- structure of Common Criteria

- client initially selects vendor based on published EAL - Evaluation Assurance Level.

3 AREAS :

- Part 1 → General concepts for evaluating IT security
- Part 2 → Security functional requirements
- Part 3 → Security assurance requirement for TOE

P.T.O

End — EAL = information that appears on various CC documents are the evaluation assurance levels.

EAL Levels (IMP)

STANDARDS

- CC → System security standard
- PCIDSS → Secure transaction + Financial data
- ISO → Standard for commercial equipment, S/W, protocol, manager

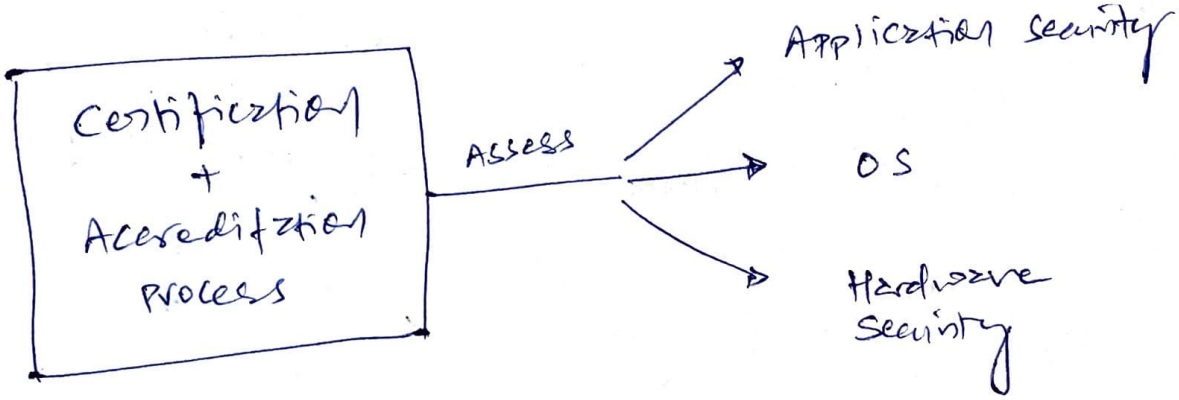
CERTIFICATION & ACCREDITATION

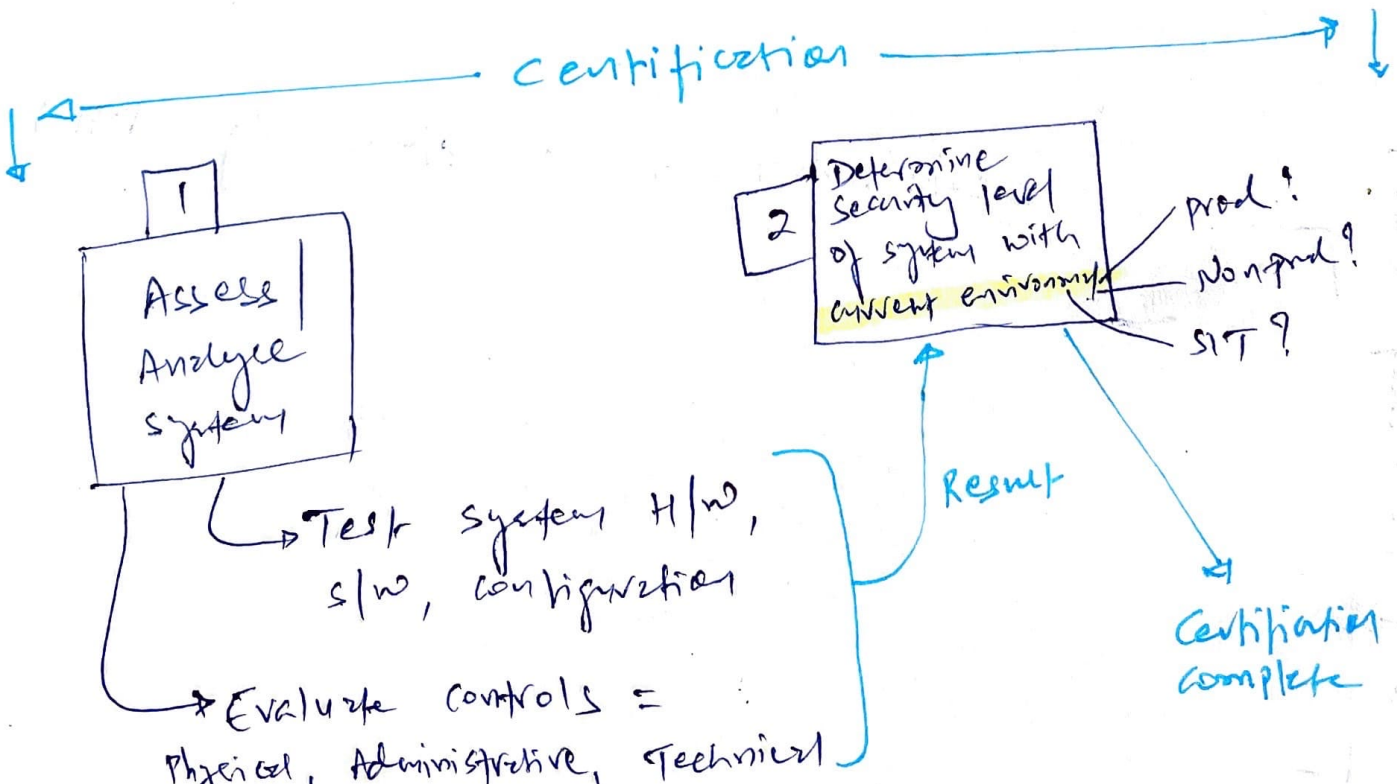
Certification: Nontechnical + Technical evaluation of system that adhers to secure design + security standards (requirements)

