CA Final ISCA Ch.3 Summary Notes by CA Amruta Sherde

Ch.3 Pg 1

# Ch.3 Protection of IS

## Basics

- Gap between need to protect sys & degree of protection applied
  Reasons [WIDE UNE]
  - Widespread use of technology
  - Interconnectivity of systems
  - Devolution of mngt & control
  - Elimination of distance, time & space as constraints
  - Unevenness of tech change
  - Attractiveness of conducting unconvent$^{n}$ electronic attacks
  - External factors

## IS Security

- Security objective [CIA]
  - Confidentiality
  - Integrity
  - Availability
- What info is sensitive? [FOS]
  - Finances
  - Business Operations
  - Strategic Plans

## IS Security Policy

- Tools to implement
  - Standards
  - Guidelines
  - Procedures
- Issues to address by IS Sec Policy
  [PEDIGREE - D]
  - Principles
  - Explanation of sec pol
  - Def$^{n}$ of IS
  - Importance of IS
  - Goals of IS
  - Responsibilities defined
  - Employees aware
  - access policy
  - Compliance requirement
  - Doc$^{n}$ supporting reference
- Members of Sec Policy [MTOL]
  - Mngt Members
  - Technical group
  - legal experts

## IS Controls - PTO

- Hierarchy

IS Sec Policy Types

- User sec Policy
  - → user sec Policy
  - → Acceptable Usage Policy
- Org$^{n}$ Sec Policy
  - → Org$^{n}$ IS Policy
  - → Info Classfn Policy
  - → Networked Sys Sec Policy
- Conditions of Connectn to Network

- Components of Sec Policy
  - Purpose & Scope
  - Intended Audience
  - Sec Infra
  - SP doc maintenance
  - compliance req
  - Incident response Mechanism
  - Incident reporting
  - Sec Org$^{n}$ structure
  - Inventory & classfn of assets
  - Tech descriptn
  - Computing standards
  - Phy & Env$^{t}$ Sec
  - Identity Mngt & Account
  - IT Op$^{n}$ Mngt
  - IT Chnum
  - Sys dvpt Maintenance
  - BCP
  - Legal Comp
  - Monitoring Req.
  - Audit Requirements

# Ch. 3 Protection of IS

## IS controls

## PTO for Classification

Ref Page 3

### Impact of tech. on Internal Controls

CR - DAD - SIPS

- Control over Assets & Record Physical.
- Recorded Accountability compared with Assets
- Delegation of Auth & Responsibility
- Authorization by Auditor
- Document & Records
- segregation of duties
- Independent Checks on Performance
- Personnel Competent & Trustworthy
- Supervision of Supervisors

Notes by CA Amruta Shevde

# Ch.3 - ISCA - Classification of IS Controls



ON FAG - PD
1 2 3 4 5 6 7

## 1 Objective of Controls
1) Preventive
2) Detective
3) Corrective
4) Compensatory

## 3 Financial
D-ABCD-SONS
Authorization - Dual control
Budget
Cancel docs
Dual controls.
Safekeeping
Output-Input verify
Numbered docs
Sign off.

## 4 Audit functions
1) Managerial
2) Application
Ref Pg. 5 & 6

## 5 General IT Controls
1) SDLC Controls
2) Computer Operation Controls
3) Syst & data backup & recovery controls.
4) Logical access controls -
5) Program Change Mngt controls -
6) Physical security cont.

## 6 Personal Computers Controls
Ref Pg.

## 7 Controls over Data Integrity & Security
Ref Pg. 7

## 2 Nature of IS Resources

### 1) Environmental Controls
- Issues & Exposures
  - Fire
  - Natural disasters
  - Power spikes
  - AC failure
  - Electrical shock
  - Equipment failure
  - Water damages
  - Floods
- Categories of IS Resources
  - HI - DSP
  - Hardware & Media
  - IS supporting Infra
  - Documentation
  - Supplies.
  - People
- Controls
  - FOR Power Spikes: EE-UP
    - Emergency power off
    - Electrical Surge Protector
    - UPS / Generator
    - Power supply Variation
  - FOR Water Damage: WW-PAID-LS
    - Water detector
    - Waterproof Walls
    - Proof ceiling/floors
    - Alarms.
    - Installations above
    - Drainage sys
    - Leakage indicator
    - Strategic location of computer room
  - FOR Pollution & others: EP-DP
    - Evacuation Plan
    - Power leads from 2 stations
    - Dust
    - Prohibitions food/drink/smoke
  - FOR Fire damage: AW-KISS-MMS-WWF-LEGS
    - Auto fire Alarm
    - Walls fire proof
    - Knowledge to staff
    - Inspection by fire dept.
    - Smoke detector
    - Supplementary Fire repression system
    - Manual fire Alarm
    - Master switches.
    - Signals to manned station
    - Wood & Plastic avoid Wiring
    - Fire extinguishers
    - Location of computer Room
    - Exit marks.
    - Gas based sys. Supression tech.

