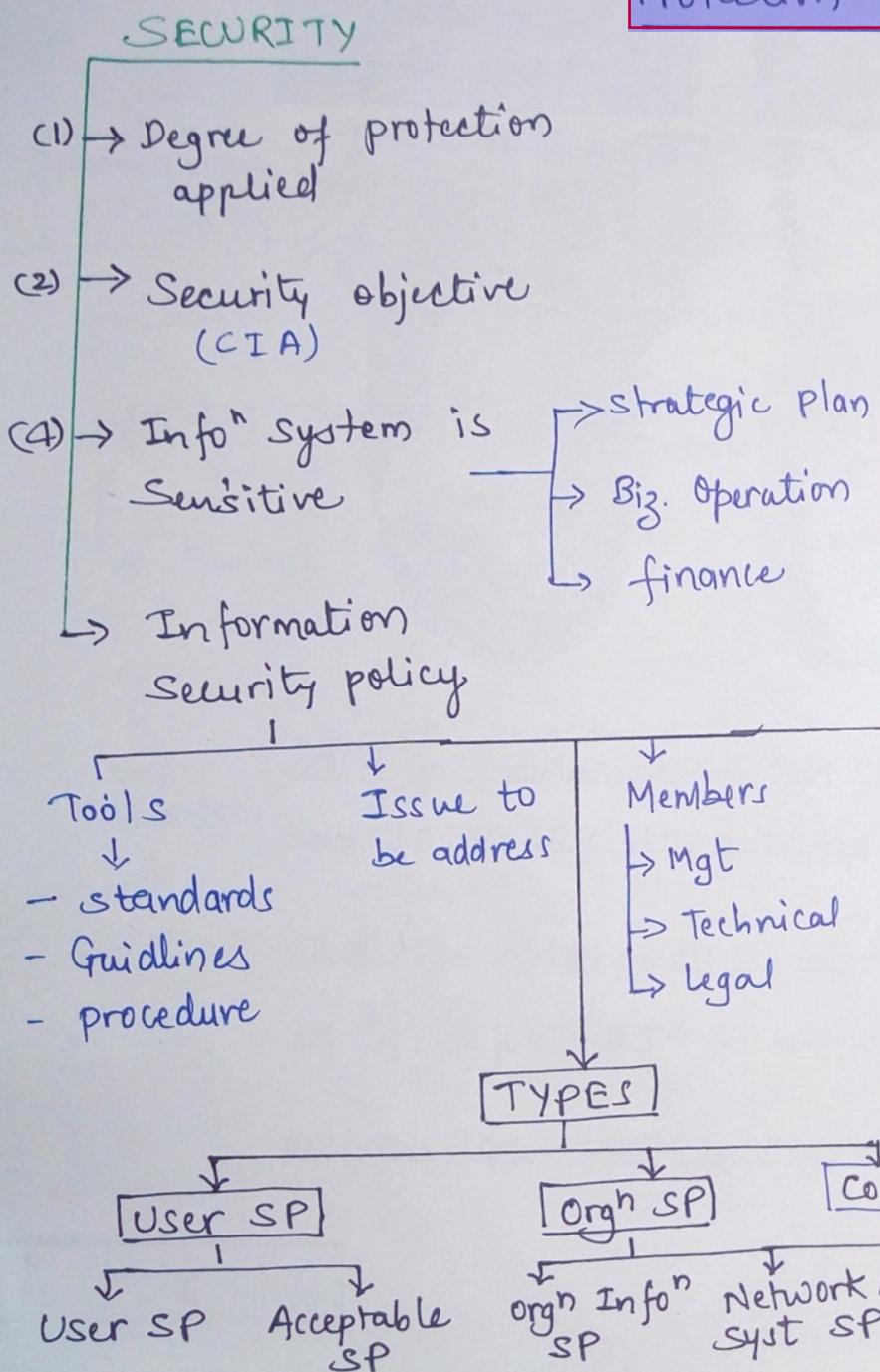


SP = Security Policy

CHP 3

(2)

(1)



