3. Business Continuity Planning

BCM
BCP
DR

SHOW MUST GO ON FOR COMPANY

BCP: Focus on Business operation
- Takes care of overall Energy
- Strategic (long term)
  - 10,000 ft
  - high-level
  - Business mgmt related

DR: Focus on IT Activities ----- ch: 18
- Tactical (short term)
  - Micro-level.
  - IT related
  - Takes care Immediate emergency

BCP PROCESS 4 STEPS

1. Project Scope & Planning
   - Business organization Analysis
   - BCP Team selection
   - Resource Requirements
     - BCP development
     - BCP Testing, training & maintenance
     - BCP Implementation
   - Legal & Regulatory Requirements

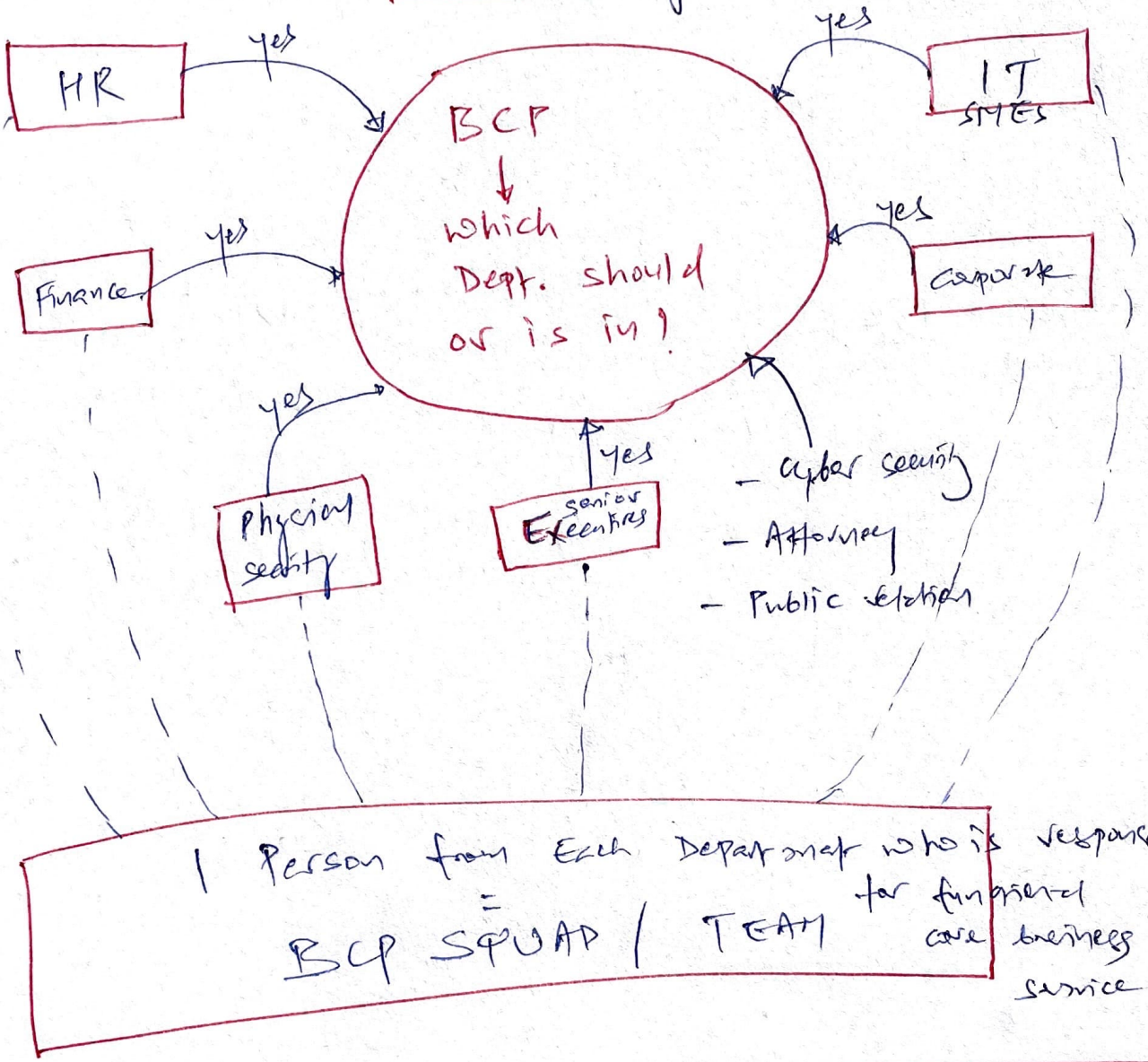
2. Business Impact Assessment (BIA)
   - Analysis
     - A - Qualitative Decision making
     - B - Qualitative Decision making.
   - (1) Identify Priorities
   - (2) Risk Identification
   - (3) Likehood Assessment
   - (4) Impact Assessment
   - (5) Resource prioritization