### 2) Physical Access Controls
- Issues & Exposures due to violation
  - AB-DE-DE-T
  - Abuse of resources
  - Blackmail
  - Damage
  - Embezzlement of assets
  - Disclosure of info
  - Entry to authorized.
  - Theft
- Possible Perpetrators: D-GOIN-DEAF
  - Discontented
  - Gamblers
  - On strike
  - Interested outsider
  - Notified for termination
  - Disciplinary action
  - Emotional problem
  - Accidentally.
  - Former employee

### 3) Logical Access Controls
Ref Pg. 4

- Controls: POLL
  - Physical Identification Medium
    - Personal Identf^n No.
    - Plastic Card
    - Identification Badge.
  - Others: BOLD SAGE CV on PC
    - Bonded Personnel
    - Out of office hrs
    - Locks
    - Dead Man Doors
    - Sensitive facilities non exposed
    - Alarm
    - Guards.
    - Entry Point Single
    - Cameras
    - Visitor Access Control.
    - Perimeter fencing
    - Cart secured for doc distribution
- Locks
  - Cipher, Bolting, Electronic, Biometric
- Logging
  - Electronic
  - Manual

Start

Classification of controls

ON FAG - PD

Nature of IS Resources -

# Segregation of Networks.
Enforced Path.
Network connection
Security of network services
Encryption
Call back device
Record Transaction Log
Policy on network use.
Firewall

Environmental Controls -
Ch-3 Pg 3

Physical Access Controls
Ch 3 Pg. 3

3) Logical Access Controls 'LA'

- Controls ~~UUN OAAA~~ UU-MOAN

- LA Paths - TO-DO
Telecom^n Network
Online Terminals
Dial up Ports
Operator console

- Issues & revelation wrt LA.

User Access Mngt
→ User Registration
→ Privilage Mngt
→ Password Mngt
→ Rights of Access.

User Responsibilities
→ Password use
→ Unattended equipment.

Mobile computing

Operating Sys Access Cont.
→ Terminal — Auto. Identfn, Log In Procedure, Time Out.
→ Access — Token, Control List, Discretionary Access.
→ User — Ident^n & Authent^n, Password Mngt, Sys Utilities -, Alarm, connection time limit

Applicatn & Monitoring sys Access
→ Sensitive sys Isolation
→ Info Access Restriction
→ Monitor sys Use
→ Event Logging -
→ Clock sync

Network Access Control
SENSE-C-RPF #
PM. 813 Others

Technical Exposures - DBT-WRST
Data diddling
Bomb
Trojan Horse
Worms -
Rounding down
Salami
Trap Doors

Asynchronous Attacks - WL-STP
Wire Tapping
Leakage of data
Shutting down PC
Threats Subversive
Piggy backing.

Computer Crime Exposures FL-DISCS-BC
Financial Loss
Legal Impact
Disclosure of Info.
Industrial Espionage
Spoofing
Credibility loss.
Sabotage
Blackmail
Competitive edge lost

Ch 3 Pg 5

# Audit functions -

## Managerial
T-IS-PD-S-SO

Top Management
Info Sys Mngt
Sys Development Mngt
Programming Mngt
Data Admin -
Quality Assurance Mng
Security Administration
Operations Mngt

## Application
BI-C-POD

Boundary
Input
Communication
Processing
Output
Database

→ Ref Ch 3 Pg 6.

