# CISSP CRIB SHEET

Risk = threat + impact + likelihood

**Quantitative RA (£)**

Single Loss Expectancy (**SLE**) = Asset Value (**AV-£**) x Exposure Factor (**EF-%**)

Annualised Loss Expectancy (**ALE-£**) = Single Loss Expectancy (**SLE**) x Annualised Rate of Occurrence (**ARO**)

**Qualitative RA (Rating Scale)**

**MAC** = Mandatory Access Control (labels)
**DAC** = Discretionary Access Control (**ACLs** - Access Ctrl Lists)
**Role Based Access Ctrl** (user in role or gp)
**Rule Based Access Ctrl** (user access based on global rules)

**ID Methods:** **Type 1:** Something you know (PIN, PW)
**Type 2:** Something you possess (smart card)
**Type 3:** Something you are (biometrics)

**Crossover Error Rate:** FAR-Type 2, FRR-Type 1
False Acceptance Rate & False Reject Rate

**Single Sign-On:** MS-Active Dir., Kerberos (KDC + TGS), SESAME

**Centralised Access Control:** RADIUS, TACACS, TACACS+, DIAMETER
AAA Protocol: Authentication, Authorisation, Accounting

**Decentralised Access Control:** Functional Manager assigns access

**IDS:** Network-based (DMZ) & Host-based (agent)

**2 methodologies to IDS:**
Knowledge/Signature based
Behaviour/Anomaly based

**The 3 Way Handshake = SYN – SYN & ACK – ACK**

**MAC Addr. – Media Access Control Addr.**
IEEE manage numbering spaces: MAC-48, EUI-48, EUI-64 (IPv6)
**ARP** – Address Resolution Protocol – used to find host MAC Addr. when only IP known

**IEEE 802.11** Set of WLAN Stds
802.11b & g use 2.4GHz band
802.11i (aka WPA2 uses AES block cypher)

**WEP:** 64(40+24 IV), 128 (104+24 IV)-RC4
**WPA:** 128 – TKIP & Michael (MIC)
**WPA2:** 128 – TKIP & Michael (MIC) + AES

| **OSI Model:** | **TCP/IP Model** | **Devices** |
|---|---|---|
| 7 **Application:** email – FTP, WWW, SNMP, SMTP, TFTP [GSS], Telnet [SSH], DNS | **Application** | |
| 6 **Presentation:** encrypt – ASCII, TIFF, JPEG, MPEG, MIDI, EDCDIC | | |
| 5 **Session** (message)**:** connect – SSL, NFS, SQL, PRC | | |
| 4 **Transport** (segments)**:** TCP, UDP, SPX | **Host to Host** | |
| 3 **Network** (packets)**:** route & address – IP, ICMP, RIP, OSPF, IPSEC | **Internet** | **Router** **FW** |
| 2 **Data Link** (frames)**:** switch – ARP(IP trans to MAC)RARP/DHCP (MAC to IP), PPP | SLIP **Network Access**, | **Bridge** **Switch** (tracks MAC Addr.) |
| 1 **Physical** (bits)**:** hub – X.21, EIA, HSSI | | **Hub** |

**Firewalls:**
1G – **Packet Filters** (using ACLs to examine packet header (port access) + accept or deny access) OSI 1-3
2G – **Proxy/Application Layer** – Circuit Level Gateways
- Application Proxies OSI 1-7
3G – **Stateful Packet Filters**-combines 1G + 2G with regard for each pkt placement in segment
4G – **Dynamic Packet Filters** –rec sess info (IP + port no) implements tighter sec posture than static packet filter

**Ports:** 1-1023 well known, 1024-49151 registered, 49152-65535 dynamic

**Firewall Topologies** – Screening Routers
– Screened host single homed bastion
– Screened host dual homed bastion
– Screened subnet (DMZ)
– Private subnet and dirty DMZ

**NAT**
Network Addr. Translation
Maps pte IP addr. to public IP addr.

**Cryptography:** DES, RSA, ROT13, IDEA, PGP, AES

**Asymmetric** = **Public Key Crypto:** RSA, ECC (cell phone), Diffle-Hellman [key distro only – modular arithmetic func. $Y^x$(mod P)], El Gamal (no encrypt),

**Symmetric** = **Private Key Crypto:** DES, 3DES, Blowfish, IDEA, RC4, SAFER, AES (Rijndael Algorithm-Block 128; Key 128, 192 & 256 bit)

**N(N-1)/2**

**Stream** – XOR – plaintxt digits encryp. One @ a time (bits) – approx action of OTPs – used for speed & simplicity of implement. in HW - RC4.

