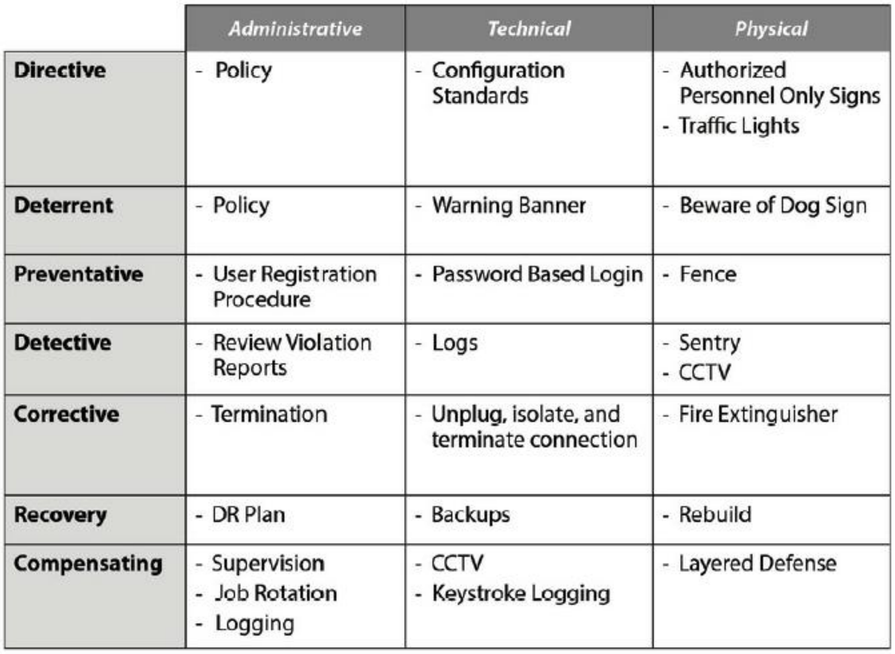
CISSP Important Points from Exam Point view-:

1. Never spend more on a control than what the access is worth
2. In Company Security Training and Awareness is Mandatory
3. Senior Management is overall Accountable for Information Security and they only the one who accept risk
4. Risk Transfer – You can transfer Financial Risk only
5. Whatever we perform in organization is come from policy
6. VPN Form Trusted Network
7. Confidentiality = Access Control, Least Privilege and Need to Know
8. Integrity = Hashes,Checksum,Dual Control,
9. Availability = Contingency Planning ,BCP, Backup
10. Access control type and Categories



	Administrative	*Technical*	*Physical*
Directive	- Policy	- Configuration Standards	- Authorized Personnel Only Signs - Traffic Lights
Deterrent	- Policy	- Warning Banner	- Beware of Dog Sign
Preventative	- User Registration Procedure	- Password Based Login	- Fence
Detective	- Review Violation Reports	- Logs	- Sentry - CCTV
Corrective	- Termination	- Unplug, isolate, and terminate connection	- Fire Extinguisher
Recovery	- DR Plan	- Backups	- Rebuild
Compensating	- Supervision - Job Rotation - Logging	- CCTV - Keystroke Logging	- Layered Defense

11. Policy = Express Management Intents
    - Standard = what is required
    - Procedures = How do I do it
12. Governance = Set of Operation (Policy,standard,baseline and due diligence)
13. Budget = Number of Controls, Level of Security ,what task to be performed ,Requirement of training ,Metrics Tracking
14. Need to Know= Military .Access Decide on the based on Need to Know
15. Due Care = Is the Act of Compliance
16. Assurance = Is Due Diligence