Accreditation: Formal acceptence of certified configuration from designated authority.

CISSP Candidate must know

- Know the need for 'C' CERT. & 'A' ACC.
- Know which criteria are required in each phase to evaluate the system.





Certification = Valid

If → Environment
→ configuration
= same

If Environment, config = change

↳ certification = Invalid.

Accreditation

Manage review certification

If meets organization security needs

DAA = Accreditation

- Security policy
- Security requirements
- System capabilities

Certification = Accepted by DAA

Designated Approving Authority.

RMF defines DAA as Authorization official (AO) for Internal accreditation

+ Security control Assessor (SCA) for External Accreditation

Imp for CISSP Exam

PERSPECTIVE

NOTE: Verification process is similar to certification, it goes steps beyond with involving 3rd party testing & service

Also about evaluation of security controls

Certification

For

Internal verification trusted by your → Organization

Accreditation

For

Performed by 3rd party trusted by everyone → WORLD

A sound security policy defines time period for valid certification & when to recertify.

p.t.o End for types of accreditation

2 standards for CERT + ACCR.

RMF (Risk Mgmt Framework)

CNSSP

Committee on National security system (CNSS) policy

Both divided into 4 phases

Phase 1 Definition

Creation of System Security Authorization Agreement (SSAA)

Drives entire CERT + ACCR process

Phase 2 Verification

Refine SSAA

Phase 3 Validation

Further refinement of SSAA + DAA recommendation + development

Phase 4 Post Accreditation

Maintenance of SSAA

UNDERSTAND SECURITY CAPABILITIES OF INFORMATION SYSTEM.

Memory Protection

is used to prevent active process from interfering with area of memory that is not assigned or allocated.

ch:9

- isolation, virtual memory, segmentation, memory mgmt, protection rings

Virtualization

- Allows any OS / multiple OS to work simultaneously on the same hardware

TPM (Trusted platform module)

TPM chip → store & process cryptographic key for hardware encryption

More secure than software-only implementation of hard-drive encryption

HSM - Hardware Security module

└ TPM is example of HSM

TPM Boot - once harddrive is encrypted with userpass & if somebody steals drive & password, they still can't decrypt it. It needs original TPM for decryption.

