    ARO (annualized rate of occurrence) = Estimated frequency a threat will occur within a year

    ALE (annualized loss expectancy) = Single loss expectancy ? Annualized rate of occurrence

73. Other types of qualitative assessment techniques include:

    The Delphi Technique—A group assessment process that allows individuals to contribute anonymous opinions.

    Facilitated Risk Assessment Process (FRAP)—Obtains results by asking questions. It is designed to be completed in a matter of hours.

74. Risk is dealt with in the following ways (these can be combined):

    Risk reduction—Implements a countermeasure to alter or reduce the risk

    Risk transference—Purchases insurance to transfer a portion of or the entire potential cost of a loss to a third party

    Risk acceptance—Deals with risk by accepting the potential cost and loss

75. Security policies can be regulatory, advisory, or informative.
76. Senior management is ultimately responsible.
77. Types of security documents include:

    Policies—General statements produced by senior management

    Standards—Tactical documents that are more specific than policies

    Guidelines—Point to a statement in a policy or procedure by which to determine a course of action

    Procedures—The lowest level in the policy that provide step-by-step instructions to achieve a certain task