CHP - 8B3
Protection of Infoⁿ system

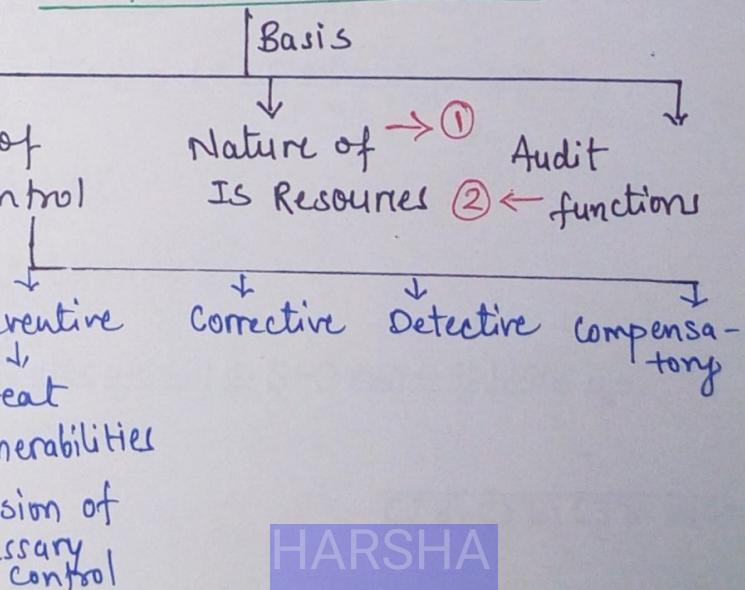
Impact of Technology
on Internal Control

- (1) Competent & Trustworthy Personnel
- (2) Segregation of Duties
- (3) Authorization Procedure
- (4) Adequate Doc^m & Records
- (5) Physical control over Assets & Records
- (6) Adequate mgt supervision
- (7) Independent check on Performance

(8) Comparing Records
Accountability with Assets

(9) Delegation of Authority & Responsibility

Classification of IS controls



CHP 3

(2)

①

Nature of Infoⁿ System Resources

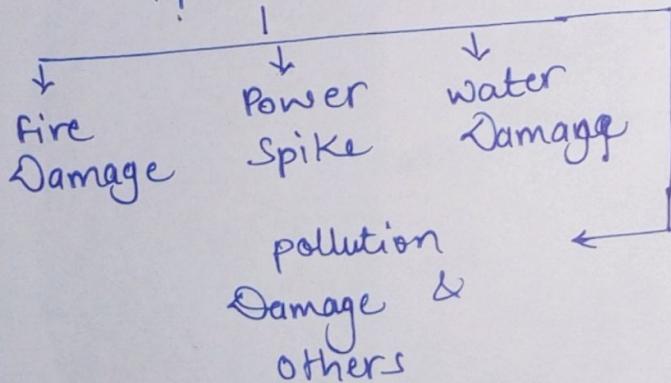
(A)

Environmental Control

→ Issue & Exposures

→ Categorization of Resources

→ Controls for Environment Exposures



- HW & Media
- facilities
- Documentation
- Supplies
- people

(B)

Physical Access control

- Lock on Doors
 - Cipher lock
 - Bolting lock
 - Electronic lock

→ Physical Identification Medium

- PIN
- Plastic cards
- Identification Badges

→ Logging on facilities

- Manual
- Electronic

→ other means of controlling physical access

(C) Logical Access (LA) control

↓
Exposures
(Exp.)

↓
LA Path

- Technical Exp.
(Data didling,
Bomb, Trojan
Horse....)
- Computer crime
Exp.
(Financial loss,
Sabotage, spoofing
etc....)
- Asynchronous
Attacks
(Data leakage
wire tapping
piggy backing...)