## Top Mngt & IS controls -

Functions of Senior Manager
POLC

Planning
- Prepare Plan
  - Types
    - Strategic
    - Operational
  - Steering committee

Organising
- Resourcing
- Staffing

Leading
- Motivate
- Communicate

Control
- IS Activities
- IS Services
- Overall

## Sys Dvp

Mngt Controls (Activities)
Sys Authorization
User Specification
Technical Design
Program Test
User Test
Acceptance
Internal Auditor

### Programming Mngt Controls -
Phases PDC-C-TOM

Planning -
Design
Control
Coding -
Testing
Operation
Maintenance

- Testing
  - Unit
  - Integration
  - Whole Program
- Maintenance
  - Repair
  - Adaptive
  - Perfective

## Data Resource Control Activities

CS-DEAU-C

Quality Controls -
Definition
Existence / Backup
Access controls
Update control
Concurrency control

## Quality Assurance

↓ Reasons

↓ WEDS-LAC

Worldwide trend
Expectations
Demand of users
Safety Critical Sys.
Liabilities.
Ambitious Projects.
Costs of low quality

## Operations Mngt Controls — Function — CC DD PP ON FH

Computer Operations — Controls
- Operation
- Scheduling
- Maintenance

Capacity Planning
Data Preparation & Entry
Documentation
Production Control
Performance Monitoring
Outsourced Operations
Network operations
File Library
Help Desk

## Security Mngt Controls

Threats — VESP-HIM-FW

Virus
Energy Variation
Structure damage
Pollution
Hackers
Intrusions
Misuse
Fire
Water

Controls Last resort
- DRP
- Insurance

Start

Audit functions -

Application Controls

BI - C - POD

Data Processing Controls -
Field Initialization
Exception reports -
Verification of reasonableness
Edit Checks -
Run-to-Run totals
Reasonableness Verification

Ch. 3 Page 6

- Standing data
- Run-to-Run totals
- Susp. alt entries
- Existence Controls

Report

Sequence Check
- All files processed
- Suspense a/c
- Multiple run

Update

**Boundary**
Biometrics
IDs
Cryptography
Passwords -
PINs

**Input** - SB-CV

**Communication** PC-LIFT-E

1. Physical component controls
   - P 1) Transmission Media
   - C 2) Communication Line
   - 3) Modem
   - F 4) Port Protection devices
   - T 5) Multiplexers & Concentrators
   - E
2. Line Error Controls
   - 1) Error detect
   - 2) Error correct
3. Flow control
4. Link Control
5. Topology Controls LAN/WAN
6. Channel Access control Methods
   - Polling
   - Contention
7. Inter networking Bridge

**Processing Controls** -
1. Processor Controls
2. Real Memory Controls
3. Virtual Mem. control
4. Data Processing Controls (#)

**Output Controls**
1. Storage & Logging of sensitive forms
2. Logging output programs
3. Spooling
4. Controls over printing
5. Retention control
6. Report distribution & collection

**Database Controls**

Source Doc Controls
1) Numbered docs -
2) Use Sequentially
3) Audit Periodically

Batch Controls -
1) Physical batch
2) Logical Batch.

Coding Controls -
↓
Error types which can corrupt data
- Transcription
  - Addition
  - Truncation
  - Substitution
- Transposition
  - Single
  - Multiple

Validation Controls -
- Record Interrogation [Ran Vcu Sign]
- Field Interrogation [LIAP-CD]
- File Interrogation
  1) Version Usage
  2) Internal & External Label
  3) Data file security
  4) Before & After Image & log
  5) File update & Maintenance
  6) Parity Check.

Reasonableness check
Valid Sign
Sequence Check
Cross Check
Limit Check
Arithmatic Check
Picture Check
Code Check
Digit Check

# Ch. 3 Pg. 7.

Classification of IS Controls -

ON-FAG-PD

Controls over Data Integrity & Security -

Classification of data : Grades -
1) Top secret
2) Highly Confidential
3) Proprietary
4) Internal use
5) Public Dos

Data Integrity Policies
V-DOSE-B
Virus signature Update
Disaster Recovery
Offsite backups.
Software Test
Environment division -
Backups - Quarterly/year ends

Data Integrity Controls categories
1) Source data Controls.
2) Input validation Routines
3) Online data entry Controls
4) Data processing & storage controls.
5) Output Controls
6) Data transmission controls -

Cyber Frauds -

Types
Pure Cyber Frauds -
Cyber Enabled.

Major Cyber Attacks
SON-PMM
Spam
Others → C-FEST
Network scan
Phishing -
Malicious Code
Malware propogation

Cracking
Forgery Email
Eaves dropping
Scavenging
Threats

Impact of Cyber frauds CC-DLFS
Competitive edge
Credibility
Disclosure of Info
Legal Impact
Financial loss -
Sabotage

(DP's)²
DDPPSS · TT BIRDZ HC

Techniques of committing Cyber Frauds.
Data Diddling
Data Leakage
Password Cracking
Piggy backing
Social Engineering
Scavenging.
Terrorism Internet
Trap Door
Bombs
Impersonation
Round down.
Denial of Service
Zapping.
Hacking
Cracking