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.

Logical and Physical Asset Security

1. Facility controls include:

   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—Gates, guards, dogs, CCTV, turnstiles, mantraps, and alarms.
2. Locks can be:

   Cipher locks—Programmable

   Preset locks—Warded or pin and tumbler
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. Lighting is used to discourage crime and protect employees, the NIST standard states that the area should be illuminated at 2 foot wide by 8 foot high.
6. Fire-suppression methods include:

   Class A—combustibles, paper or wood; suppressed with water or soda acid

   Class B—Gasoline or oil fires; suppressed by using CO2, soda acid, or halon

   Class C—Electronic or computer fires; suppressed by using CO2, FM200, or halon

   Class D—Fires caused by combustible metals; suppressed by applying dry powder or using special techniques
7. Data access does not extend indefinitely, all data objects must have owners, users tend to gain more access over time than what is needed
8. International property laws protect trade secrets, trademarks, patents, and copyrights.
9. A data warehouse is a database that contains data from many different data-bases, whereas data mining is the process of analyzing data to find and under-stand patterns and relationships about the data.
10. PCI DSS version is comprised of six control objectives that contain one or more requirements.

Security and Risk Management

11. 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.
12. 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.
13. 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.
14. 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? x Exposure factor

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

    ALE (annualized loss expectancy) = Single loss expectancy? x Annualized rate of occurrence
15. Other risk management techniques include:

    Factor analysis of information risk (FAIR)—An add-on to existing risk frameworks that develops baselines of probabilities for the frequency and magnitude of loss events.

    Risk factor analysis—Another approach to risk analysis that uses a six step methodology to identify factors that drive the behavior of the project schedule, cost, and technical performance.

    Probabilistic risk assessment—Designed for use with large-scale complex projects where risk is defined as a feasible detrimental outcome. The results are expressed numerically.
16. Risk is dealt with in the following ways (think ATM):

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

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

    Risk mitigation—Implements a countermeasure to alter or reduce the risk
17. Security policies can be regulatory, advisory, or informative.
18. Senior management is ultimately responsible.
19. 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

Security Engineering

20. The Trusted Computing Base (TCB) is the combination of protection mechanisms, including hardware, software, and firmware, that maintain security within a computer system.
21. The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects.
22. 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
23. Resource isolation is the process of segmentation so that memory is separated physically, not just logically.
24. Protection Rings 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.
25. 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—Enforces Integrity 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. Remember this integrity model has an “i” in its name.

    Clark-Wilson—Integrity model that enforces all goals of integrity maintaining consistency, preventing unauthorized access, and preventing improper modification. Properties include tamperproof, logged, and consistent.

    State machine—Basis of the Bell-LaPadula and Biba model. Concerned with state transaction and modes of operation.
26. 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 Com-mon Criteria, EAL 1-7.

The Application and Use of Cryptography

27. Cryptography can be used for privacy, integrity, authentication, or nonrepudiation. Remember “PAIN”.
28. Internet security applications include; SSH, a secure replacement for Telnet; TLS/SSL, both used to protect web communications; IPSec, the standard for VPNs and secure communication.
29. 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.
30. 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 ECB, CBC, CFB, and OFB.
31. Asymmetric algorithms use two different keys. The advantage is that key distribution is easier. Asymmetric algorithms are not as fast as symmetric systems.
32. Asymmetric algorithms include Diffie-Hellman, El Gamal, and Elliptic Curve Cryptosystem algorithms.
33. Hashing algorithms work well for integrity verification and include the MD series, HAVAL, Tiger, and SHA.
34. 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.
35. Terms to know: one-time pad, Vigenére cipher, block cipher, stream cipher, key escrow, and Kerckhoff’s principle.

Telecommunications and Communications and Network Security

36. ARP poisoning sends fake ARP packets to change ARP cache tables and redirect traffic.
37. DNS spoofing is much like ARP poisoning, except the attack attempts to poison the DNS cache. Victims can be redirected to bogus Internet sites.
38. Security DNS (DNSSEC) is an alternative to DNS. With DNSSEC, the DNS server provides a signature and digitally signs every response.
39. Storage area networks (SANs) are networks of storage disks and devices. SANs connect multiple servers to a centralized pool of disk storage.
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 including application, transport, Internet, and Network Access. TCP/IP includes:

    TCP—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. Wireless modes include, open, WEP (weak) WPA (short term fix), WPA2 (newest, uses AES and CCMP for integrity).

