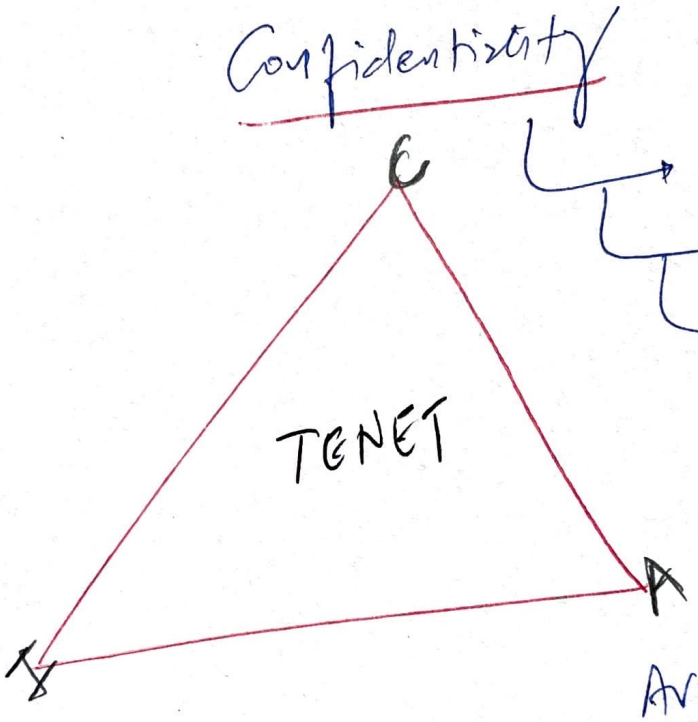
DOMAIN 1

1. Security Governance + Principles + Policies

Confidentiality ⟷ Integrity

Availability $\propto$ Integrity + Confidentiality.



Confidentiality
- At Rest
- Transit
- In use

Integrity
- Non-repudiation
  - Accountability
- 3 Perspectives

Availability
- DDoS
- BCP
- Log monitoring

Government

1 Confidentiality

2+3 Availability + Integrity

Private

1 Availability

2+3 Confidentiality + Integrity

Security

+

CIA

- Confidentiality
- Integrity
- Availability

AAA

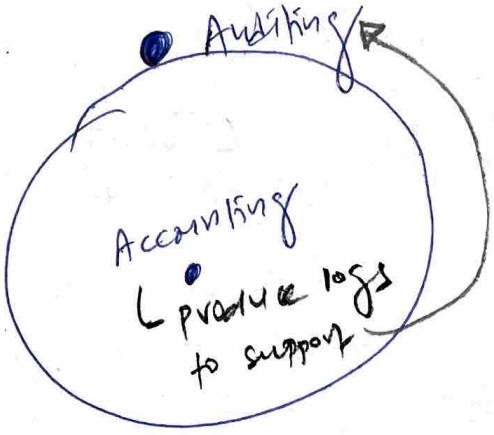
- Identification + Authentication
- Authorization
- Auditing
- Accounting

Non-Repudiation

Accounting vs Auditing

Logs

Trails
↳ logs + user activity



vs Monitoring

watching logs (not recording to file)

Also P to scratch at the end

Possible to monitor without Auditing. But, we can't audit without monitoring.

Something
- You Do
- You Have
- You Know
- You Are

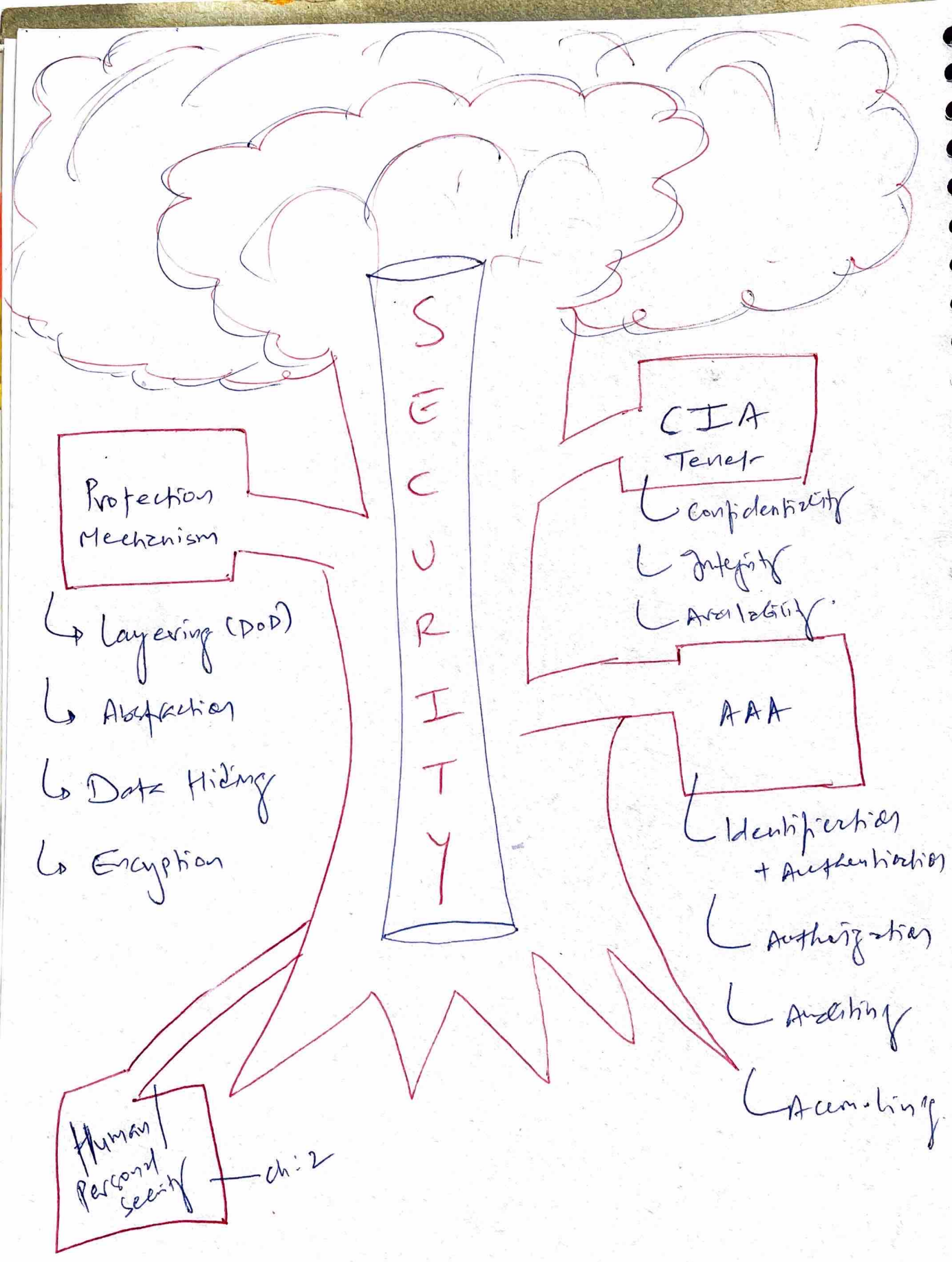
Access Control
↳ Subject + object

Security Control = counter measures
↳ RBAC

CRITICAL

② Accounting :- Review log files to check compliance & violations in order to hold subjects accountable for their actions.