Fault Tolerance

- Critical element of secure design = redundancy

└ ch:18 (DRP)

Interfaces

(Restricted)

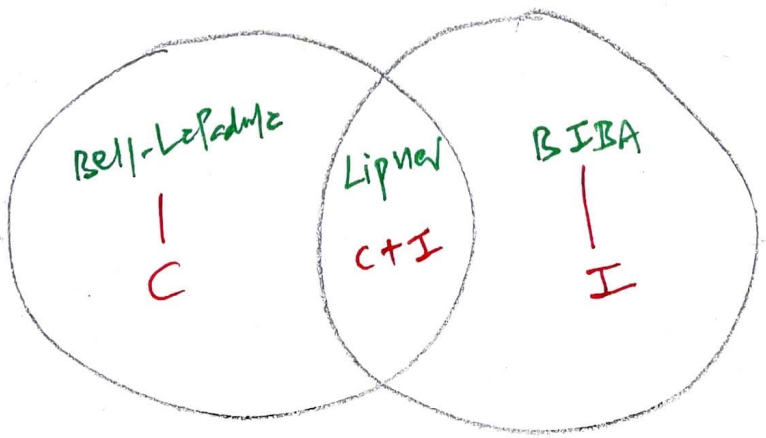
- Constrained interface = to restrict actions of authorised & unauthorised users
- Practical implementation of Clark-Wilson model of security.

Mindmaps Notes

Bell-LaPadula — C	Biba — I
- Protects from low to high No Read ↑ Read ↓ simple security write ↑ No write down ↓ star - For military / Federal	Read ↑ No Read ↓ simple Integrity No write ↑ write ↓ star - For commercial Applications

3 goals of Integrity

1. Prevent Unauthorised subject making ANY changes.
2. Prevent Authorised Subject making BAD changes
3. Maintain System consistency



SECURITY MODEL TREE

Lattice Based
(layers of "C" & "I")

Bell-LaPadula
↳ C

- No read up, no write down

MAC is not system model.

MAC
It's access control model.

- subject & object use label / classification level as privilege
- Each classification represents security domain / level of security

Biba
↳ I

- No read down, No write up

Lipner
↳ Bell & Biba

↳ C + I

Rule Based
(what can be read / write by layers to maintain "C" & "I")

p.t.o End (diagram)

Clark-Wilson
↳ 3 goal of Integrity

3 Rules

① Tripple (object - subject - program)
② Well-formed Transactions
③ Seperation of Duties
↳ based on classification labels

Brewer-Nash
- chinese wall
- prevents conflict of interests
- Data isolation as core principle

Graham-Denning
- secure creation & deletion of objects & subjects

Harrison-Ruzzo-Ullman

Common Criteria Evaluation Process

identifies security requirements for devices (class of devices) — PP (Protection Profile) — Database, FW, OS, Biometric

defines specific product from vendor that will be evaluated — ToE (Target of Evaluation) — FW → Cisco ASA

Vendor documents that claims what's in-built in the product — ST (Security Targets)

Independent lab perform test on

Security Functional Requirements

Security Assurance Requirements

Is the system provide better system security?

Are we sure it is able to provide necessary amount of security.

EVALUATE

Assign EAL — Evaluation Assurance Level

Software / OS / (P.T.O)