3. Continuity Planning

4. Approval & Implementation

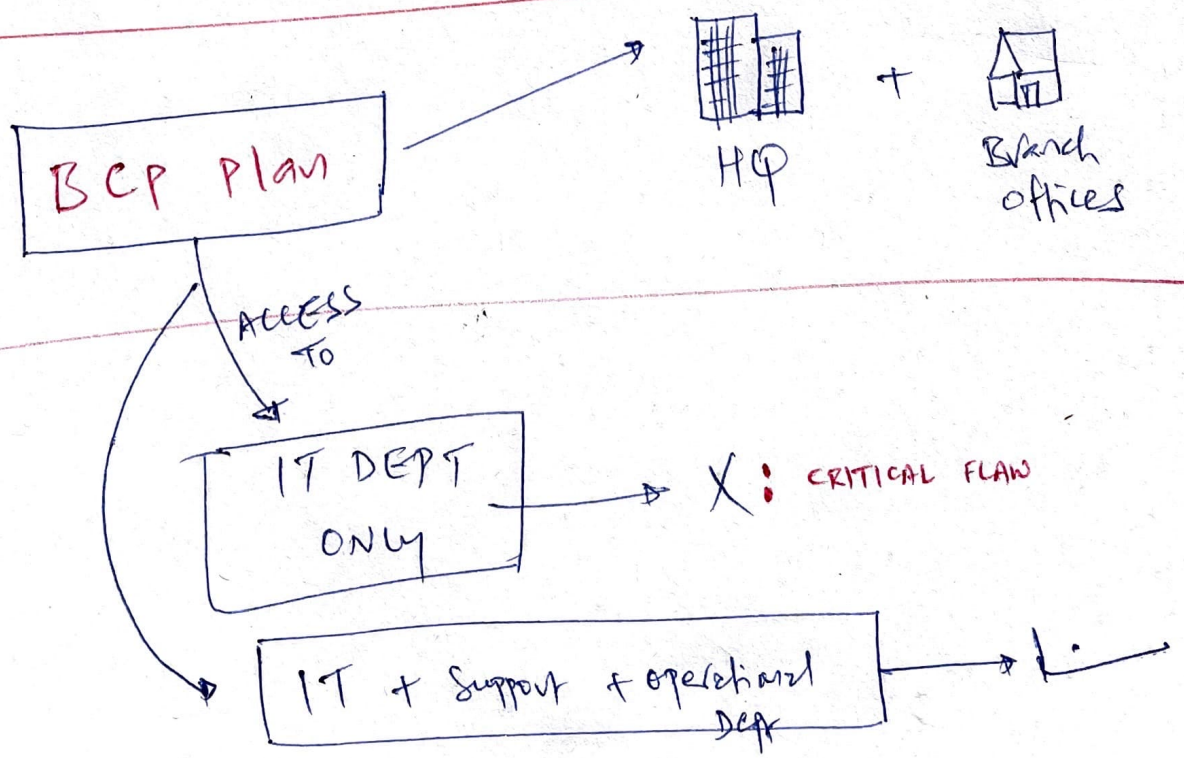
PTO

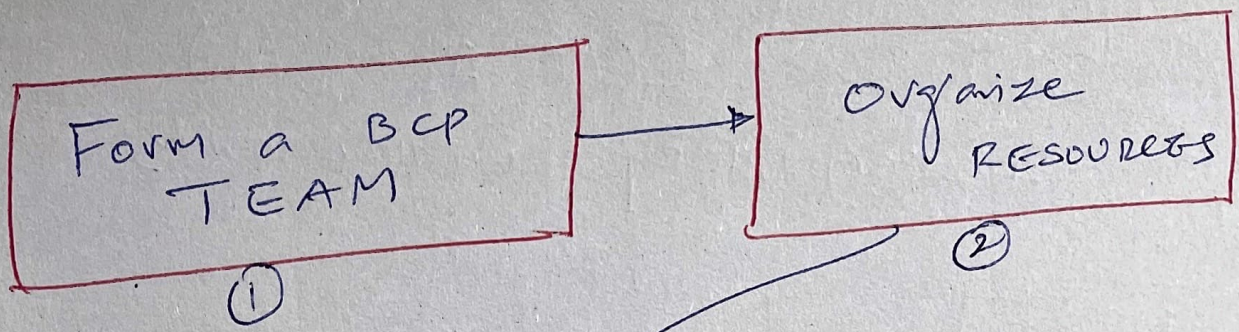
1 | BCP | Project Scope & Planning



1 Person from Each Department who is responsible for financial core business service

= BCP SQUAD / TEAM





3 Phases

1. BCP Development
   - ↳ mostly BCP team members
2. BCP Testing, Training & Maintenance
   - ↳ H/W + S/W commitments
   - ↳ Employees involved into BCP.
3. BCP Implementation
   - ↳ Requires significant resources
   - ↳ prepare to fight with senior mgmt to get more resources with BCP business cases.