↓
Online
Terminals

↓
- Dial up
ports

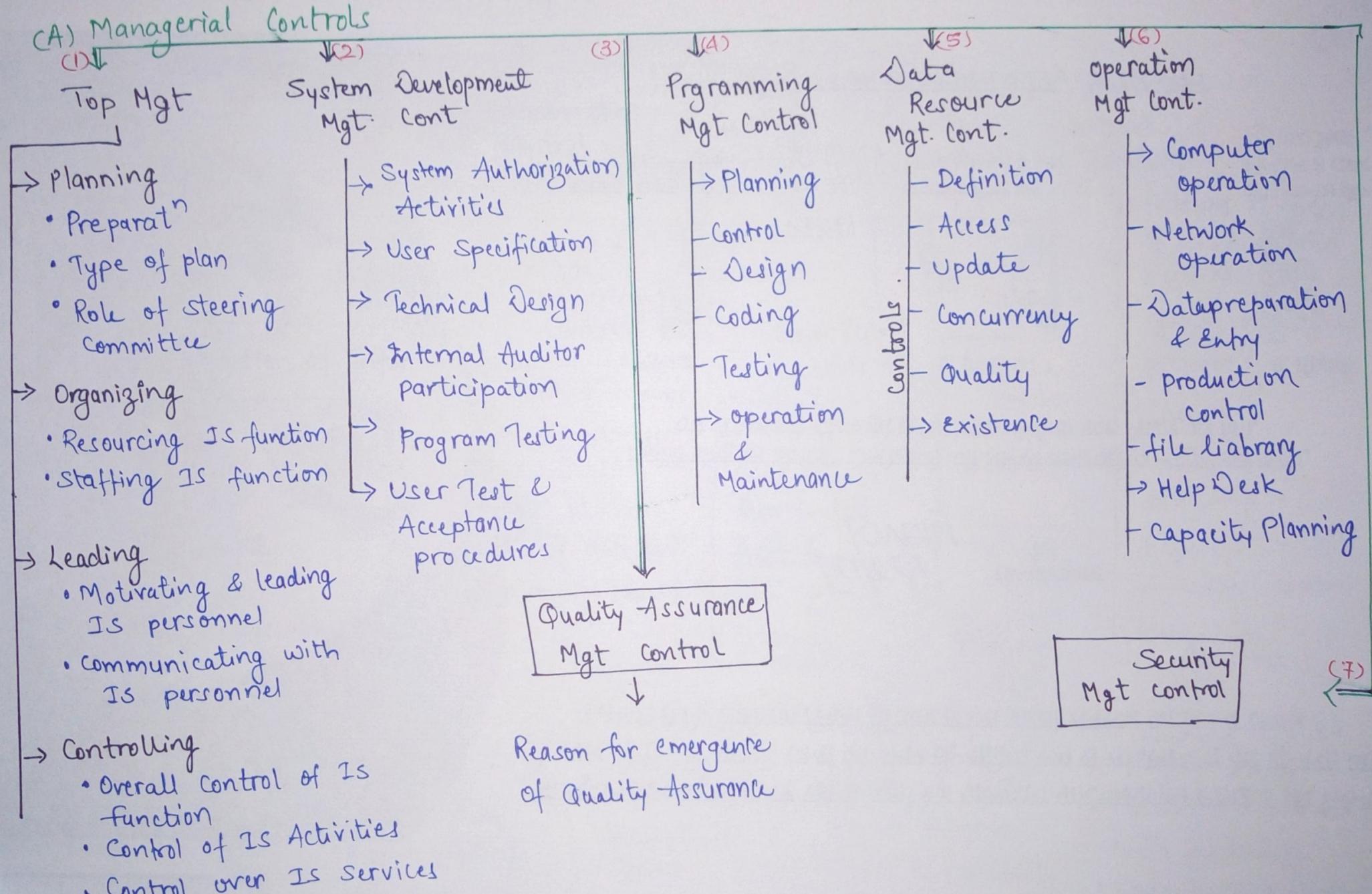
↓
- Telecomm
Network

HARSHA