Memorize Common Criteria EAL Levels

lowest

EAL 1 — Functionally tested

EAL 2 — Structurally tested

EAL 3 — Methodically tested & checked

EAL 4 — Methodically designed, tested & Reviewed

EAL 5 — Semi Formally designed & tested

EAL 6 — Semi Formally verified, designed & tested

EAL 7 — Formally verified, design & tested

Higher EAL means not more secure, it means it's more stringently tested

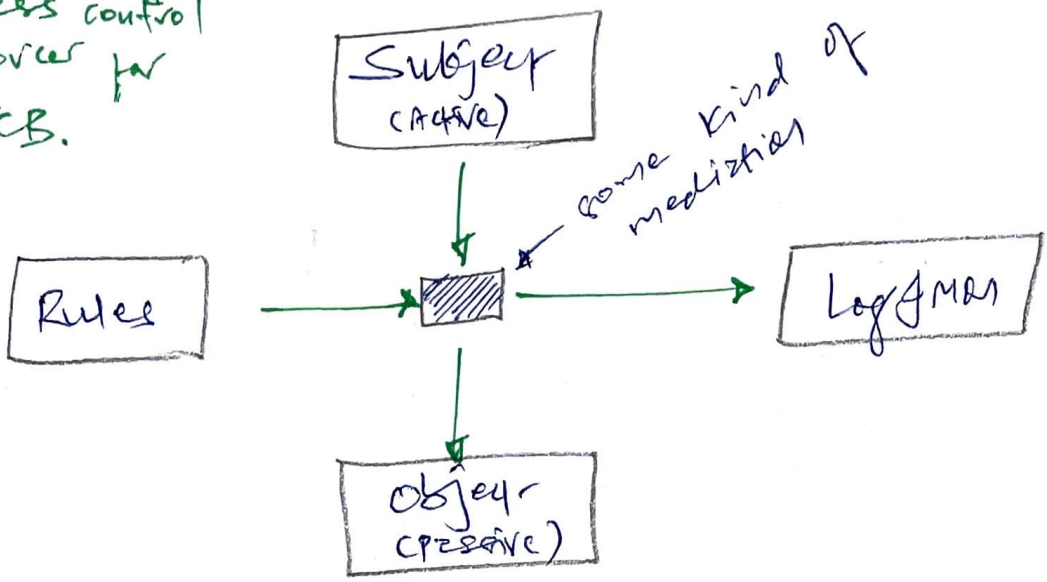
highest

MAC one or more

- Every subject & object gets ^ pre-defined ~~levels~~ lables. Based on the access, System will provide access.
- Eg. Users with "Veg" lable also need another label for "Nonveg" as data is stored in compartments. Need-to-know as being "veg", you can't have access to all Vegie options!!

Reference Monitor Concept (RMC)

Access control enforcer for TCB.