Mgmt don't want to invest $$ for BCP?
Ask this question —
How long seat-of-the-pant recovery might take when compare to orderly, planned continuity of operations

SEAT-OF-THE PANTS ATTITUDE

$1M

vs

BCP

$200K

→ consider disaster business cost & indirect cost of lost opportunities.

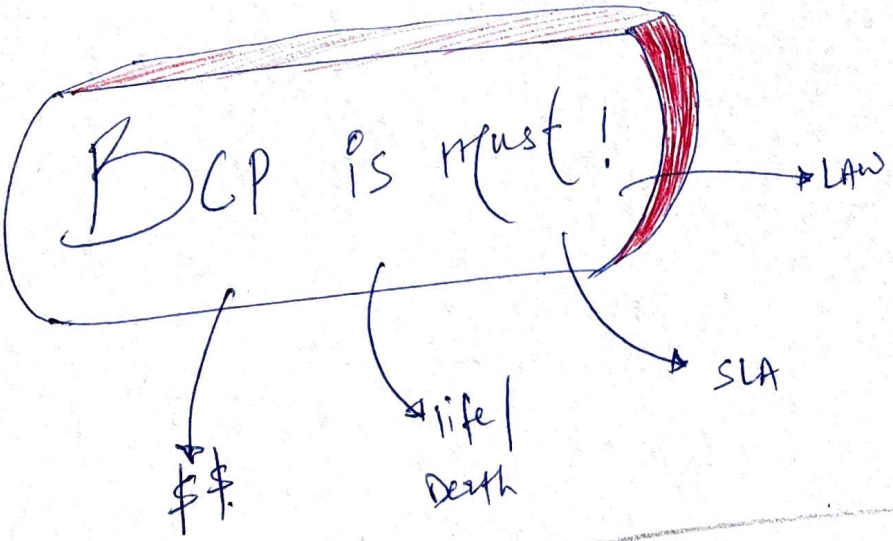
ENFORCE BCP AS LAW + REGULATORY REQUIREMENTS

BCP = LIFE OR DEATH.

BCP Promises = Contractual obligation | SLA from customers.

w/ 3 parties

Win NEW clients $ $$$



Get BCP policy Documented & get a formal approval from the management.

2 | BCP | BIA

STEP-1 , Business Impact Analysis STEP-2 = HEART , STEP-3 → P.T.O

STEP-4 → P.T.O

STEP-5 → P.T.O

YOU ARE HERE

Analysis

Quantative (Numbers + Formula + $$ figures)

Qualitative (scenario + intuition + experience)

~~Plan Implement Tests~~

Decision

WHAT IS BIA ANYWAY ??

↑ BIA identifies RESOURCES that are critical to organization, also threats to those RESOURCES, & likelihood of impact those threats on business

Data loss tolerance = defined back up strategy

RPO = Recovery of Data

NETFLIX IS DOWN

Plan for DIF/WIFE SKETCH

MTD / MTO
- Maximum Tolerable Downtime or outage

2 hours

RTO = Recovery of ~~data~~ mission critical process
- Recovery Time Objective

1 hour

MTD > RTO — should be

BIA Process

1. Identify Priorities
   - Quantitative measure
   - Netflix Example (← P.T.O)
   - with MTD & RTO
2. Risk Identification
   - Qualitative in nature
   - Natural Risks
   - Man-made Risks
3. Likelihood Assessment
   - ARO
4. P.T.O
5. P.T.O +2

USGS
- US Geological survey
FREE RISK REPORTS

JAPAN'S EARTHQUAKE
↳ 5-6 / year
⇓
ARO
Annualized Rate of occurance

Organization + Insurance company = Risk transfer

⇓
Perform Risk Assessment
=
MUTUAL BENEFIT.