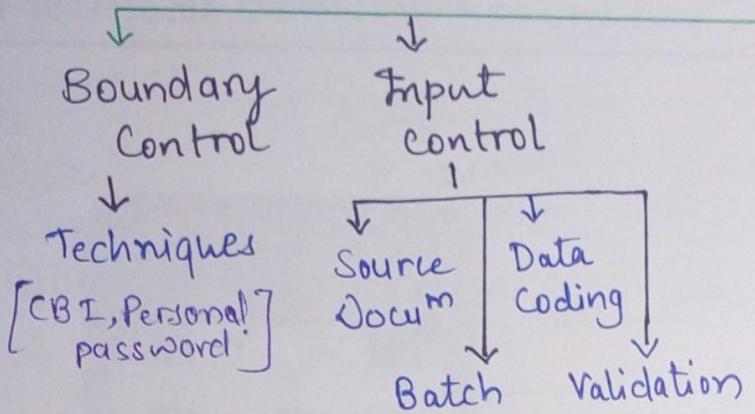
ON The Basis of Audit function

CHP 3

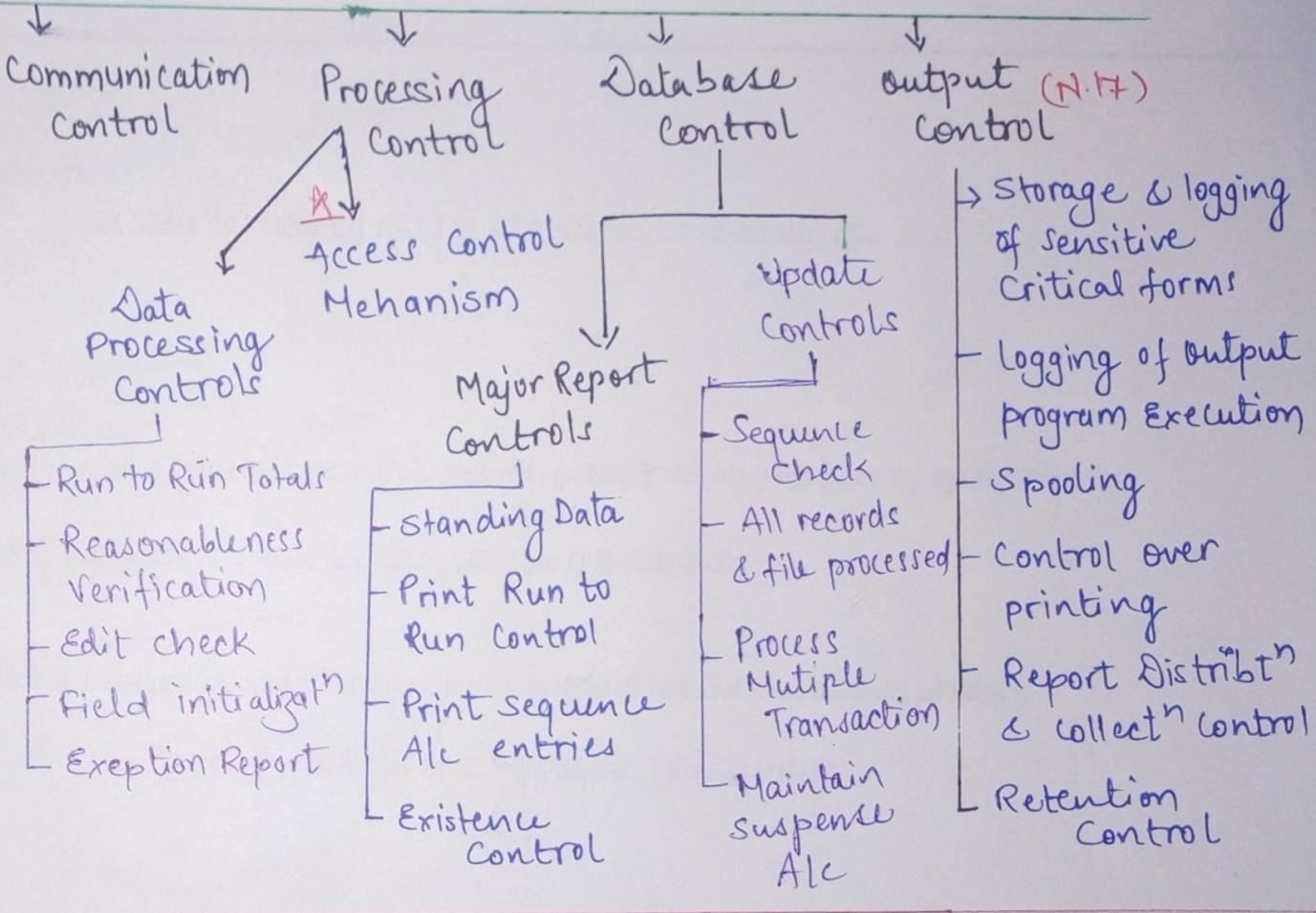
(3)