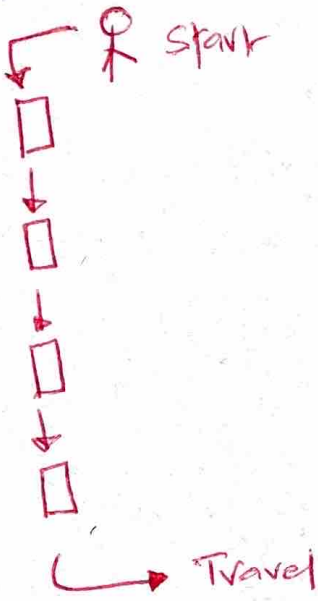
① Auditing :- Recording log of events and activities related to subjects & objects.


SECURITY
Protection Mechanism
Layering (DoD)
Abstraction
Data Hiding
Encryption
CIA Tenet
Confidentiality
Integrity
Availability
AAA
Identification + Authentication
Authorization
Auditing
Accounting
Human / personnel security
ch: 2

Layering – (Defense of Depth)

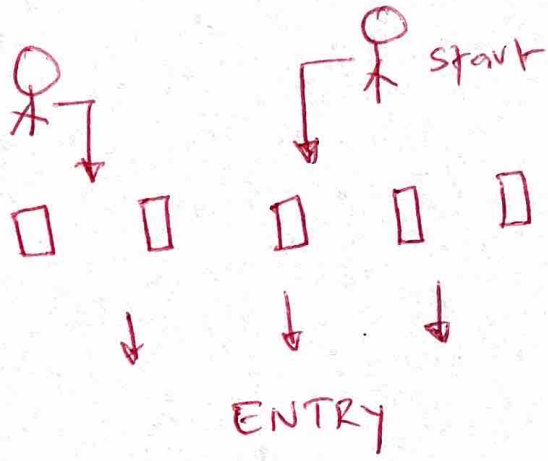
Serial config.

- Immigration

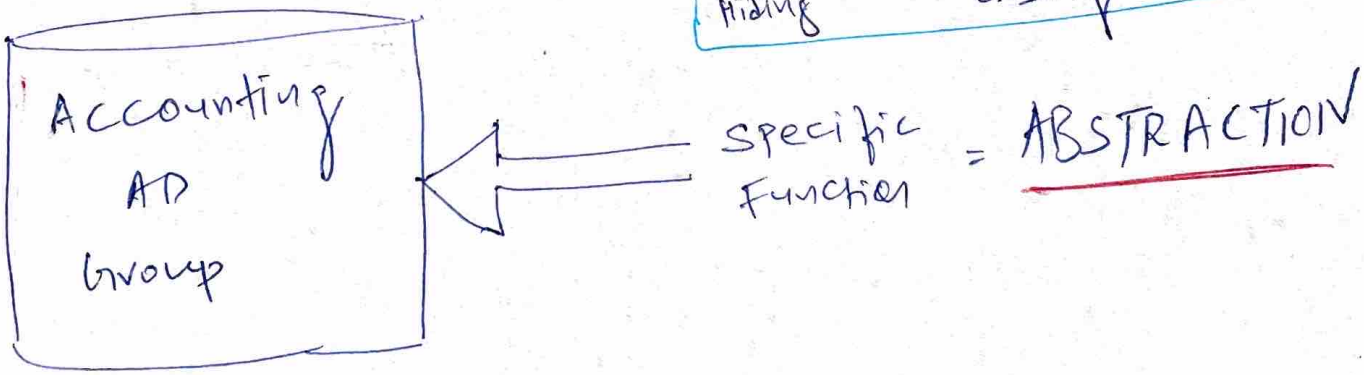


Parallel config.