17. PCI = Payement Card Industry is a Contract law
18. Intellectual Property =
    - Patent= Protect Novel Ideas (20 Years from Date of Application)
    - Copyright = 70 Years ,work of Author
    - Trademark law= Symbol logo
    - Trade Secret = Taste Buisness Process (Coca Cola,Pepsi)
19. Privacy = The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.
20. Event = An event is an observed change to the normal behavior of a system, environment, process, workflow or person. Examples: router ACLs were updated, firewall policy was pushed.
21. An alert = Is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action. Examples: the events above sent to on-call personnel.
22. Incident = Is a human-caused, malicious event that leads to (or may lead to) a significant disruption of business. Examples: attacker posts company credentials online, attacker steals customer credit card database, worm spreading through network.*
23. Breach = Incident that Disclosure data
24. Ethics
    - Code of Ethics Preamble:
        - The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
        - Therefore, strict adherence to this Code is a condition of certification.
    - Code of Ethics Canons:
        - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
        - Act honorably, honestly, justly, responsibly, and legally.
        - Provide diligent and competent service to principals.
        - Advance and protect the profession.
25. BCP
    - DRP is a part of BCP
    - BCP = “"*if we lost this building how would we recommence our business?"*
    - DRP = “*if we lost our IT services how would recover them*?"
    - • Business Continuity Plan (BCP)—A long-term plan to ensure the continuity of business operations.
    - • Continuity of Operations Plan (COOP)—A plan to maintain operations during a disaster.

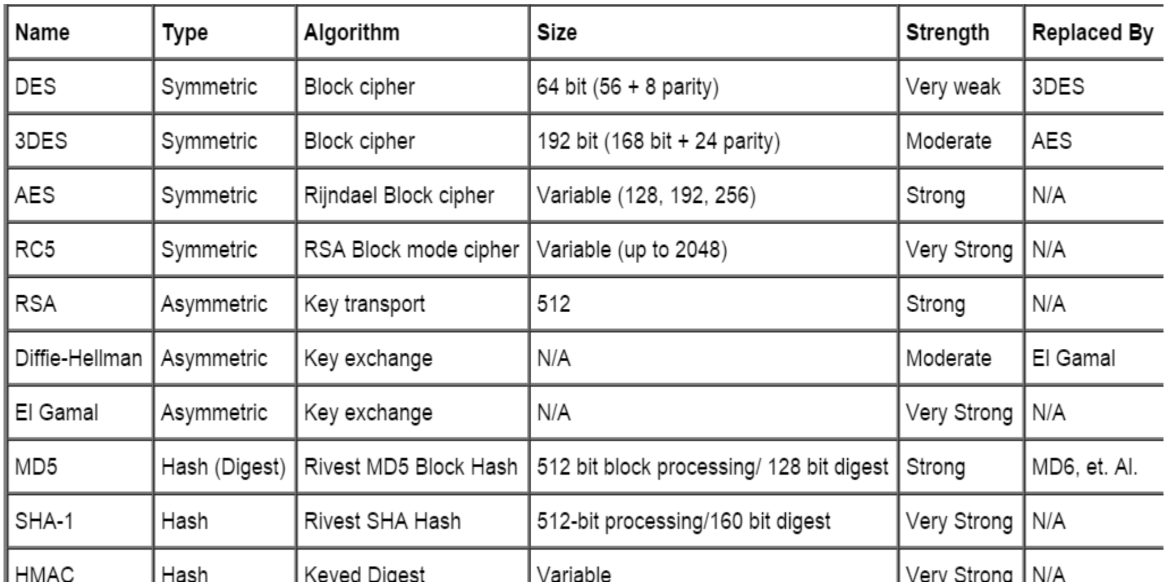
- Disaster—Any disruptive event that interrupts normal system operations.
- Disaster Recovery Plan (DRP)—A short-term plan to recover from a disruptive event.
- Mean Time Between Failures (MTBF)—Quantifies how long a new or repaired system will run on average before failing.
- Mean Time to Repair (MTTR)—Describes how long it will take to recover a failed system.
- BCP Process
  - Project Initiation
  - Scope the Project
  - Business Impact Analysis
  - Identify Preventive Controls
  - Recovery Strategy
  - Plan Design and Development
  - Implementation, Training, and Testing
  - BCP/DRP Maintenance
- BIA = IT systems and components. A template for developing the BIA is also provided to assist the user. The BIA is comprised of two processes: (1) identification of critical assets, and (2) comprehensive risk assessment.