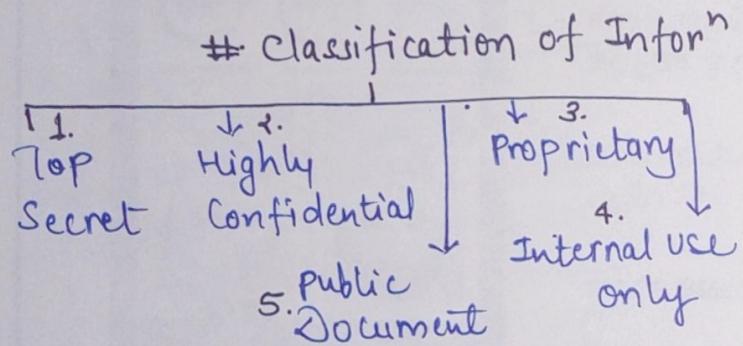
CHP 3



(B) APPLICATION Control



(4)



financial controls
[Input ABCD in safe document]

Personnel computer controls

- | | |
|---|--|
| Risk | Measures |
| <ul style="list-style-type: none"> • Small in size • Conveniently Transported • Single user oriented • No segregation duty • Weak access control | <ul style="list-style-type: none"> • Physical lock • Proper logging • Dis lock • Centralized purchase • antimalware s/w |

cyber Attack

- Phishing
- N/w scanning
- Virus code
- spam
- others

Impact of cyber fraud

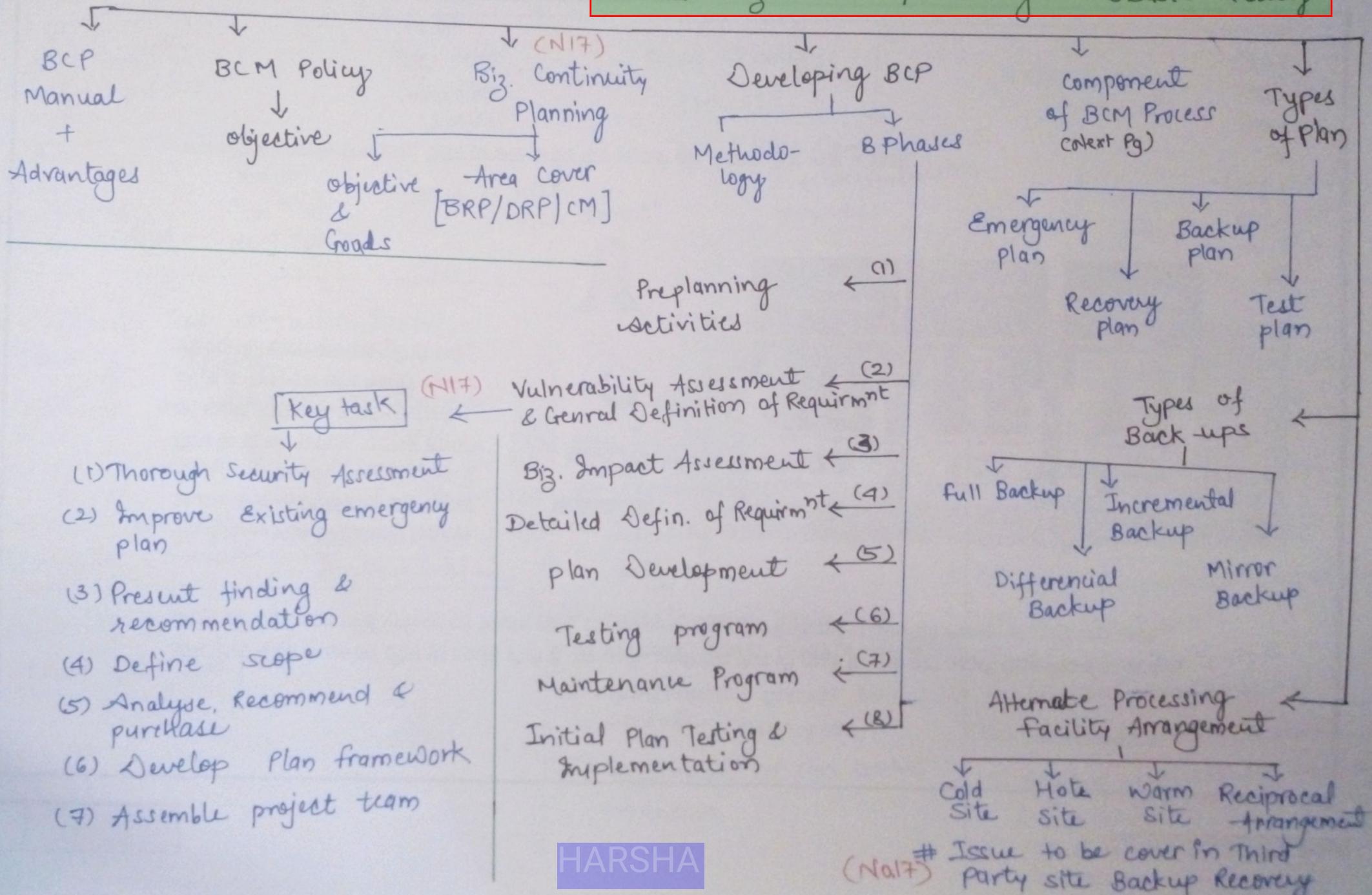
- financial loss
- Legal Reperc.
- Loss of credibility
- Disclosure
- sabotage