SPIN-OFF
(side note)

BIA for cloud = SOC

Service Organization control

Form of Assessment → SOC Report

cloud vendor → Provide

✗ SOC 1 → only internal control / descriptions

✓ SOC 2/3 → Security, Privacy, Availability controls

4 MOST CRITICAL STEP

Impact Assessment

FEED ①
- 3. Identified Risks +
- 4. Likelihood

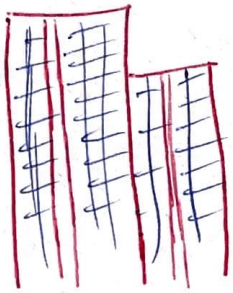
② Produce overall Business Impact.

Quantitive Perspective
- AV
- EF
- SLE
- ALE
- ARO

ARO = likelihood
Eg Five 1 in 30 year

$$30 \overline{)100} \quad 0.03$$

ARO = 0.03%.



BUILDING
$500K

AV = Asset value

one Five = 70% Damage

EF = Exposure Factore

Single time loss due to Five

SLE

$$SLE = AV * EF$$

$$= \$500K * 70\%$$

$$SLE = \$350K$$

Five occurs once every 30 years

ARO = 1/30
= 0.03

$$ALE = SLE * ARO$$
$$= \$350K * 0.03$$
$$= \$10,500$$

Annualized Loss Expectancy - Business can expect loss of $10,500 every year due to Five in Building.

→ stock price ↓

→ Negative publicity = News

→ loss of client / Damage Reputation

→ loss of Employees

BUSINESS IMPACT.

5th

Resource Prioritization

Quantitative Analysis

Qualitative Analysis

FEED

PRIORITY LIST

1. Fire ALE ~~
2. Earthquake ~~
3. ~~
4. ~~
5. ~~

→ See what happens to this list in strategy development (p. to x2)