**Block** – plaintxt must be of std length eg 128bit – padding scheme is used to 'make up' blocks – Lucifer, DES, AES (3xblock cyphers)

**IV-Initilisation Vector**
**ECB-Elect. Code Book**
**CBC-Cipher Block Chaining**
**PCBC-PropagatingCBC**
**CFB-CipherFeedBack**
**OFB-OutputFeedBack**
**CTR-Counter**

**Hash** = RSA, MD2 4 5 (128), SHA (160 / DSA), HAVAL (var)

**Encryption Alternatives**

**SSL**– Secure Socket Layer (sessions occur on Port 443 by default)
**TLS** – Transport Layer Security
} Use symmetric crypto & keyed MAC (Msg Auth. Code) – hash function
**IPSec** – Tpt, Tunnel modes & Key Mgt
**Steganography** – hiding txt in image/data files

Associating a public key is typically done by protocols implementing a **Public Key Infrastructure (PKI):**
Hierarchical – CA – X.509
Local Trust Model – SPKI
Web of trust scheme - PGP

**Encryption Strength** (based on 3 factors)**:**
**1** Strength of algorithms
**2** Secrecy of keys
**3** Length of the key

**Circuit Switched NW:** Public Switched Telephone Nwk (PSTN)
**Packet Switched NW:** X.25, Frame Relay & ATM

**Security Architecture**

**Common Architecture Frameworks:** Zachman, SABSA, TOGAF, ITIL
**Creating and Doc. Sec. Architecture:** ISO27000, COBIT
**Verifying Sec. Architecture:** Control Objectives for Information and related Technology

**Confidentiality Models**
**Bell-LaPadula** = confidentiality; no read up / no write down (*-property rule)

**ISO 15408** – standard for computer security

**Integrity Models**
**Biba** = integrity; no read down / no write up
**Clark-Wilson**= audit, separation of duties, access through programs (internal consistency)

**Trusted Computer System Evaluation Criteria (TCSEC)** = The 'Orange Book' - US DoD standard, part of the rainbow series.
Coined the acronym **TCB** Trusted Computing Base.

**Orange** – computer systems - classification
**Red** – networks
**Green** – password management

**Common Criteria**

**Information Technology Security Evaluation Criteria (ITSEC)** = separate ratings for functionality & assurance – 10 predefined functionality classes (FC).

**RAID:**
Redundant Array of Indep. Disks
**0:** Stripe
**1:** Mirror & Duplexing
**3:** Striping - Byte
**4:** Striping - Block
**5:** Stripe & Parity (N+1)
**10:** 1 + 0 (Raid0 HDD Mirrored)
Requires 3 HDDs min

**Backup Concepts:** Full
Incremental
Differential

**Evidence Life Cycle:**
- ID & Collect
- Analyse
- Preserve
- Store
- Present
- Return

**BCP**
- Scope & Plan Initiation
- Buiss. Impact Ass. (BIA)
- Plan Development
- Plan Approval & Implementation

**DRP**
- Data Proc. Cont. & Plan Maint.
- Testing the Plan
- Recovery Procedures

**MTBF** – Mean Time Between Failure
**MTTR** – Mean Time To Recovery

**Fire Ext. (Class):**
A – Common Combustibles
B – Flammable or Combustible liquids
C – Electrical Eqpt
D – Combustible Metals

**Temp:**
70 – 74°F

**Humidity:**
40 – 60%

**Power Definitions**

**Fault** Momentary loss of pwr
**Blackout** Complete loss of pwr
**Sag** Momentary low voltage
**Brownout** Prolonged low voltage

**Spike** Momentary high voltage
**Surge** Prolonged high voltage
**Inrush** Initial surge of power
**Noise** Steady interference

**Transient** Short duration of line noise
**Clean** Non-fluctuating pwr
**Ground** One wire is grounded