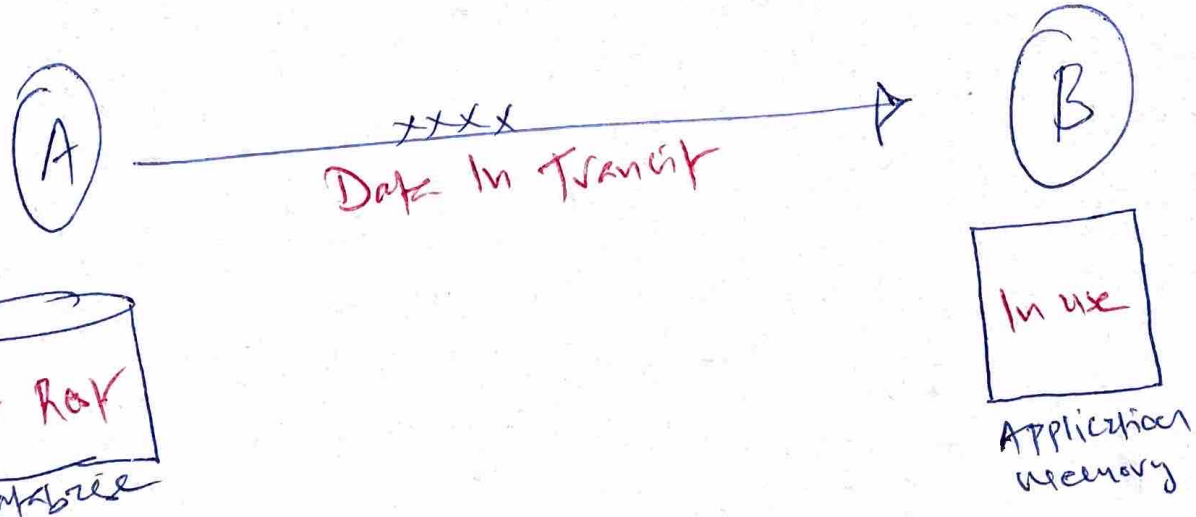
- Shopping mall



Data Hiding = security through obscurity



Think Encryption



Governance = Vision | Broader Risk

↓

Management = Specific Risk | Planning & Implementation

└ Senior mgt ← Security Policy

└ Middle mgt [CISO] → Policy, Standards & Guidelines + Procedures

↓

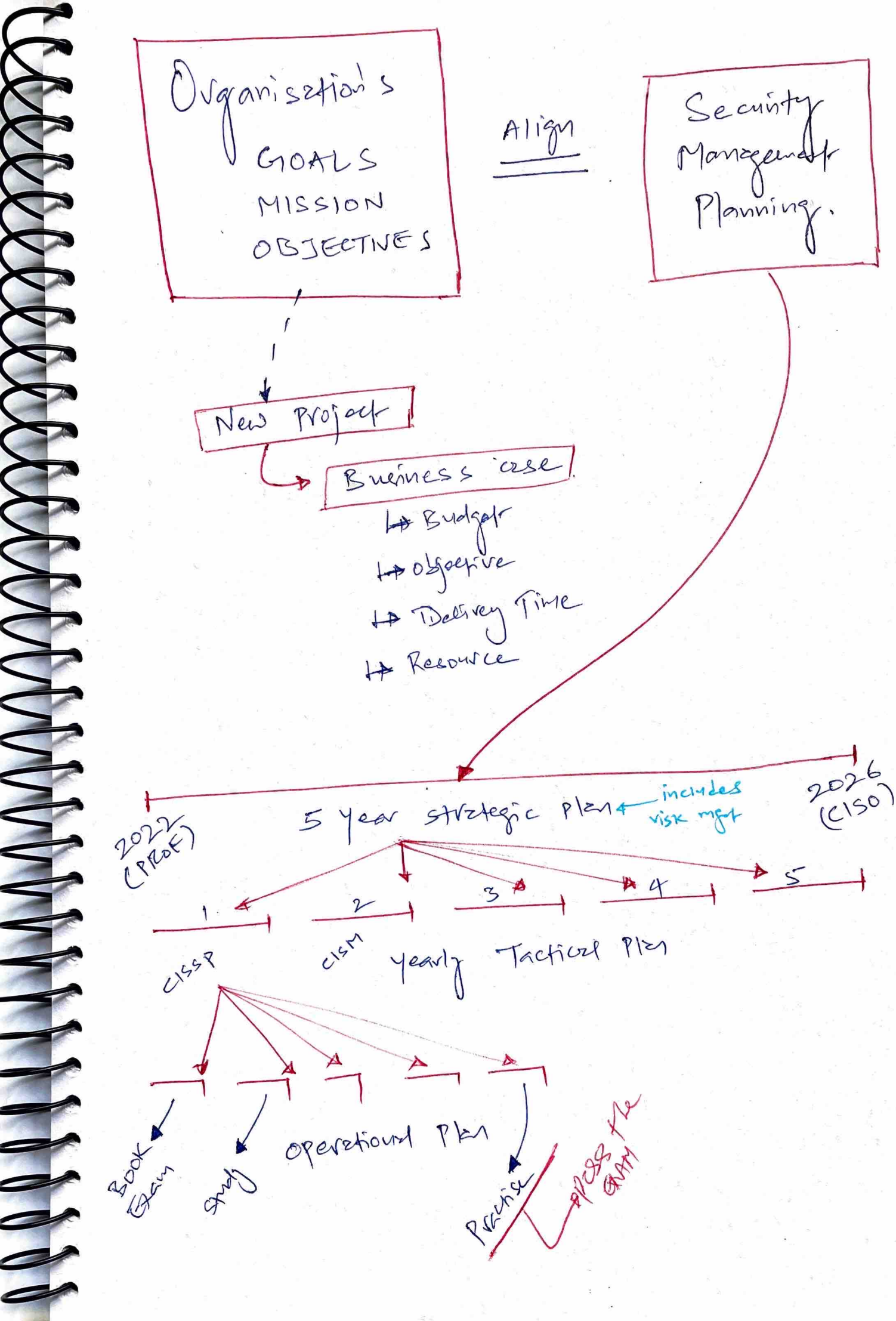
(Operational Managers) Security Professionals ← Assess + implement security controls

↓

End users ← Comply to security policy + controls

10,000 FT. VIEW

[TOP-DOWN APPROACH]


Organisation's
GOALS
MISSION
OBJECTIVES
Align
Security Management Planning.
New Project
Business case
Budget
objective
Delivery Time
Resource
2022 (PROF)
5 year strategic plan
includes risk mgt
2026 (CISO)
1
2
3
4
5
CISSP
CISM
yearly Tactical Plan
Book
Exam
study
operational Plan
Revise
Pass the exam