~~BCP PROCESS - TREE SO FAR~~

BCP PROCESS

Project Scope & planning

BIA

1

2

3 Continuity Planning

4 Approval & Implementation

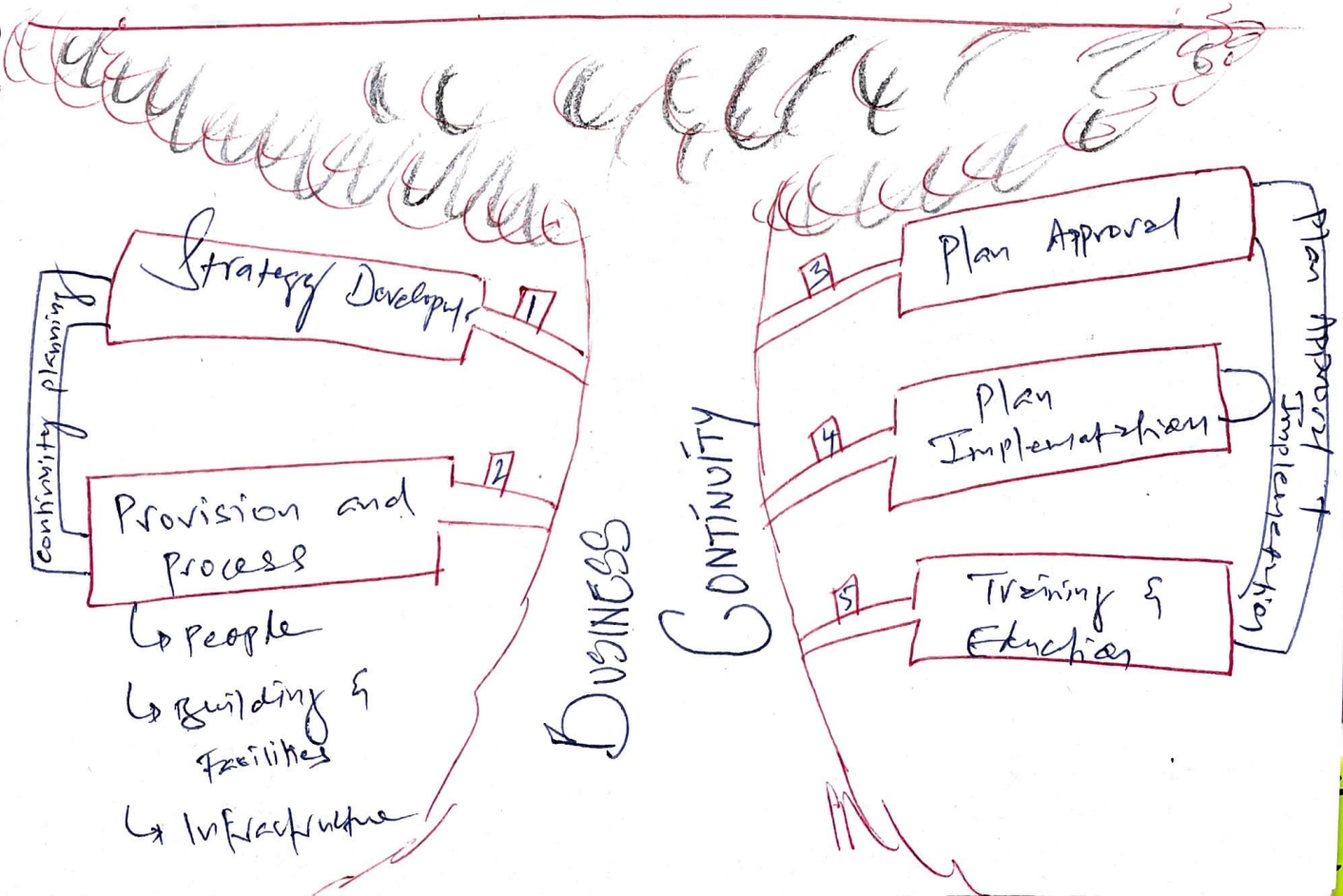
3	BCP	CONTINUITY PLANNING

1	Project planning
2	BIA

FOCUS —
- How BCP Process will work
- BCP speed
- What are the Priority Business Asset in case of interruption.

FOCUS 1

- Whatever impact we realized from (1) & (2)
  - → How BCP strategy will be DEVELOPED + IMPLEMENTED.



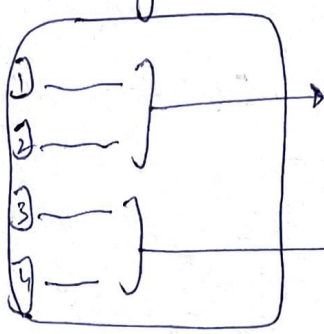
1. STRATEGY DEVELOPMENT

BIA — STRATEGY DEVEL. — CONTINUITY PLANNING PHASE

BRIDGE

BIA's step (5)

Priority list



1, 2 → Risk Accepted = No Problem

3, 4 → Risk to be mitigated

- Who will mitigate? (Resource)
- How it will mitigate? (Plan + implementation)

Feed into Next step

2. PROVISION & PROCESSES

Because this is where we mitigate

→ MEAT OF BCP

Saves 3 types of Assets

1. People
2. Building & Facilities
3. Infrastructure

HUMAN = MOST VALUABLE ASSET

Building Facilities

- Hardening provisions → Existing site → Fix leaky roof
- Alternate site → if Existing site hardening fails.

Hot, Cold, Warm sites

Infrastructure

→ Physical Hardening

- UPS x Racks
- Fire Alarms
- sprinklers

Alternate systems

Redundancy ---- Availability

DC1 Sydney

DC2 Melb.

4	BCP Plan Approval + Implementation

Business continuity planning

5	BCP

BRIDGE

1	BCP
2	

GET APPROVAL FROM SENIOR MGMT.

1. Plan Approval

Try to get endorsed by top executive such as CEO for BCP importance + WEIGHT

2. Plan Implementation

↳ Deploy BCP resources

3. Training & Education

↳ BCP resource

↳ Backup resource

4. BCP Documentation

↳ Event / Emergency

↳ Historic records

Important components of BCP

1. Statement of Importance
   - Signed by BCP Lead, CEO with CEO signature
   - BCP Lead, CEO = weight
   - BCP Team, lower mgt = Resistance
2. Statement of Priorities
   - critical Business Functions in order of priority for continue operation
   - Priority list from BIA
3. Statement of Organization Responsibility
   - can be incorated to Statement of Importance
   - SENTIMENT: BCP IS EVERYONE'S RESPONSIBILITY.
4. Statement of Urgency & Timing
   - outlines implementation of timetable
   - shows why BCP is critical.
5. Risk Assessment → All that Formulas & Maths.
6. Risk Acceptance / Mitigation
   - RISK → Accepted = Reason?
   - RISK → Unaccepted = Security control

ASK BUSINESS LEADER A QUESTION

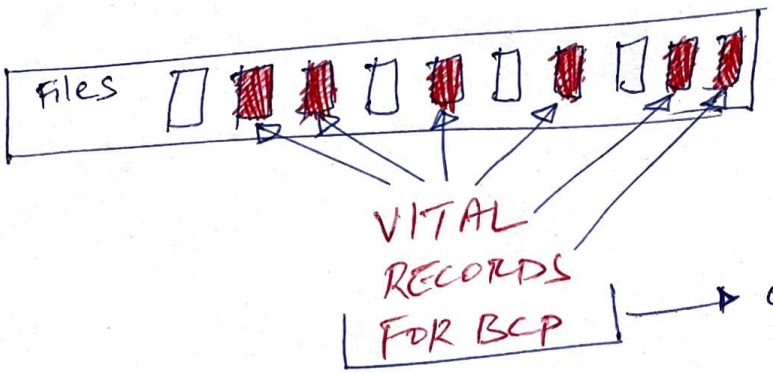
Why Risk is accepted! (residual risk)

7 Vital Records Program

→ what records you need if we have to rebuild the organization in new location without accessing computers?