Technique of cyber fraud

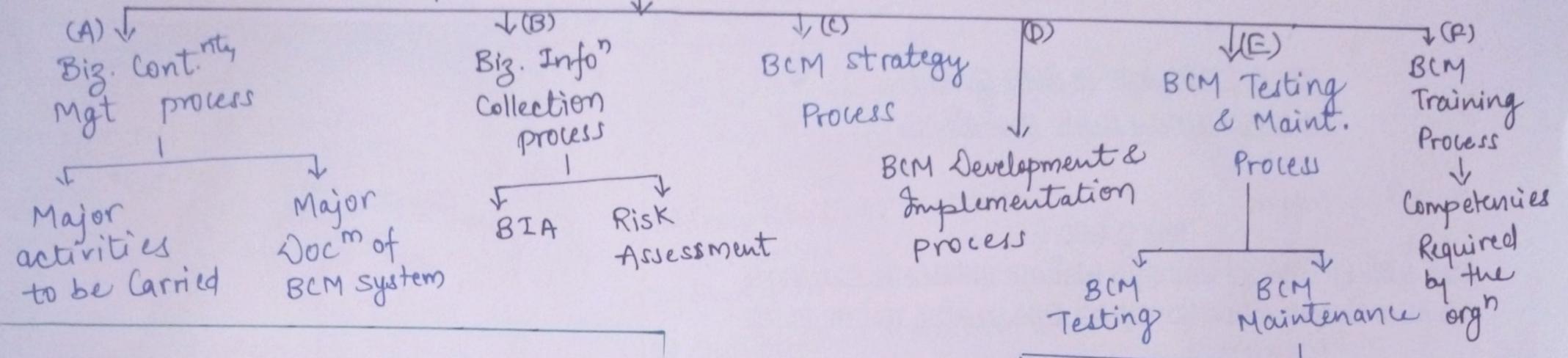
- Hacking • Cracking
- Data Diddling
- Data Leakage
- Piggybacking
- Logic Time Bomb
- B Dos etc.

CHP 4

CHP - 4 Biz. Continuity Planning & Disaster Recovery



Components of BIM Process



Contents of Disaster Recovery Planning Document

- | | |
|--------------------------------|--------------------------------------|
| (1) Cond'n for activating plan | (5) Maintenance schedule |
| (2) Emergency procedure | (6) Awareness & education activities |
| (3) fallback procedure | (7) Responsibilities of individuals |
| (4) Resumption procedure | |

Audit of BCP & DRP (Read from Book / PM)

- Maintenance Task in Development of BCP
- (1) Determine ownership & responsibility
 - (2) Identify BCP maintenance triggers
 - (3) maintenance regime to ensure plan remain up to date
 - (4) maintenance process to update the plan
 - (5) Implement version control procedure
 - (6) Audit/self assessment of BIM program
 - (7) Identify & include key product & services
 - (8) Priorities & requirement
 - (9) BIM competence & capability
 - (10) BIM solutions
 - (11) Exercising program & effective implementation
 - (12) Incorporate improvement
 - (13) Ongoing program for training & awareness
 - (14) Effective Comm'n of prod procedure