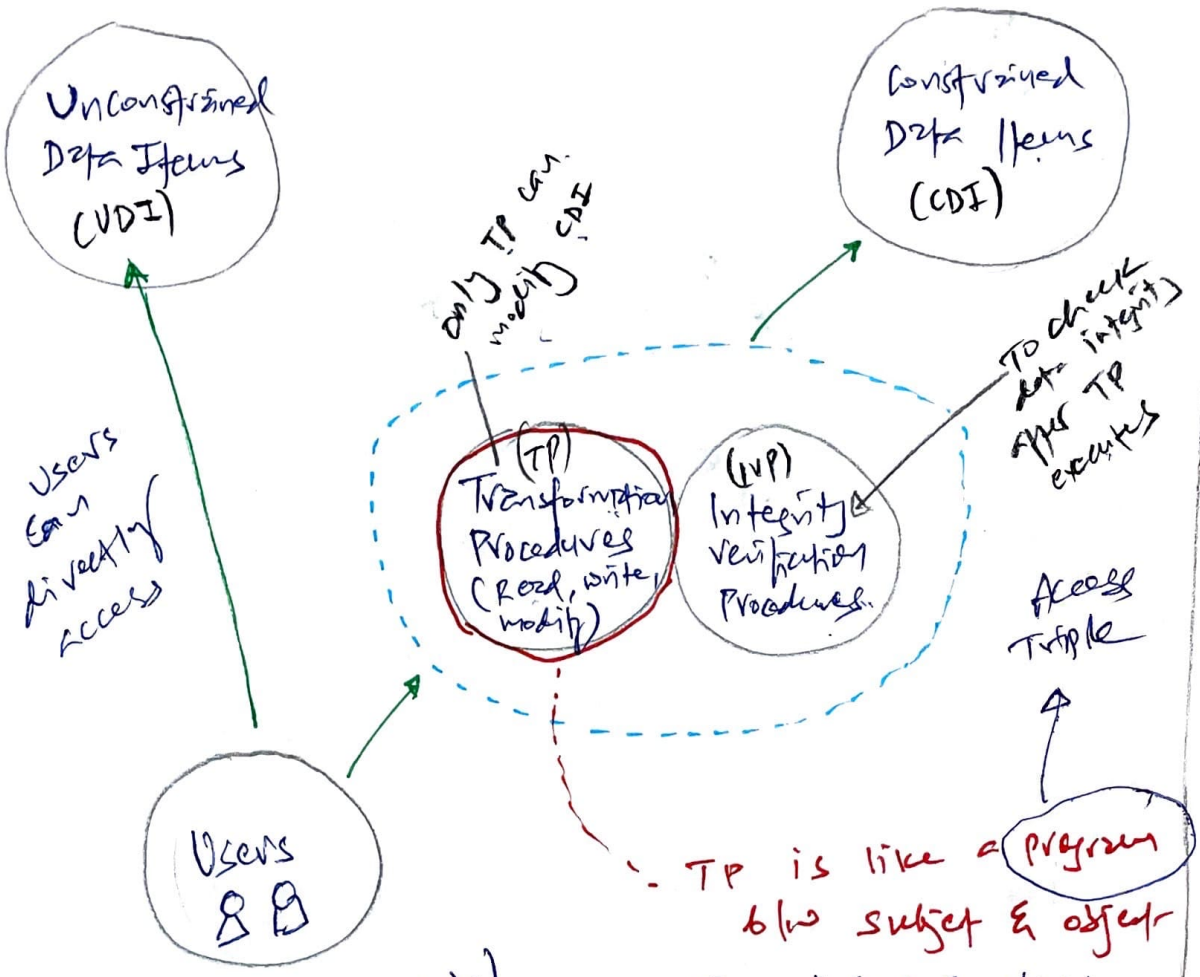
Implementation of RMC = SECURITY KERNEL

we use this to control how ~~of~~ subject will access to objects.

For RMC + security kernel, must satisfy three principles

- completeness: subject should never bypass mediation such as backdoor
- Isolation: Rules are tamperproof, only authorised can change it
- Verifiability: logging mon. to ensure mediation is working properly.

clark - wilson model



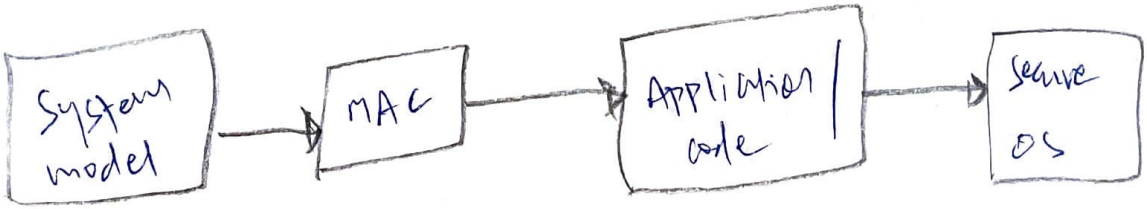
Biba Model (integrity)

write
Strong Integrity → A subject can't write to files of higher integrity level.

Read
Simple Integrity → A subject can't read files from lower integrity level.

Invocation Property → A subject can't invocate data, files or service from higher integrity

Bigger picture



3 Types of Accredition

System accredition

- System / application evaluation

site accredition

- App / system specific, self-contained location

type accredition

- App / system that is distributed to number of different locations to be evaluated.

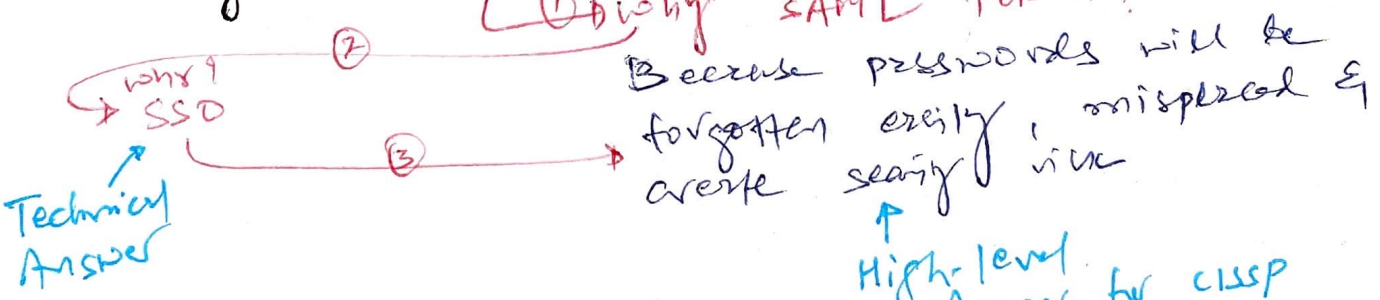
CISSP MINDSET: THINK LIKE A MANAGER

↳ Which process / systems / solution is best / fastest / most secure?