26. Employment candidate screening
    - job Descriptions,
    - Reference checks
      Background investigations
      Education, licensing, certification verification
27. Job Rotation = Reduce Fraud
28. Job Description = Need to Know and Least Privilege
29. Mandatory Vaccation = Detectiing Frauds
30. Type of Termination
    - Voluntary
    - Involuntary
31. Third Party Control = Vendors, Contractors and Independent Consultant
32. Risk Management = Collection of Risk Identification,Analysis,Risk Evaluation and Risk Treatment
    - Annualized loss expectancy—The cost of loss due to a risk over a year.
    - • Threat—A potentially negative occurrence.
    - • Vulnerability—A weakness in a system.
    - • Risk—A matched threat and vulnerability.
    - • Safeguard—A measure taken to reduce risk.
    - • Total Cost of Ownership—The cost of a safeguard.
    - • Return on Investment—Money saved by deploying a safeguard.

- Residual Risk = Risk left after countermeasure
- Risk Analysis
  - Qualitative = Subjective
  - Quantitative= Monetary (SLE = EF*ASSET Value) (ALE=SLE*ARO)

33. Human Safety is First in the Orgnaization
34. In Organization We Have Three Elements = People ,Process and Technology(First to Protect People)
35. Cryptography

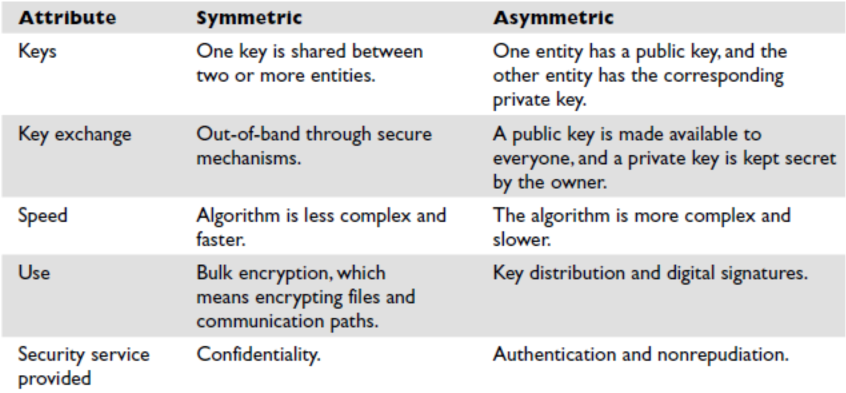
- • Plaintext—An unencrypted message.
- • Ciphertext—An encrypted message.
- • Cryptology—The science of secure communications.
- • Symmetric Encryption—Encryption that uses one key to encrypt and decrypt.
  - Block and Stream
- • Asymmetric Encryption—Encryption that uses two keys; if you encrypt with one, you made decrypt with the other.
- .Exclusive or – 1100 if different it's a 1 or if same its a 0
  1010
- • Hash Function—One-way encryption using an algorithm and no key.
- Below are the algorithms



Name	Type	Algorithm	Size	Strength	Replaced By
DES	Symmetric	Block cipher	64 bit (56 + 8 parity)	Very weak	3DES
3DES	Symmetric	Block cipher	192 bit (168 bit + 24 parity)	Moderate	AES
AES	Symmetric	Rijndael Block cipher	Variable (128, 192, 256)	Strong	N/A
RC5	Symmetric	RSA Block mode cipher	Variable (up to 2048)	Very Strong	N/A
RSA	Asymmetric	Key transport	512	Strong	N/A
Diffie-Hellman	Asymmetric	Key exchange	N/A	Moderate	El Gamal
El Gamal	Asymmetric	Key exchange	N/A	Very Strong	N/A
MD5	Hash (Digest)	Rivest MD5 Block Hash	512 bit block processing/ 128 bit digest	Strong	MD6, et. Al.
SHA-1	Hash	Rivest SHA Hash	512-bit processing/160 bit digest	Very Strong	N/A
HMAC	Hash	Keyed Digest	Variable	Very Strong	N/A