Company → Acquire, Merge, Divestitures = RISK

PROCESSES To mitigate

Change control mgmt ... CAB

Data classification

... CIA

↳ To ensure Security is not compromised

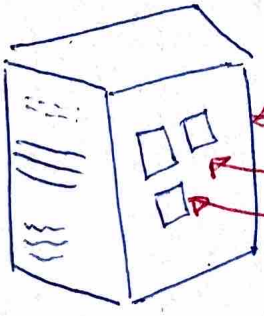
↳ To document for auditing

Restricted Data ← Give importance

Public Data ← Trick it easy

Declassification

- Equally important



classify physical Asset that holds data — System owner

classify data = Data owner's job

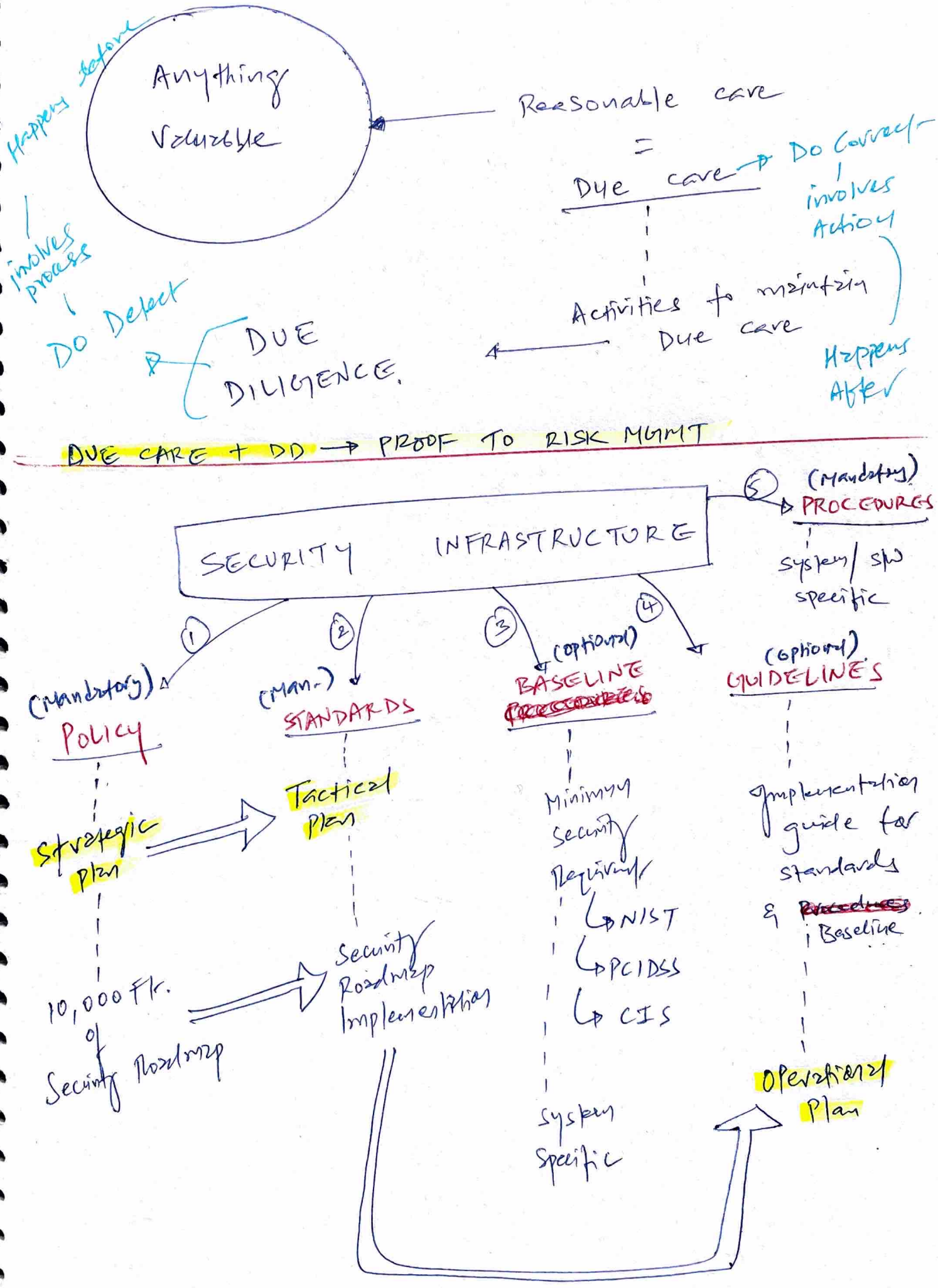
US CAN'T STOP TERRORISM

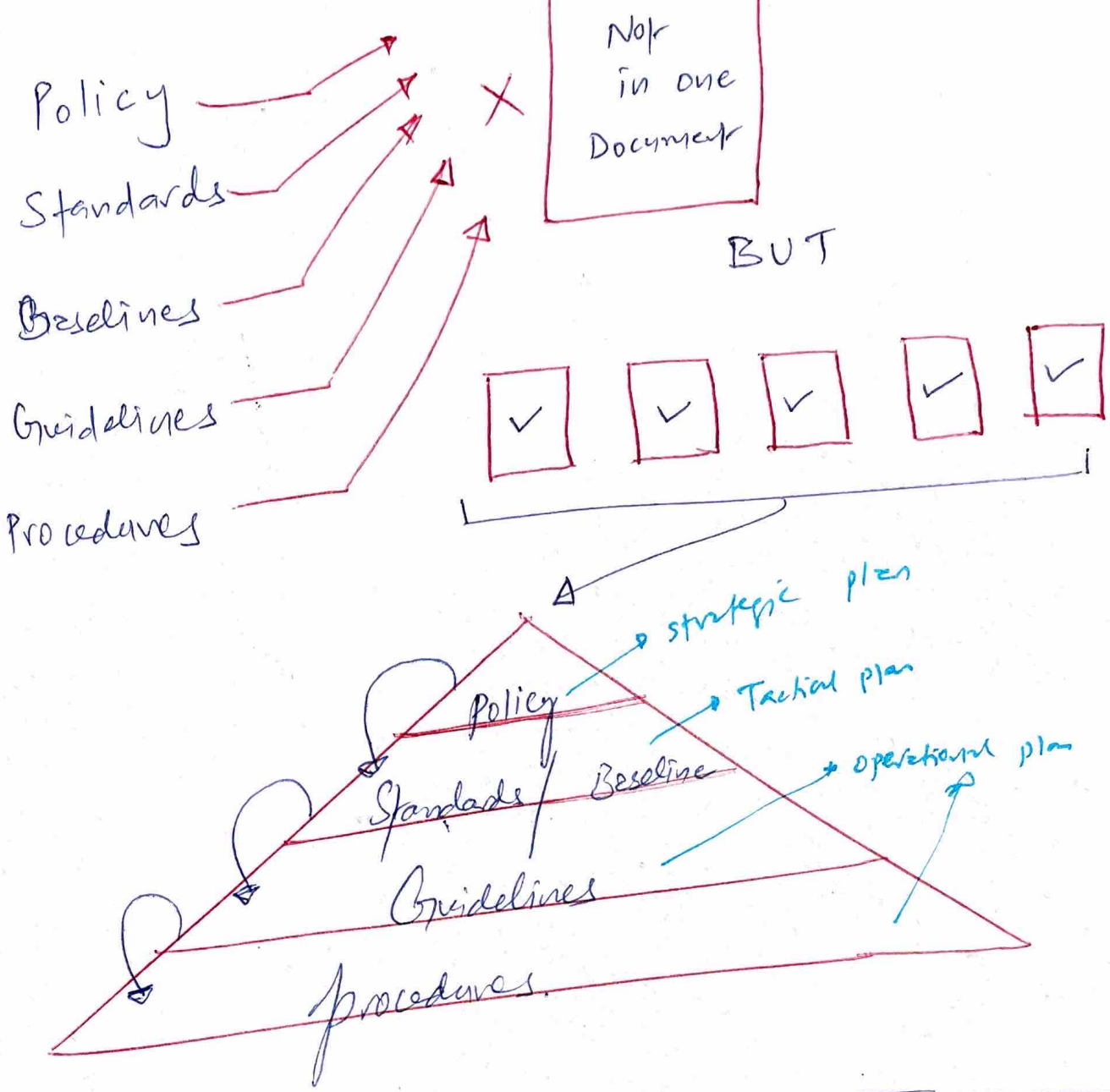
US: Unclassified, Sensitive

CAN'T: Confidential

STOP: Secret

TERRORISM: Top Secret


Anything Valuable
Happens before
involves process
Do Detect
DUE DILIGENCE.
Reasonable care
=
Due care → Do Correct
involves Action
Activities to maintain Due care
Happens After
DUE CARE + DD → PROOF TO RISK MGMT
SECURITY INFRASTRUCTURE
(Mandatory) PROCEDURES
system/sw specific
1
2
3
4
(Mandatory) POLICY
(Man.) STANDARDS
(optional) BASELINE
(optional) GUIDELINES
Strategic plan
10,000 ft. of Security Roadmap
Tactical Plan
Security Roadmap Implementation
Minimum Security Requirements
NIST
PCIDSS
CIS
system Specific
Implementation guide for standards & Baseline
Operational Plan



IDENTIFY → CATEGORIZE → ANALYZE → MITIGATE → RESPOND

Threat Modeling ⇒ Reduce Risk

→ 2 Approaches

Proactive / Defensive → SAST

Reactive / Adversarial → DAST

START (Non-Prod) → SYSTEM DESIGN → FINISH (Prod)

PenTest

Fuzz Test

APPROCHES

Threat Modeling

1. Proactive / Defensive
2. Reactive / Adversarial

(IDENTIFY) Identifying Threats

1. Focus on Assets — Valuations — Implement Access controls
2. Focus on Applications / softwares
3. Focus on Attackers Goals

Understand ETHICAL HACKING

Consider OWAPS TOP 10 — OAP

(CATEGORIZE)

SOFTWARE FOCUSED ← Microsoft's

STRIDE threat model methodology

- S – Spoofing — why not add "Social Engineering"
- T – Tampering
- R – Repudiation
- I – Information Disclosure
- D – DDoS
- E – Elevation of Privileges

(CATEGORIZE)

Threat Model Methodologies

- **STRIDE** — To assess threats against
  - OS
  - Applications
- **PASTA** — For Asset Protection
- **DREAD** — For Response P.T.O
  - based on 5 questions:
    - Damage
    - Reproducibility
    - exploitability
    - Affected Users
    - Discoverability
- **TRIKE** — Open source.
  - Accepted Risk level for each class of Asset
- **VAST** — For Agile Project Mgmt.

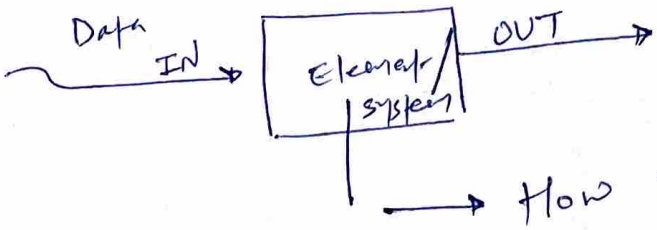
(ANALYZE) = Data Flow Diagram

Define

- Protocol
- Technology
- Application
- OS
- Environment

Think each with STRIDE Perspective

Threat Reduction (MITIGATE) = Decompose or Dissection



THINK!