↳ How to retriere Docs | Records in Disester!

↳ where is it stored!



8 Maintainance

↳ Living Document for BCP

↳ Periodic update

↳ version control

↳ Destroy old versions.

It's good practise to include BCP components in job descriptions, to keep it remains fresh.

9 Emergy - Response Guidelines

↳ New employee should be able respond to emergency situation

↳ guidelize response procedures

↳ whom to contact / notified of the incident

↳ secondary response procedures.

Emergency guidelines should be easily accessible to employee in the organization

10 Testing & Exercise

↳ chap: 18

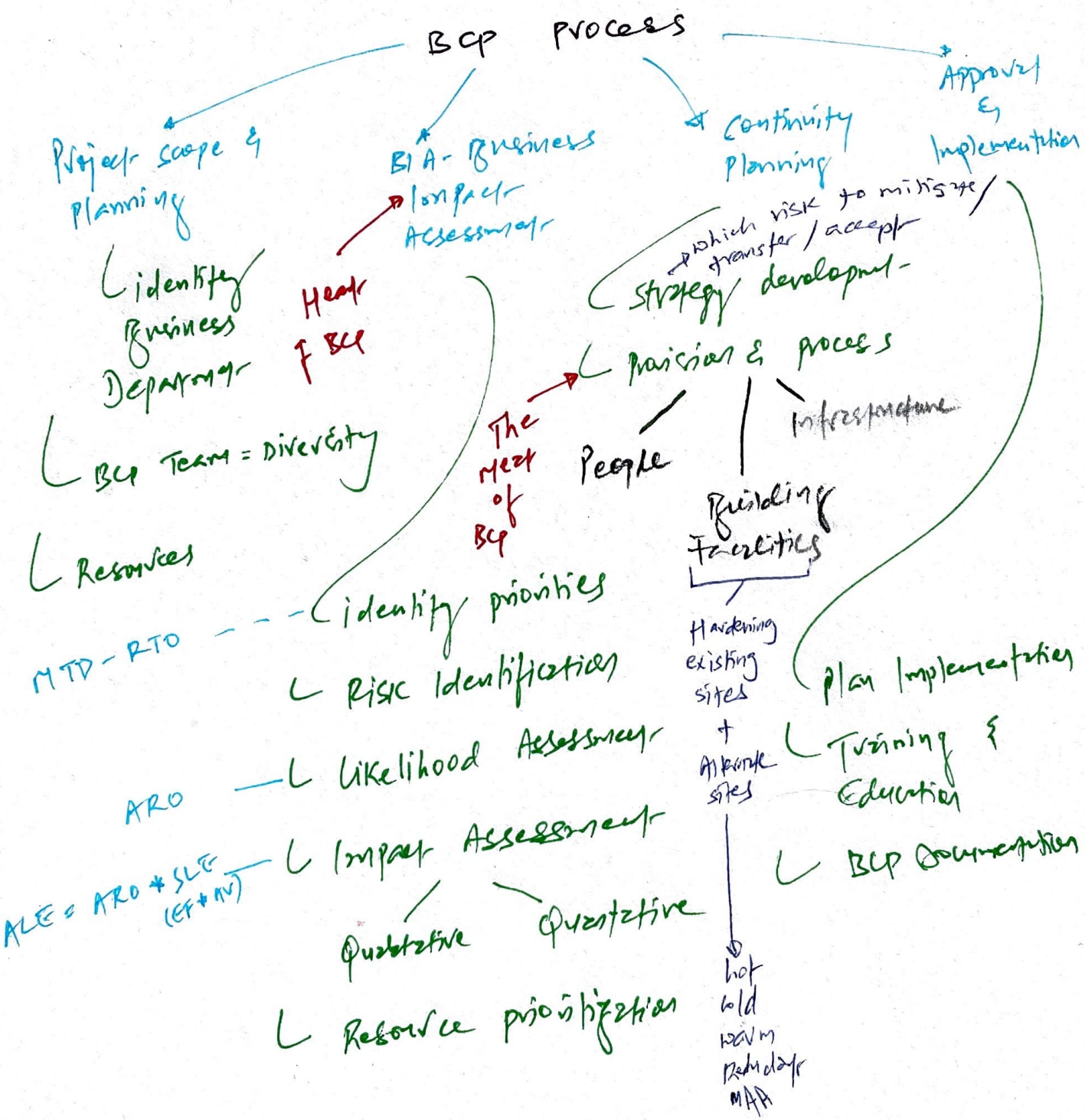
BCP doc to ensure that personnels are trained to perform their duties in the event of disaster.

