ISCA
CA FINAL
CHP 3
SUMMARY OF MAIN POINTS

BY- Ankita Chawla

P.S. - Do update from Jan 2016 Module as some changes made.

Chp 3.

★ IS Control Tech (Pg 3.12 to 3.50 + 3.11)

↓

Categories of Control

↓

On basis of

↓

1) Obj
   a) Preventive ← understand Vulnerabilities, probable threat, Prov for control
   b) Detective
   c) Corrective
   d) Compensatory

2) Functional
   a) Int Ac"
   b) operational
   c) Adm."

3) IS Resource.
   a) Environmental
      - IS resource in regard to env
        - i) Hardware & Media
        - IS supporting Infra & facilities
        - Documentation
        - Supplies
        - People.

(Control for Env exposures)

i) Water Detector
ii) Hand Held Fix extinguisher
iii) Manual Fix Alarms
iv) Smoke Detectors
v) Fire suppression system
   - Dry Pipe Sprinkling System
   - Water based system
   - Halon.

vi) Strategically locating the compu room
vii) Regular inspection by Fire deptt
viii) Fireproof walls, floor, & ceilings surrounding the computer room
ix) Electrical surge Protection
x) UPS / generator
xi) Power leads from two substation
xii) Emergency Power off switch
xiii) Wiring placed in Electrical panels and conduit
xiv) Prohibition against eating, drink^n, smoking within the inf^n proces^n facility.
xv) Fire resistant office material
xvi) Documented & Tested Emergency Evacuation plans.
xvii) Power Supply variation

b) Physical Access Controls
i) Locks on Doors
- Cipher Locks
- Bolting Door Locks
- Electronic Door Locks
- Biometric Door Locks

ii) Physical Identification Medium
- PIN
- Plastic card
- Identification Badges

iii) Logging on Facilities
- ~~Logging of Acces~~ Manual logging
- Electronic Logging

iv) Others
- Video cameras
- Security guards
- Controlled Visitor Access
- Bonded Personnel
- Dead Man Doors
- Non Exposure of sensitive facilities
- Computer Terminal locks
- Controlled single entry point
- Alarm system
- Perimeter fencing
- Control of out of hour of employee
- Secured Report / Docu dist" cart

c) Logical Access Controls

1) Logical Access Paths
   a) Online Terminals
   b) operator Console
   c) Dial up Ports
   d) Telecommunication Network Issues and Revelations related to
2) Logical ~~Contrl Exposure~~ Access
   a) Technical Exposures
      i) Data Diddling
      ii) Bombs
         - Time Bomb
         - Logic Bomb.
      iii) Trojan Horse
      iv) Worms
      v) Rounding down
      vi) Salami Technique
      vii) Trap doors

   b) Computer Crime Exposures
      i) Financial Loss
      ii) Legal Repurcations
      iii) Loss of Credibility or competitive edg.
      iv) Blackmail / Industrial Espionage
      v) Disclosure of confidential sensitive or Embarassing inf^{n}.

vi) Sabotage
vii) Spoofing

c) Asynchronous Attacks
i) Data leakage
ii) Wire tapping
iii) Piggybacking
iv) Denial of service / shutting down of computer

4) Audit functions
a) Managerial Controls (Subsystems)
i) Top Mngmt
(Function: Planning, org, leading, Controlling)
ii) System developement Mngmt controls
(Types of audit during SDMC)
- Concurrent, Post-implementation general.
iii) Prog Mngmt Cntl
(Phases: Planning, Design, Coding, Testing)
iv) Data Resource Mngmt Cntl
v) Quality Assurance Mngmt Cntl

vi) Security Mngmt Cntl
vii) Operations Mngmt Cntl

b) Applications Controls (Categories)

i) Boundary
- Cryptography
- Passwords
- PIN
- Identification Cards
- Biometric devices

ii) Input Controls
- Source Document Cntrl
  a) Pre-numbered
  b) Sequence
  c) Periodical audit
- Data Coding Controls
  a) Transcription
     - Addition
     - Truncation
     - Substitution
  b) Transposition
     - Single
     - Multiple
- Batch Controls
  a) Physical
  b) Logical