↳ Don't fix the issue. Know the process.
  ↳ Don't pick the technical answers.

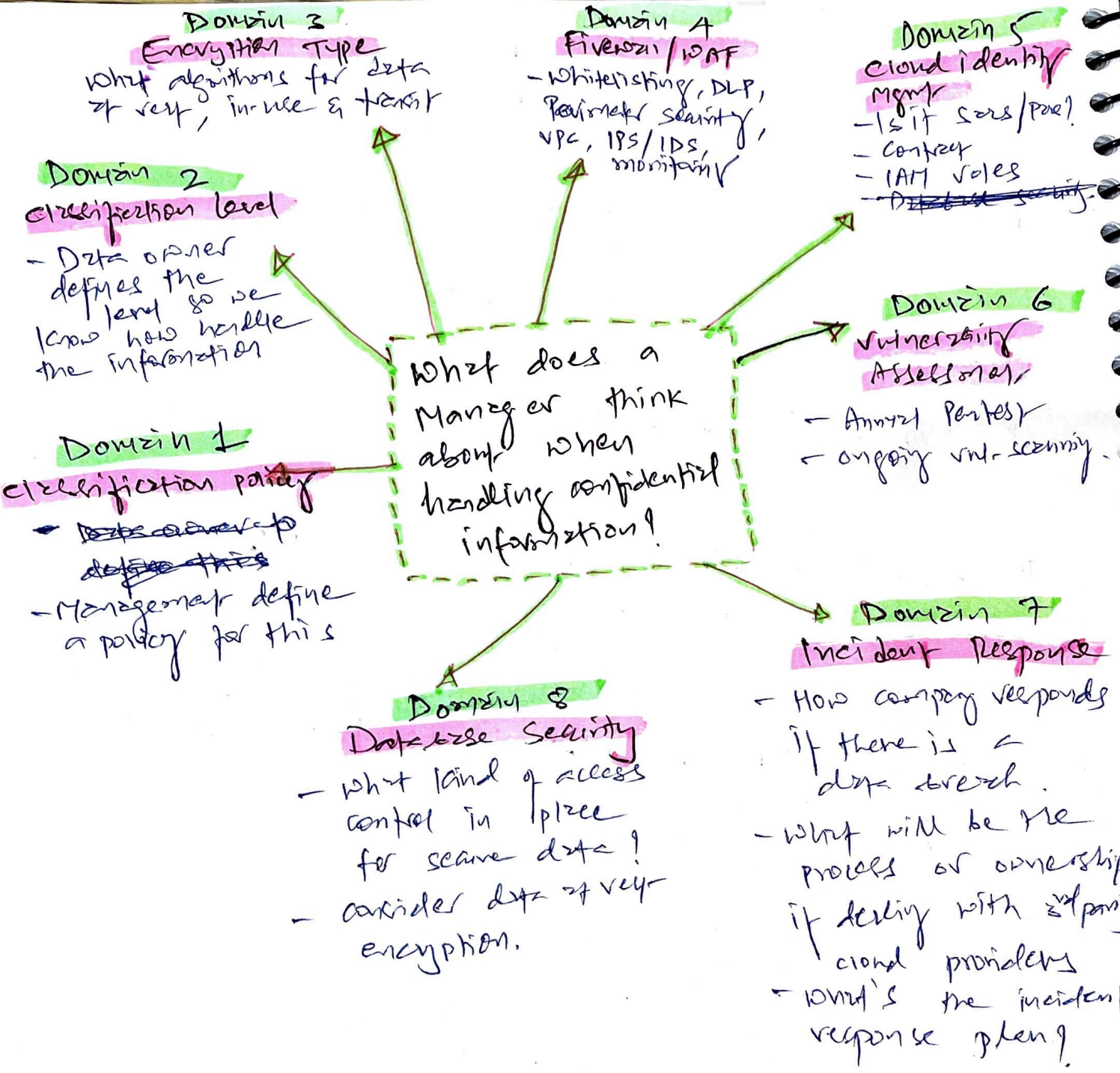
↳ Save Money. Save Human life.
  ↑ But first,

↳ Ask WHY multiple times to reach to high-level answer.