Slowing down continuity process will blow MTD!!

BCP / DRP Planning High level steps

Blueprint

BCP/DRP Ultimate Goal – To restore normal business operations after disaster struck using effective and secure strategies.



BCP / DR → Deals with → Availability of CIA Triad

You very need a BCP coordinator who would liaise with employees, mgmt

Business Impact Analysis is different than Risk Analysis

Identify critical business process & functions & assign criticality score to those processes

→ if router is down, what's the MTD? what's the RTO? Before business losing $$$

identify Assets & assign criticality or risk score

Router has higher Risk score than desktop computer

BIA's two exclusive thoughts

→ if it doesn't happen, that doesn't mean we can't plan for it.

→ if it most likely won't happen, that doesn't mean we can't assign the risk score. just assign the lower risk score

Eg (>100M file must be scanned for malware = 100 risk)

location, location, location

Mantra Real Estate agent

Document, Document, Document

IT mantra

BIA General steps

- Who is going to be interviewed / (Identify stakeholders)?
- What techniques to gather data?
  - Q&A / interview
  - Quantative + Qualitative Analysis
- What are business critical functions?
  - Amazon APP - Products
    (Netflix) — movie Portal
- What critical resources each critical function requires?
  - Front End UI

How long each critical functions survive without critical resources?

- Without Web UI, how impact will be for Amazon (Netflix)

What are the THREATS to these critical Functions?

- Hack
- DDoS
- Misconfiguration
- Human Error / mistake

Amazon (Netflix) Front UI = Mission critical

Assign MTD rating to each critical Function (business)

Document & Submit to Senior management.

THIS IS LUKE AHMED'S BIA PERSPECTIVE

BCP Development Process

1. Develop BCP Policy statement (RMF Prepare)
   - High-level executive direction on what BCP accomplish + required resources
2. Conduct BIA
   - How to mitigate & their associated costs
   - (below :-)
3. Identify Preventive Controls (above :-) NIST-800-53
   - Identify critical business process + function (MTD, RTO, RPO, WRT)
4. Develop Recovery strategies — IT staff develop DRP
   - How IT service will be restored in order of priority. This includes
5. Develop an IT contigency plan
6. Perform DRP testing & training
   - Test DRP to ensure method + identify Gaps.
7. Perform BCP / DRP maintenance. (RMF Phase 6)
   - Review BCP & DRP process every three months
   - Audit annually.

Development of BCP starts from these steps.

4. Laws, Regulations, & Compliance

PERSPECTIVE

Four Security Issues

- Computer crime
- Intellectual Property
- Data Privacy
- Software Licencing.

To Govern these issues

WE HAVE **LAWS**

- Criminal Law
- Civil Law
- Administrative Law

--- overlapping laws ↓ + Multiple Jurisdictions =

CONFUSION

CRIMINAL LAW

100%.