- DES Modes
  - 1. Electronic Code Book (ECB) = Block Mode , No IV
  - 2. Cipher Block Chaining (CBC) = Block Mode , IV
  - 3. Cipher Feedback (CFB) = Stream Mode , IV
  - 4. Output Feedback (OFB) = Stream Mode , IV
  - 5. Counter Mode (CTR) = Stream Mode. IV

- DH Algorithm = Discrete Logarithm
- Cryptography Attacks
    - Passive attack =Attack where the attacker does not interact with processing or communication activities, but only carries out observation and data collection, as in network sniffing.
    - Active attack=Attack where the attacker does interact with processing or communication activities.
    - Ciphertext-only attack = Cryptanalysis attack where the attacker is assumed to have access only to a set of ciphertexts.
    - Known-plaintext attack= Cryptanalysis attack where the attacker is assumed to have access to sets of corresponding plaintext and ciphertext.
    - Chosen-plaintext attack =Cryptanalysis attack where the attacker can choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts.
    - Chosen-ciphertext attack= Cryptanalysis attack where the attacker chooses a ciphertext and obtains its decryption under an unknown key.
    - Differential cryptanalysis= Cryptanalysis method that uses the study of how differences in an input can affect the resultant difference at the output.
    - Side-channel attack =Attack that uses information (timing, power consumption) that has been gathered to uncover sensitive data or processing functions.
    - Replay attack =Valid data transmission is maliciously or fraudulently repeated to allow an entity gain unauthorized access.
    - Meet-in-the-middle attack= Cryptanalysis attack that tries to uncover a mathematical problem from two different ends.
- Below Diagram Difference Between Symmetric and Asymmetric



Attribute	Symmetric	Asymmetric
Keys	One key is shared between two or more entities.	One entity has a public key, and the other entity has the corresponding private key.
Key exchange	Out-of-band through secure mechanisms.	A public key is made available to everyone, and a private key is kept secret by the owner.
Speed	Algorithm is less complex and faster.	The algorithm is more complex and slower.
Use	Bulk encryption, which means encrypting files and communication paths.	Key distribution and digital signatures.
Security service provided	Confidentiality.	Authentication and nonrepudiation.

- International Export Control
- PKI
    - X.509 Standard
    - Key Management Process
        - XKMS (XML Key Management System)

        - X-KRSS (XML Key Registration Service Specification) = For Registration
        - X-KISS (XML Key Information Services Specification)
    - Protocols such as SSL, PGP, and S/MIME use the services of KEKs to provide session key confidentiality, integrity, and sometimes to authenticate
    - A more scalable method of exchanging keys is through the use of a PKI key server
    - KDC (Key Distribution Center)
    - Key Escrow = Third Party Maintain copy of Private Key
    - OCSP is used for obtaining the revocation status of an X.509 digital certificate.

36. SDLC

- Memorizing the specific steps of each SDLC is not required, but be sure to understand the logical (secure) flow of the SDLC process.
- Security is part of every step of secure SDLC on the exam. Any step that omits security is the wrong answer. Also, any SDLC plan that omits secure disposal as the final lifecycle step is also the wrong answer.
- SDLC Phases
    - Conceptual Definition
    - Functional requirements determination
    - Control specification development
    - Design review
    - Code review walk through
    - System test review
    - Maintenance and change management
- Database
    - The data dictionary contains a description of the database tables. This is called metadata, which is data about data
    - Data definition language (DDL) and data manipulation language (DML). DDL is used to create, modify, and delete tables. DML is used to query and update data stored in the tables.
    - A database journal is a log of all database transactions.
    - Database Transaction have four Characteristics -; (Atomicity,Consisteny,Isolation and Durablity)
    - Database contamination :Mixing data with different classification levels and/or need-to-know requirements
    - Concurrency:uses a “lock” feature to allow one user to make changes
    - but deny other users access to views or make changes to data elements at the same time
    - Polyinstantiation used as a defense against some types of inference attacks
    - Polymorphism used as a defense against some type of aggregation attack