↳ Every Domains are connected with each other. Everything connects with everything in CISSP.
  ↳ All 8 domains: see it as one Fluid Entity.

P.T.O
To understand the CISSP universe.



CISSP EXAM IS NOT BASED ON WHAT YOU DO IN THE REAL WORLD.

INSTEAD, IT IS BASED ON 2 PREMISES:

1. THINK LIKE A MANAGER →
2. APPLY BEST PRACTISE →

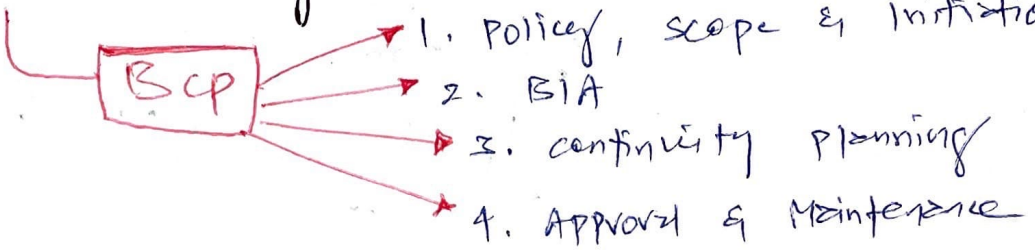
→ MITIGATE RISK

What to memorize? PRIMARY CONCEPTS IN ORDER
- Don't understand it.

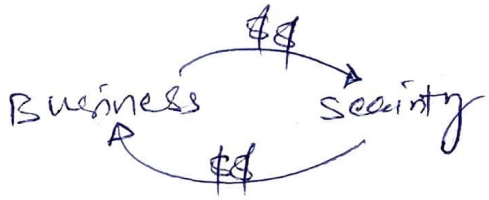
(1) Human safety is the top priority. Business later.

(2) Behave ethically (laws vs. boss) —— $(ISC)^2$ code of Ethics

(3) Business continuity — Business should never fail



(4) Maximize corporate benefit.



(5) Avoid or minimize threats.
Learn why, when & how to accept, reject, transfer, mitigate or avoid risk.
(Risk never disappears. It can be only reduced.)

(6) All controls must be cost justified (Safeguard)
Don't spend $100k on controls to protect $10K Asset.

(7) Security mgmt must drive security program. (top-bottom approach)

→ for CISSP Exam, pretend to be consultant for 3 wks. Advise. Don't touch anything.

(8) Security professionals has no decision making authority.

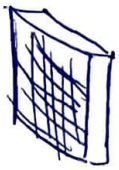
(9) Use automated tools where appropriate

MONEY

~~Funds~~ → Understand the difference b/w cost & value

What does it mean to be GDPR ready?

With GDPR context



Firewall cost = $5K

Firewall that protect sensitive data, value = $100K

Cost of GDPR compliance = $10K for $100K loss in revenue if not GDPR as no client wants to do business. And it cost $1M if there is a breach without GDPR.

CISSP CORE CONCEPT

if there is no process, there is no solution. (DR/BCP)

(Input to BIA) what's the role's responsibility for this process?

(Mgmt) which roles are assigned to this process?

KNOW THESE PROCESSES

- PKI
- Incident Mgmt
- eDiscovery
- change control
- Forensic Investigation
- *BCP/DR
- Info. security Program
- RMF
- *SDLC
- Info. Lifecycle

How much technical knowledge I need for CISSP?

Do I Need to be technical? (Domain 4). N/o security.

- IPSec
- SAML
- OAuth
- SSO
- SPML
- WEP / WPA2
- Switching (broadcast + collision domain).
- TCP (3-way handshake).
- Federated Identity
- 802.1X (layer 2 technology).
- Kerberos
- OSI Model (Heart of Everything)