Federal + state government

↳ Computer fraud

↳ Abuse Act

↳ Electronic & comms. privacy Act

↳ Identity Theft

↳ Digital Millennium copyright

CIVIL LAW

Min. Govt involvment

Transaction

People

organization

↳ Trademark

↳ Patent laws

Branch

Administrative Law

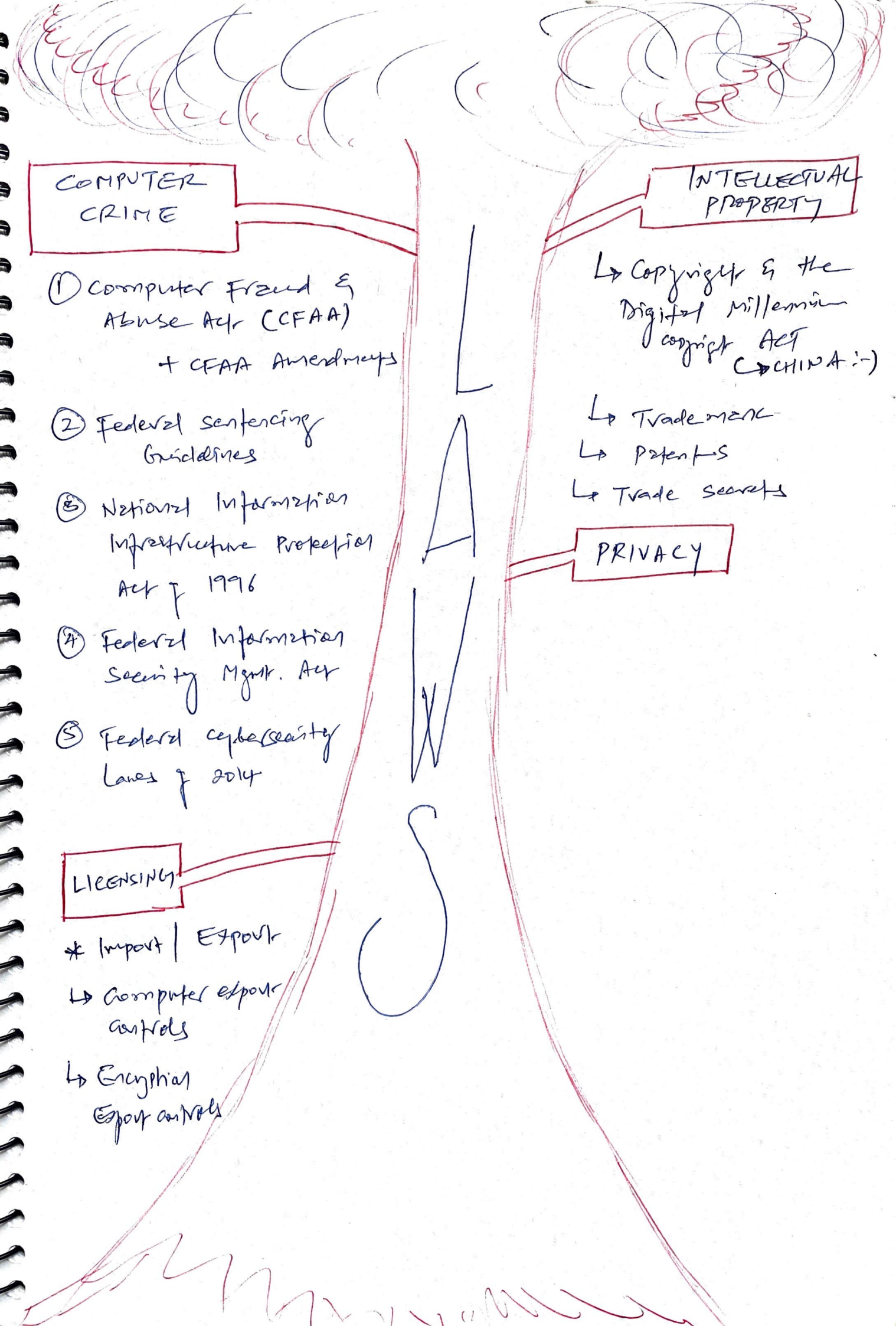
Government Agencies

↳ Day to day activities

↳ HIPPA :

/

Specific industry + Data Types


COMPUTER CRIME
1) Computer Fraud & Abuse Act (CFAA) + CFAA Amendments
2) Federal sentencing Guidelines
3) National Information Infrastructure Protection Act of 1996
4) Federal Information Security Mgmt. Act
5) Federal cybersecurity Laws of 2014
LICENSING
* Import | Export
↳ Computer export controls
↳ Encryption Export controls
INTELLECTUAL PROPERTY
↳ Copyright & the Digital Millennium copyright ACT
↳ CHINA :-)
↳ Trademark
↳ patents
↳ Trade secrets
PRIVACY
LAWS

Copyright

Protects the original work of Aut

Protects the work, not the creator

Trademark

Name, slogan, logo

Patent

Protection for creators of new inventions

protects the creator

- right to obscurity for death

Trade secret

protects the operating law of firm

Digital Millenium copyright Act of 1998

- prohibits copy protection mechanism placed in digital media + limits the liability of ISP for activities of their users

Economic Espionage Act of 1996

- Penalty to individuals who found guilty of the theft of trade secret

(If it's a benefit of foreign govmt)

Licensing

- Contractual
- Shrink-wrap
- Click-Through
- Cloud Services

NOTES FROM PSA

Multi-factor Authentication

- Something you know
  - Password
  - PIN
  - Security question
- Something you ARE
  - Fingerprint
- Something you have
- Somewhere you are

Note :- True MFA is the one when we use technique from each category (Password + Fingerprint)

To licence manifacturing process to other companies

- Patent
  - ✓ Suitable
- Trade secret
  - ✗ only appropriate when details can be tightly controlled within organization