→ How Data is entered
→ What happens to Data inside the element
→ How Data is stored?
→ How Data is secured inside the element?
→ How Data is coming out?

threat reduction / decomposition process

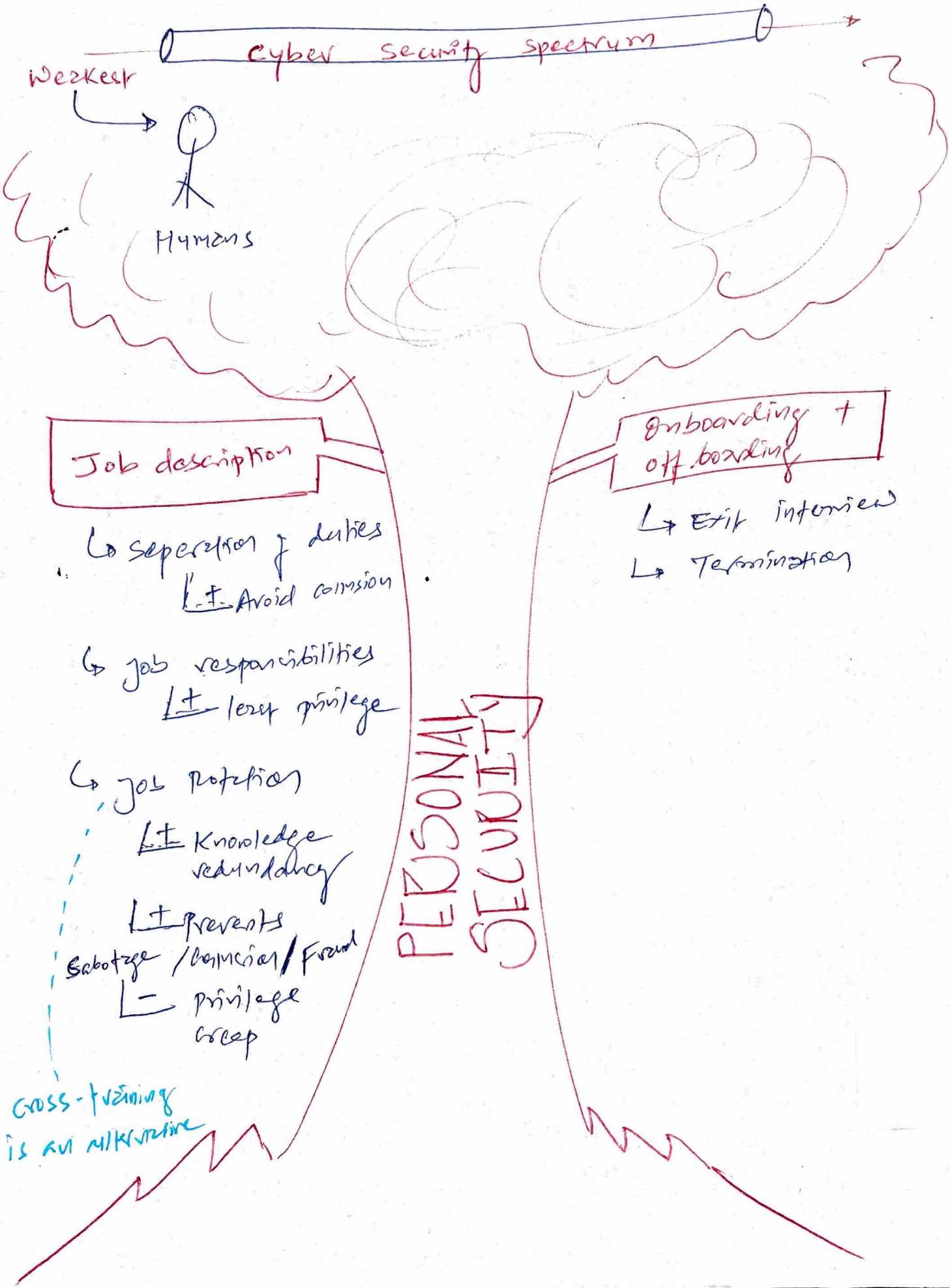
REDUCTION ANALYSIS

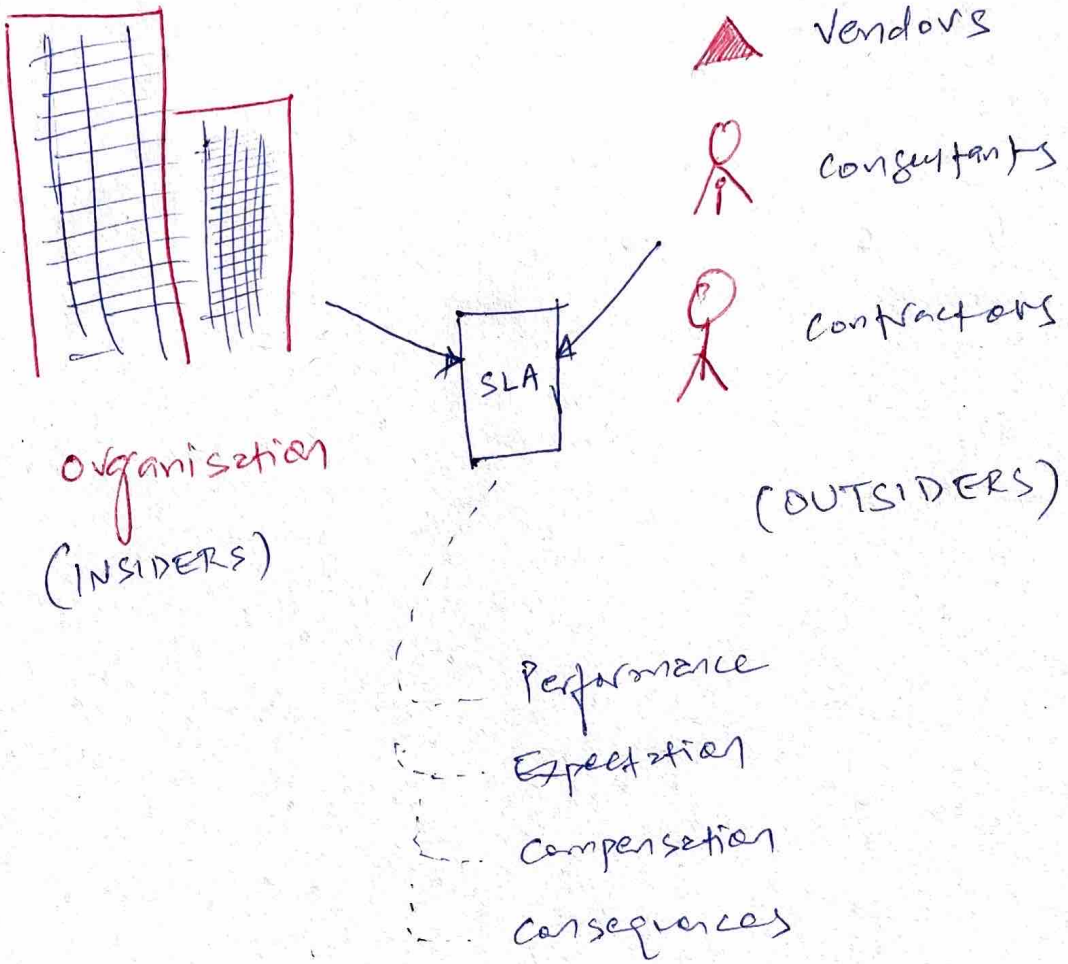
1. Trust Boundaries = VPCSC
2. Data Flow Path - movement & data flow locations
3. Input Points - location where external input is received
4. Privileged Operations = SA / Admin A/Cs. → cyberARC (PAM)
5. Security stance & Approval = Align with sec. policy.

(RESPOND) — D R E A D

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability.