. Data can be transmitted in two fundamental methods: analog and digital. Each converts the signal to a binary value.

. 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.

. Baseband transmission means the entire cable is used for the transmission of data so that only one thing can happen at a time.

. Broadband transmission means the cable is divided into channels so that different types of data can be transmitted all at the same time.

. Firewalls focus security to one point and don't protect against insiders behind the firewall.

. 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.

. Port mirroring is used to send a copy of network packets seen on one switch port to a network monitoring connection on another switch port.

dentity and Access Management

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

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

. 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.

56. Cognitive passwords are facts used to verify identity such as maiden name, pet, high school, and so on.
57. Controls can be applied as preventive, detective, deterrent, corrective, compensating, or recovery.
58. Centralized access control, such as RADIUS, TACACS, TACACS+, and Diameter, can be used to maintain user IDs, rights, and permissions in one central location.
59. Diameter is unique because it provides services for tablets, handheld devices, and mobile devices.
60. 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.
61. 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/she 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 places users into groups and implicitly assigns access. Used by companies with high turnover.

Security Assessment and Testing

62. Honeypots, fake systems designed to fool and distract an attacker.
63. Penetration testing is the process of evaluating the organization's security measures. These tests can be performed in a number of ways, including white box testing, black box testing, and gray box testing.
64. Some C functions are susceptible to buffer overflow and can be exploited be-cause they do not check for proper buffer size.
65. A sniffer is a packet-capturing program that captures network traffic and can decode the captured frames.
66. Passwords are susceptible to dictionary, hybrid, brute force, and rainbow table password attacks
67. Spoofing can best be defined as the act of pretending to be something other than what you are.
68. Rootkits are a collection of tools that allow an attacker to take control of a sys-tem and can be hard to detect.
69. Forensics requires evidence to be acquired (bit-for-bit copy), authenticated (hashing MD5, SHA, etc), and analyzed (copies of the disk, protect original).
70. Chain of custody is the process of documenting the journey of any and all evi-dence (who collected, transported, stored, controlled, and accessed it) while keeping it under control.

Security Assessment

71. 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.
72. Clipping levels are the thresholds implemented for certain types of errors or mistakes that are allowed without alarm.
73. Clustering is suitable for high security projects, whereas distributed computing is not.
74. RAID can be used for fault tolerance and speed. The most used levels are 0, 1, and 5.
75. Intrusion detection can be signature, statistical, or anomaly based, and is host or network based.
76. 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
77. 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

Software Development Security

78. Secure software development includes: DCOM (Microsoft only), SOAP (extension to DCOM), EJB (server-side JAVA app) and CORBA (middleware, applied to distributed systems.)
79. Database models include 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.
80. The software development life cycle includes the following: project initiation, functional design and planning, system design, functional review, software development, product installation, operation and maintenance, and disposal and replacement.
81. DevOps is the emerging practice of collaboration between software developers and IT professionals.

Business Continuity Planning

82. Key BCP terms include:

    CBF—Functions that the company cannot live without

    MTD—The amount of time a business can survive without a CBF.

    RPO—How current the data must be or the amount of tolerable data loss.

    RTO—Used to describe the amount of time for a a business for a CBDF to be restored at a recovery location
83. Protection mechanisms and expected life controls include:

    SLAs—Ensure that vendors will provide the necessary maintenance and up-time

    MTBF—Used to calculate the expected lifetime of the device
84. No demonstrated recovery exists until the BCP plan has been tested. 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 walk-thru 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[md]A complete a test of the BCP plan is performed.
85. Subscription services include:

    Cold site—An empty room with only rudimentary electrical, power, and com-puting capability

    Warm site—Partially configured

    Hot site—Ready to go; an expensive option