- Expert system has two main components: the knowledge base and the inference engine

37. Security Engineering

- The primary role of the security architect is to translate business requirements into solutions that provide security for key assets.
- System Components = Processors,Storage,Periherals and OS
- Multitasking. Multiprocessing and Multithreading
- Security Zone
- Zachman Framework = TOGAF
- Type of Security Models
  - State Machine Model
  - Multilevel Lattice Model
  - Noninterference Model
  - Matrix Based
  - Information Flow Model
- Bell-LaPadula = Confidentiality
  - Simple security rule = A subject cannot read data within an object that resides at a higher security level (the “no read up” rule).
  - *- property rule = A subject cannot write to an object at a lower security level (the “no write down” rule).
  - Strong star property rule = For a subject to be able to read and write to an object, the subject’s clearance and the object’s classification must be equal.

- Biba Model = Integrity
  - • *-integrity axiom = A subject cannot write data to an object at a higher Integrity level (referred to as “no write up”).
  - • Simple integrity axiom = A subject cannot read data from a lower integrity level (referred to as “no read down”).
  - • Invocation property = A subject cannot request service (invoke) of higher integrity.
  -
- Clark-Wilson Integrity Model = Extending of Integrity
- Brewer –Nash(Chinese Wall) = Conflicting of Interest
- Graham-Denning Model = (Set of Subjects, Set of Objects and Set of Right)
- Product Evaluation Models
  - TCSEC= DOD ,ORANGE BOOK

Evaluation Divison	Evaluation Class	Degree of Trust
A Verified Protection	A1 – Verified Design	Higest

B Mandatory Protection	B3 – Security Domains B2 – Structured Protection B1 – Labeled Security Protection	○
C –Discretionary Protection	C2 – Controlled Access Protection C1 – Discretionary Security Protection	○
D- Minimal Protection	D1 Minimal Protection	Lowest

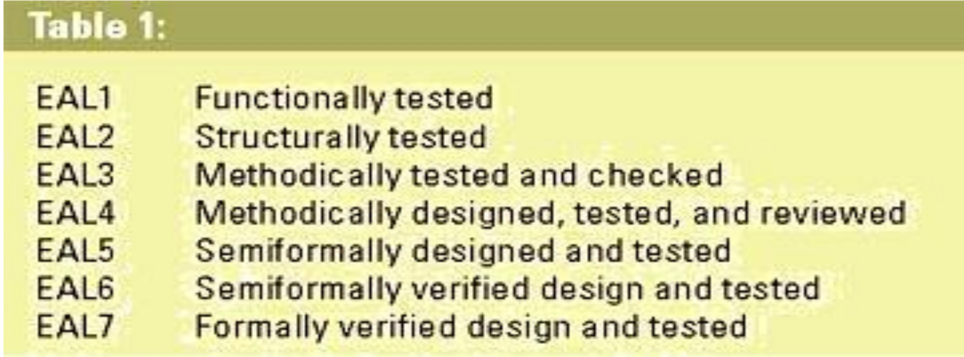
- Common Criteria = ISO/IEC 15408 (also Same)
  - PP (Protection Profiles)
  - TOE(Target of Evaluation)
  - Below are the Standard of Common Criteria (Need to Remember)
  - 

Table 1:

EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested, and reviewed
EAL5	Semiformally designed and tested
EAL6	Semiformally verified design and tested
EAL7	Formally verified design and tested