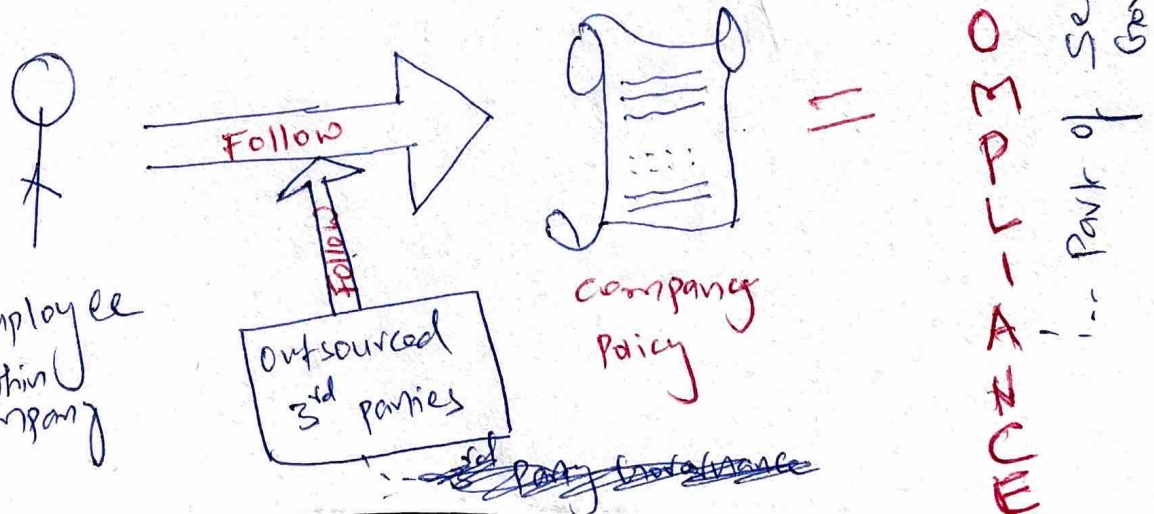
2. Personal Security + Risk Mgt.