- Validation Controls
  a) Field Interrogation
     - Limit check
     - Picture checks
     - Valid Code
     - Check digit
     - Arithmetic
  b) Record Interrogation
     - Reasonableness check
     - Valid sign
     - Sequence check
  c) File Interrogation
     - Version usage
     - Internal & External labeling
     - Data file security
     - Before & After Image & logging
     - File updating & maintenance authorization
     - Parity check

iii) Commⁿ Controls
- Physical Component Controls
  a) Transmission Media < Guided/Bound, unguided
  b) Communication lines
  c) Modem
  d) Pod Protection Devices

e) Multiplexers & Concentrators
- Line Error Control
  a) Error Detection
  b) Error Correction
- Flow Control
- Link Control
- Topological Control
  a) LAN
  b) WAN
- Channel Access Control
  a) Polling
  b) Contention Methods
- Internetworking Control

Devices used to connect sub networks:
  a) Bridge
  b) Router
  c) Gateway

iv) Processing Control
- Processor Control
- Real Memory Control
  a) Error Detection & Correction
  b) Multiple Execution States
  c) Timing Control
  d) Component Replication
- Virtual Memory control

Data Processing Controls
- Run to Run totals
- Reasonable verification
- Edit Checks
- Field Initialization
- Exception reports

v) Output Controls
- Storage & logging of sensitive, critical forms
- Logging of output program executions
- Spooling / Queuing
- Controls over printing
- Report dist" & collection controls
- Retention Controls

vi) Database Controls
- Major Update Controls
a) Sequence Check bet trnsc" and Master files
b) Ensure all record on files are processed
c) Maintain a suspense a/c
- Major Report Controls
a) Standing data

b) Print Run to Run Control totals
c) Print suspense a/c entries
d) Existence / Recovery Control

★ General Controls (Pg 3.50 to 3.64)

1) Operating System Controls
- Operating system task
- Control obj
- Opr System security (security components)
  a) Log-in Procedure
  b) Access Token
  c) Acan Control list
  d) Discretionary Accen Control
- Remedy from destructive programs

2) Data Management Controls
- Access Controls
- Back up controls (Back up strategies)
  a) Dual Recording of data
  b) Periodic dumping of data
  c) Logging input transaction
  d) Logging changes to the data

3) Organisational Controls
(Techniques include documentation of:)
a) Responsibilities & objectives
b) Policies, std's, procedures and practices
c) Job descriptions
d) Segregation of duties

4) Financial Controls:
(Techniques)
a) Authorization
b) Budgets
c) Cancellation of documents
d) Documentation
e) Dual Control
f) Input / Output verification
g) SafeKeeping
h) Sequentially numbered docs
i) Supervisory reviews

5) BCP Controls

6) Management Controls (Considerations)
a) Responsibility
b) An IT org" structure
c) An IT steering committee

7) System Developement Controls
(Six activities)
a) System Authorization
b) User Specification
c) Technical Design
d) Internal Auditor's Participation
e) Program Testing
f) User Test & Acceptance procedures.

8) Computer Centre Security and controls
- Physical Security
a) Fire Damage
b) Water Damage
c) Power Supply Variation
d) Pollution Damage
e) Unauthorised Intrusion
- Software & Data Security (Pg 3.61)
- Data communication Security (Pg 3.61)

9) Internet & Intranet Controls
- Major Exposures
a) Component Failure

1) Communication line
2) Hardware
3) Software

b) Subversive threats
1) Invasive Tap
2) Inductive Tap

- Mechanism to control risk
a) Firewall
b) Controlling DOS Attack
c) Encryption
d) Recording of Transaction Log
e) Call Back Device

10) Personal Computer Controls (Pg 3.64)

☆ Data Integrity

Five Scale grade
- Top secret
- Highly confidential
- Proprietory
- Internal use only
- Public Documents

Ankita

6 Categories of Integrity control
- Source Data Control
- Input Validation Control
- On line Data Entry Controls
- Data Processing and storage control
- Output controls
- Data communication control

Data Integrity Policies
- Virus signature updating
- Software testing
- Division of Environments
- Offsite Backup Storage
- Quarter end and year end Backups
- Disaster Recovery

→ Q33 to Q37
Pg 3.17 to 3.19 of summary book.