- ISO 27001 = ISMS Standard
- PCI DSS = Payment Card Industry
- Process Isolation
  - Ring 0 ,1 ,2 ,3 and 4

38. Communication and Network Security
    - You Need to Understand Protocols associated vulnerabilities and how it get Exploit
    - As a CISSP you can recommend which Protocol we can use
    - OSI

- ICMP
- Simplex, half duplex, and full duplex communication.
- Type of Wan technology
- TCP Ports
  - Well-Known Ports – Ports 0 through 1023
  - Registered Ports – Ports 1024 through 49151
  - Dynamic or Private Ports – Ports 49152 through 65535
- MPLS Is Very Important (Please Understand the Diagram how its work)
  - Label Edge Router (LER)
  - Label Switching Router
  - Egress Node
- VOIP and SIP
- Secure Design Network
  - Boundary Router
  - Secure Routing
- DMZ = Understand Placement of Host in DMZ and Secure Network
- Type of Attack = Please Go through all Attack Part

39. Security Operations
    - Security operations are primarily concerned with the daily tasks required to keep security services operating reliably and efficiently.
    - Operations security is a quality of other services and also a set of services in its own right.
    - Forensic Process
      - Identifying Evidence –
      - Collecting or Acquiring Evidence –
      - Examining or Analyzing the Evidence –
      - Presentation of Findings –
    - Locard's exchange principle states that when a crime is committed, the perpetrators leave something behind and take something with them,
    - MOM , SWGDE,IOCE
    - TRIAGE Phase = Detection, Identification, and Notification
    - Chain of Custody
    - Evidence Principle
      - Be authentic
      - Be accurate
      - Be complete
      - Be convincing
      - Be admissible
    - Criminal Investigation Components
      - Information, Instrumentation, and Interviewing
    - SIEM
      - Normalization and Aggregate
    - DATA in Rest
    - Data in Motion

- Data in Use
- Steganography and Watermarking
- SLA is Very Important
    - OLA
    - Indemnification
- Disposal Data
    - Degaussers can be used to erase data saved to magnetic media
- A successful incident management program combines people, processes, and technology
- RCA (Root Cause Analysis)

- IDS
    - HIDS
    - NIDS
- Dynamic application security testing (DAST) technologies are designed to detect conditions indicative of a security vulnerability in an application in its running state
- Patch and Vulnerability Management
- Change Management Process
    - Request
    - Impact Assessment
    - Approval / Disapproval
    - Build and Test
    - Notification
    - Implementation
    - Validation
    - Documentation
- Recovery Strategy
    - Type of Site
- Backup Strategy
    - RTO,RPO
- RAID = Type
- Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site.
- Journaling is a technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location.

40. Physical Security
    - Mantrap—A preventive physical control with two doors. Each door requires a separate form of authentication to open.
    - Smart Card—A physical access control device containing an integrated circuit.

- Tailgating—Following an authorized person into a building without providing credentials.
- Physical Safety is a prime concern for physical security domain
- Fence ,Gates
- Lighting levels of at least 10 to 12 foot-candles over parked cars and 15 to 20 foot-candles in walking and driving aisles is recommended.
- Fire Extinguisher Categories
    - (Fire Extinguisher Categories are important topic of CISSP. They Divided into four Catagories,but the challenge is how to memorize the which categories used where .So i am sharing some key note on this
    -
    - Class A = (Stand for Ash) -: Wood and Paper (
    - Class B = (Stand for Boil) =: Liquid,Flammable Gases
    - Class C = (Stand for Current) =: ElectricalCurrent
    - Class D = (Stand for Dilute) =: Combustible Metals
    -
    - Class A Extinguish with Water and Soda
    - Class B Extinguish With Gas and Soda Acid
    - Class C Extinguish With Non Conductive like gas
    - Class D Extinguish With Dry Powder
- Fire Detection System
- GAS Suppression System
    - Aero k
    - Fm 200

-