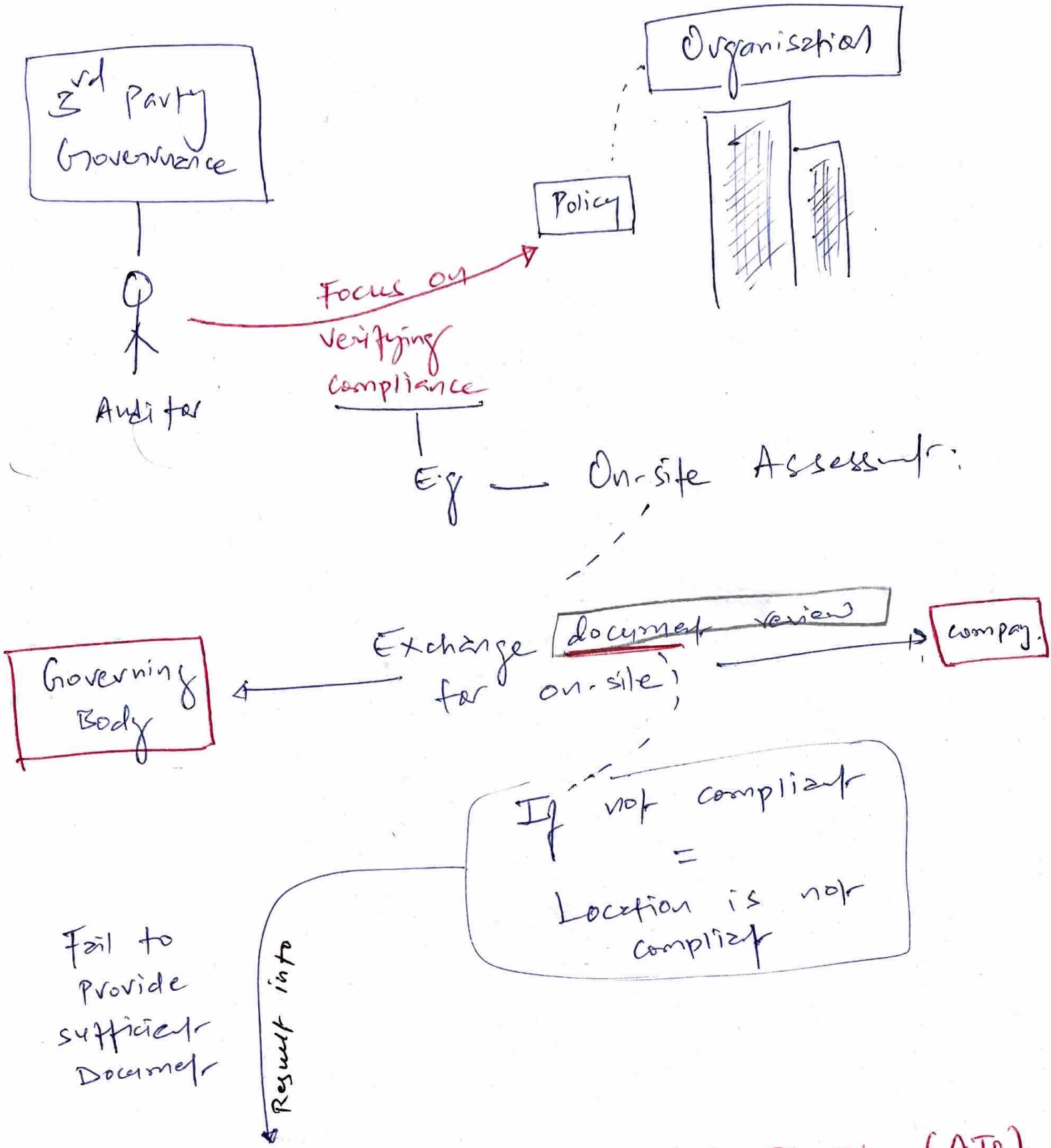




Name
Address
Mobile
Passport

PII Data ⟹ Need PRIVACY POLICY

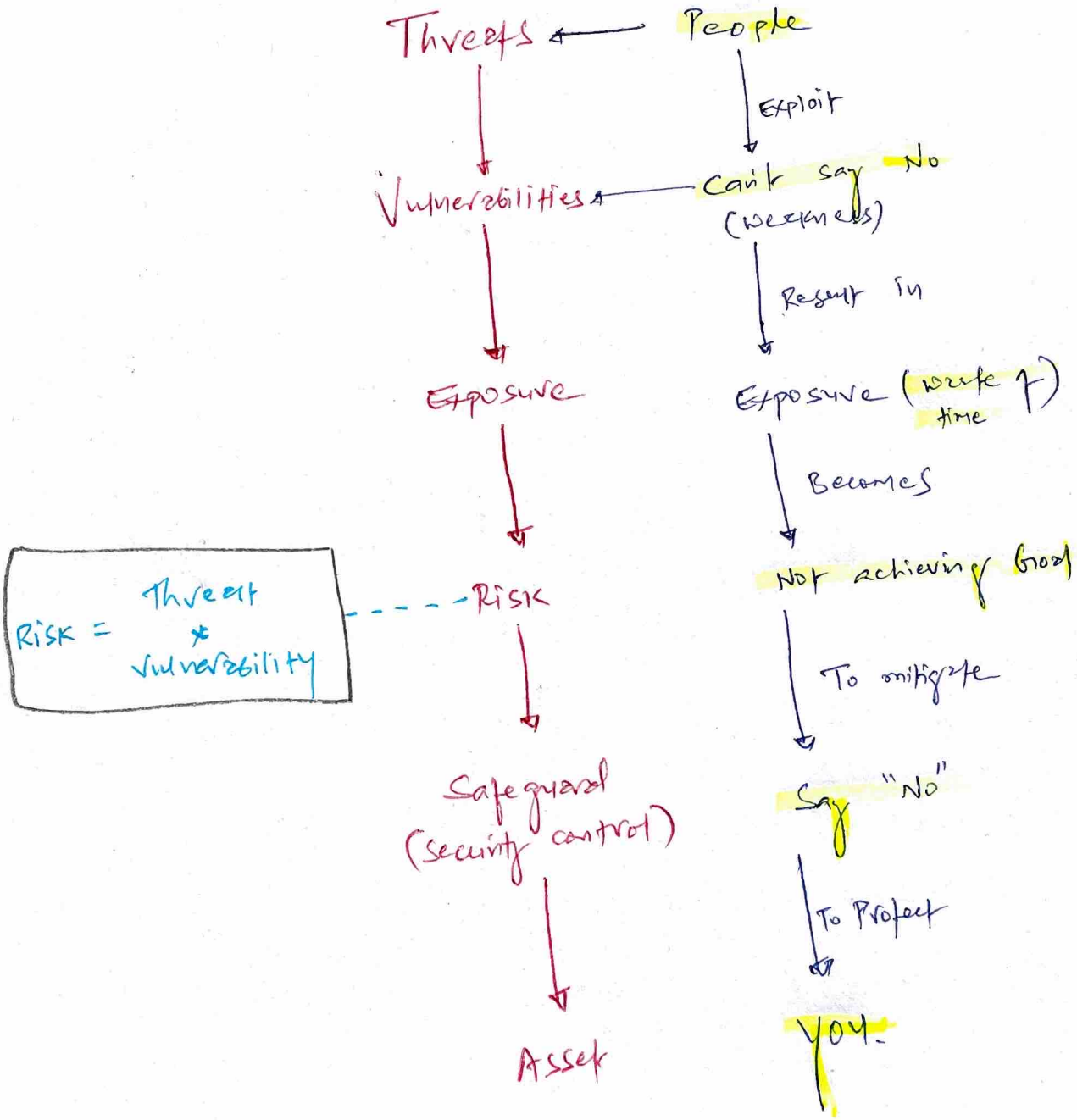




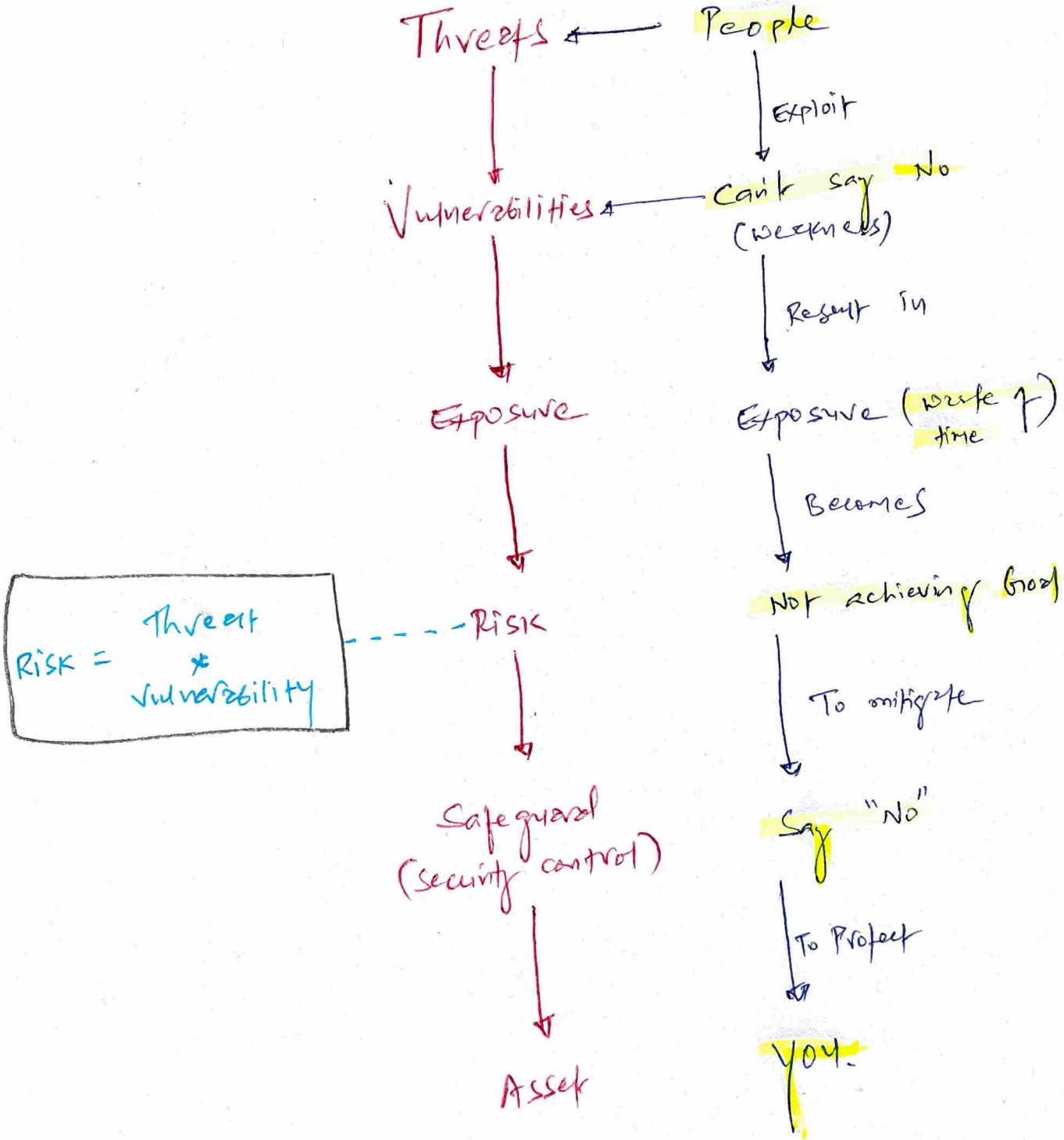
Loss of Authorization to Operate (ATO)

- once ATO is lost or revoked, a complete documentation review & on-site review showing full compliance is necessary to reestablish the ATO.

RISK MANAGEMENT
CONCEPTS



RISK MANAGEMENT
CONCEPTS



Risk Management

Primary goal: To reduce the risk to acceptable level.

1. Identify
   - Threats
   - Vulnerabilities
2. Analysis / Assessment
   - Quantative (P.T.O END: 6 STEPS OF RISK ANALYSIS) (P.T.O End (more notes))
     - EF
     - AV
     - SLE
     - ARO
     - ALE
     - ACS
   - Qualitative
     - Delphi technique
   - ALE = SLE * ARO
     - SLE = AV * EF
   - Safeguard Evaluation
     - (Pre-ALE) - (Post-ALE) - ACS
3. Response — $200 SPEED FINE
   - Mitigate / Implement security controls. (max speed 60.)
   - Assignment / Transfer to friend.
   - Accept (A.K.A Risk Appetite) (Risk tolerance) — Pay fine — when cost/benefit analysis has negative value
   - Deterrence — (60) — speed sign
   - Avoidance / Find alternate route
   - Risk Rejection (P.T.O)

ignoring risk that exists ——— driving Around / Smoky

Risk Rejection

Residual Risk ← This is Mgmt chose to accept the risk rather than to mitigate.

