

ISC2 Ethics: PAPA = Protect, Act, Provide, Advance.

CIA: Confidentiality, Integrity, Availability (opposite of **DAD**).

Due Diligence: Do Detect | **Due Care:** Do correct.

Security Labels: "*U Should Count Six Tauntauns*" = **Unclassified**, **Sensitive But Unclassified**, **Classified**, **Secret**, **Top Secret**.

Defense in Depth: Layering, or Onion defense.



Security through obscurity: Data Hiding.

RMF: "*Crime Scene Investigators Always Act Modestly*" = **Categorize**, **Select**, **Implement**, **Assess**, **Authorize**, **Maintain**.

COBIT: Has IT in it; IT governance.

Quantitative Risk Analysis:

ALE = SLE x ARO: *ArROw SLEd* = ALE is beer, so "A Drunk guy shooting arrows on a sled".

SLE = AV x EF: (Mario saying): "I've got something up my **sleav-ef**".

ISO: "*Raging Crackheads Risk Health*" = Requirements, Code of practice, Risk Management, Health (ISO27001, 27002, 27005, 27799).

Security Models: Simple/**R** = read ; ***/W** = write ; **U** = UP ; **D** = DOWN

Bell LaPadula: Confidentiality – Simple **N R U** || *** N W D** || Strong *** N R/W** U/D.

Biba: Integrity – Simple **N R D** || *** N W U** || Invocation **N R/W U**.



Access Control types: **2C - 3D - PR** = **corrective compensating**, **detective deterrent directive**, **preventative recovering**.

Hashing: **HA** or **MD** in the name.

Asymmetric: **DEREK-Q** = Diffie, El Gamal, RSA, ECC, Knapsack, Quantum.

Symmetric: **23BRAIDS** = **2**fish, **3**DES, **B**lowfish, **R**C5, **A**ES, **I**DEA, **D**ES, **S**kipjack.

23

Ciphers: Stream = RC4 / Block - Everything else.

Fire Extinguisher Classes: **A** (Ash) Combustible, **B** (Boil) Liquid, **C** (Current) Electrical, **D** (Dent) Metal, **K** (Kitchen) Oil/Fat.

CPU Pipelining order: **FDEW** = **Fetch**, **Decode**, **Execute**, **Write**.

OSI Model:

Physical, Datalink, Network, Transport, Session, Presentation, Application.

Layer 1-7: Please **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way.

Layer 7-1: All **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing.

TCP/IP Model:

NITA - Network access, Internet, Transport, Application.



Thor's Mnemonics - CISSP® and CISM®

Threat Modeling:

STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, DoS, Escalation of privilege.

DREAD: Damage, Reproducibility, Exploitability, Affected users, Discoverability.

4 Ds of Physical Security: Deter → Deny → Detect → Delay.

Evaluation Assurance Level (EAL):

FSMM-SSF: For Sure My Mother-So Sweet Forever.

Fun Stress Method Medical-Doctors Seem Somewhat Verifiably Foolish.

Functionally, Structurally, Methodically, Methodically Designed, Semi-formally, Semi-formally Designed, Verified, Formally Verified.

Multi-Factor Authentication:

Something you **know**, something you **have**, something you **are**.

Incident Response Forensics: PDRMR3L = Prepare, Detect, Response, Mitigate, Reporting, Recovery, Remediation, Lesson Learned.



IDEAL: Initiating, Diagnosing, Establishing, Acting, Learning.

DHCP: DORA - Discover, Offer, Request, ACK.

The Ring Model: -VM KODU = -1 VM hosts, 0 Kernel, 1 Operating System, 2 Drivers, 3 User.

TCP Header Flags: URG ACK PSH RST SYN FIN = **Unskilled Attackers Pester Real Security Folks**

Digital forensics model: I Prefer Coffee Everytime Anyone Provides Donuts = Identification, Preservation, Collection, Examination, Analysis, Presentation, Decision.

Change Management Steps: RRA/RTID Request, Review, Approve or Reject, Test, Implement, Document.

The 7 steps of a cyber-attack: RSA ESA O = Reconnaissance, Scanning, Access and Escalation, Exfiltration, Sustainment, Assault, Obfuscation.

BCP Steps: BCP policy → BIA → Identify preventive controls → Develop recovery strategies → Develop DRP → DRP training/testing → BCP/DRP maintenance



SW-CMM: I Ran Down My Ostrich = Initial, Repeatable, Defined, Managed, Optimized.

SDLC1: IDIOD - Don't be an **IDIOD** = Initiation, Design, Implement, Operations, Disposal.

SDLC2: "I Reckon All Dem Dere Taters' Really Delicious" = Initiation, Requirements, Architecture, Design, Develop, Testing, Release, Disposal.

ACID: Atomic, Consistency, Isolation, Durability.