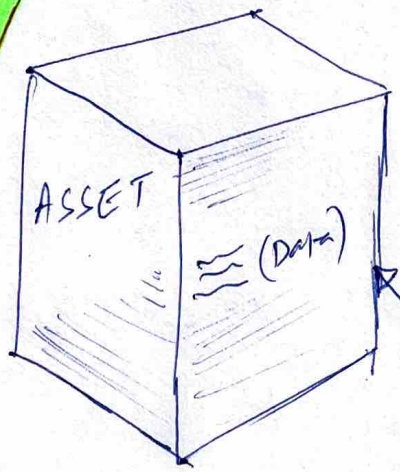
Total Risk

Threat * Vulnerabilities * Asset Value

Total Risk – Controls Gap

Countermeasure / Security control ---- Recipe to Risk Mitigation.

4.



3. Physical.

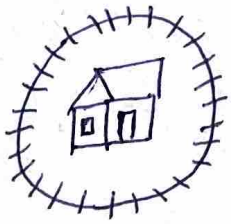
2. Technical / Logical

1. Administrative

SECURITY CONTROL MAIN CATEGORIES.

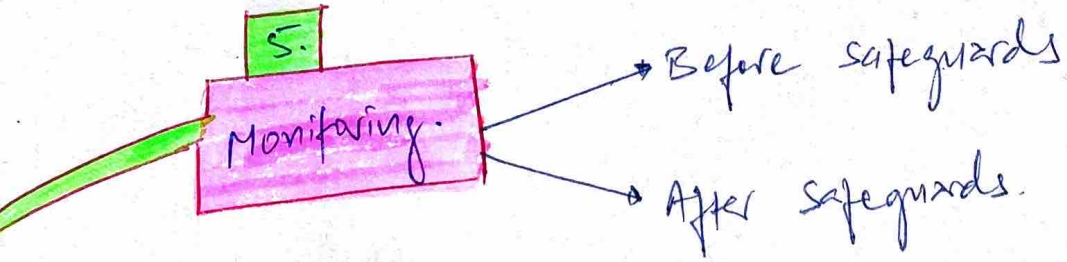
other controls. P.T.O.

Applicable Types of controls.



1. Deterrent → Physical
2. Preventive → physical + technical.
   - Firewall
   - Pen Test
   - Fencing
   - IPS
   - Data classification
   - Least privilege
   - Sec. Awareness training.
3. Detective → 

4. Compensating → defense of depth
5. Corrective
   - virus → Quarantine → Fixed.
6. Recovery
   - RAID
   - Backup & Restore
   - BCP
     - Backup & Restore
     - Hot / warm / cold sites
7. Directive
   - Force subject to comply → EXIT SIGN.
   - SIEM – monitoring



RMF - RISK MANAGEMENT FRAMEWORK

NIST 800-37

7 STEPS. with 2 PERSPECTIVE

NIST 800-53

Information System

1. Prepare
2. Categorize
6. Authorize

Security CONTROL

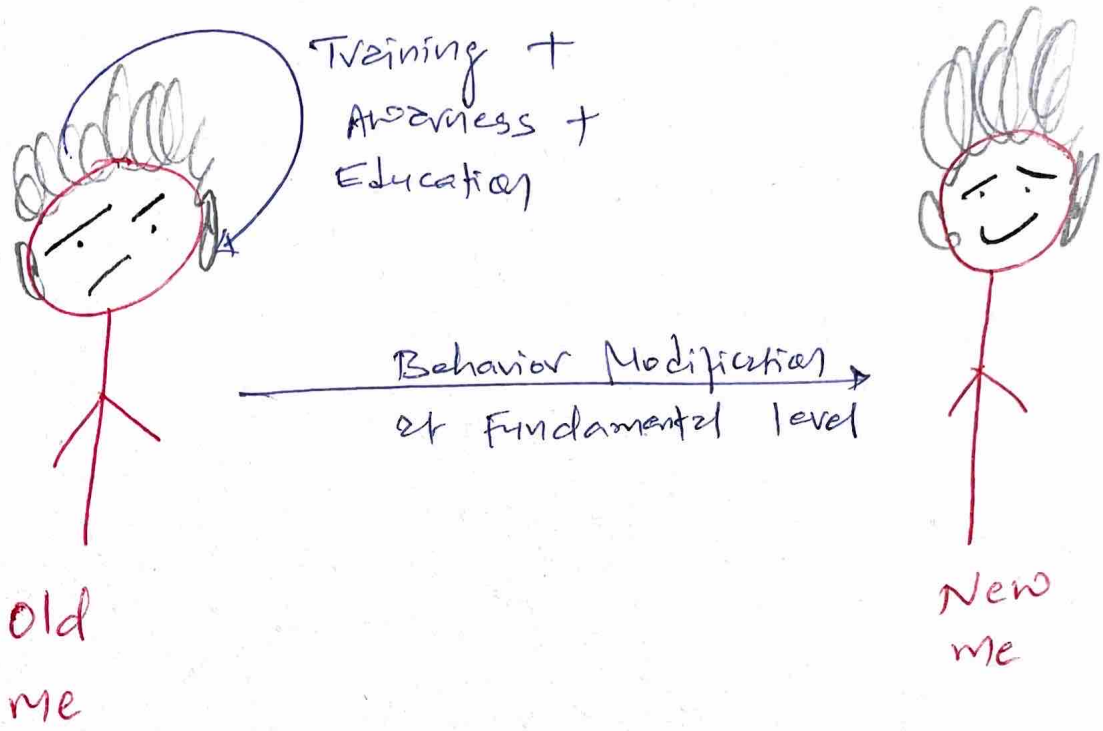
3. Select
4. Implement
5. Assess
7. Monitor

People can See I Am Always Monitoring

CISSP = NIST 800-37 RMF

Other RMFs

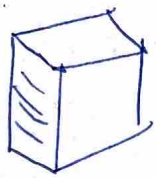
- OCTAVE
- TARA
- FAIR



Perform Risk Assessment

SECURITY FUNCTION → SHOULD BE

COST-EFFECTIVE



AV = $10K

Safeguard = $5K

Profit = $5K

MEASURABLE

Pre-safeguard 50% RISK

Post-safeguard 20% RISK.

QUANTATIVE
* RISK ANALYSIS STEPS :

① Inventory Assets — find AV (Asset value)
$200K

② Identify Threats — calculate EF & SLE
50%

$$SLE = AV * EF$$
$$= 200 \times 50\%$$
$$= 100K$$

③ Perform Threat Analysis — calculate the likelihood of vertical threat (ARO) = 10% (0.10)

$10 \overline{)1} \quad .1$
10
10 — 1 in every 10 year

④ Estimate the potential loss — $ALE = SLE * ARO$
100 * 0.10
$= \$10K$

⑤ Research countermeasures for each threat.
— security controls to reduce risk

ALE1 − ALE2 − ACS (Annual maintenance cost) = True value safeguard

⑥ Perform cost/benefit Analysis
— For each countermeasures for each threat for each asset.

Total Safeguard value should not exceed more than $10K.

Risk = threat * Vulnerability

↳ This is absolute

Exposure = is a possibility

↳ low exposure can result to high risk

↳ high exposure can result to low risk

Safeguards

- Not only purchasing new products
- Reconfigure existing elements
- Removing elements from Infra.

Attack Vs Breach

Intentional attempt to exploit vulnerability

when security mechanism is bypassed ↳ Backdoor

if bullet still hit with body armour, you still die

=

if safeguard fails, the loss of Asset is same as there is no safeguard.