SP = Security Policy

CHP 3

(1)

CHP - 03
Protection of Info^{n} System

SECURITY

(1) → Degree of protection applied

(2) → Security objective (CIA)

(4) → Info^{n} System is Sensitive
- → Strategic plan
- → Biz. Operation
- → finance

→ Information Security policy
- Tools
  - standards
  - Guidlines
  - procedure
- Issue to be address
- Members
  - → Mgt
  - → Technical
  - → Legal
- Components of security policy
- TYPES
  - User SP
    - User SP
    - Acceptable SP
  - Orgn SP
    - orgn Info^{n} SP
    - Network & Syst SP
    - Info^{n} classification SP
  - Cond^{n} of Connection

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) Indpendent check on performance
(8) Comparing Records Accountability with Assets
(9) Delegation of Authority & Responsibility

Classification of IS Controls

Basis
- Obj. of Control
  - Preventive
    - Threat
    - Vulnerabilities
    - Provision of necessary control
  - Corrective
  - Detective
  - Compensatory
- Nature of IS Resources → (1), (2) ← Audit functions

HARSHA

CHP 3

(1)

- Nature of Info^n System Resources

(A)

Environmental Control

- Issue & Exposures
- Categorization of Resources
  - H/w & Media
  - facilities
  - Documentation
  - Supplies
  - People
- Controls for Environment exposures
  - Fire Damage
  - Power Spike
  - water Damage
  - pollution Damage & others

(B)

Physical Access control

- Lock on Doors
  - Cipher lock
  - Bolting lock
  - Electronic lock
- Physical Identification Medium
  - PIN
  - Plastic Cards
  - Identification Badges
- Logging on facilities
  - Mannual
  - Electronic
- Other Means of controlling physical access

(C) Logical Access (LA) Control

- Exposures (Exp.)
  - Technical Exp. (Data didling, Bomb, Trojan Horse .....)
  - Computer crime Exp. (Financial loss, Sabotage, spoofing etc ----)
  - Asynchronous Attacks (Data leakage wire tapping Piggy backing...)
- LA Path
  - Online
    - Terminals
    - Dial up ports
    - Tele comm^n Network

HARSHA

ON The Basis of Audit function

(A) Managerial Controls

(1) Top Mgt

- Planning
  - Preparation
  - Type of plan
  - Role of steering committee
- Organizing
  - Resourcing IS function
  - Staffing IS function
- Leading
  - Motivating & leading IS personnel
  - communicating with IS personnel
- Controlling
  - Overall control of IS function
  - Control of IS Activities
  - Control over IS services

(2) System Development Mgt. Cont

- System Authorization Activities
- User Specification
- Technical Design
- Internal Auditor participation
- Program Testing
- User Test & Acceptance procedures

(3) Quality Assurance Mgt control

Reason for emergence of Quality Assurance

(4) Programming Mgt Control

- Planning
- Control
- Design
- Coding
- Testing
- operation & Maintenance

(5) Data Resource Mgt. Cont.

Controls
- Definition
- Access
- Update
- Concurrency
- Quality
- Existence

(6) operation Mgt Cont.

- Computer operation
- Network operation
- Datapreparation & Entry
- production control
- file liabrary
- Help Desk
- Capacity Planning

Security Mgt control (7)

HARSHA

(B) APPLICATION Control

- Boundary Control
  - Techniques [CBI, Personal password]
- Input control
  - Source Docum
  - Data Coding
  - Batch
  - Validation
- Communication Control
- Processing Control
  - Data Processing Controls
    - Run to Run Totals
    - Reasonableness Verification
    - Edit check
    - Field initializatn
    - Exeption Report
  - Access Control Mechanism
- Database Control
  - Major Report Controls
    - Standing Data
    - Print Run to Run Control
    - Print sequence A/c entries
    - Existence Control
  - Update Controls
    - Sequence Check
    - All records & file processed
    - Process Mutiple Transaction
    - Maintain suspense A/c
- Output Control (N.17)
  - Storage & logging of sensitive Critical forms
  - Logging of output program Execution
  - Spooling
  - Control over printing
  - Report Distribtn & collectn control
  - Retention Control

Classification of Infornn

1. Top Secret
2. Highly Confidential
3. Proprietary
4. Internal use only
5. Public Document

Financial Controls

[Input ABCD in safe Document]

Personel computer Controls

Risk

- Small in size
- Conveniently Transported
- Single user oriented
- No segregation Duty
- Weak access control

Measures

- 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
- DoS etc.

HARSHA

CHP 4

CHP – 4 Biz. Continuity Planning & Disaster Recovery

- BCP Manual + Advantages
- BCM Policy
  - objective
- Biz. Continuity Planning (N17)
  - objective & Goals
  - Area cover [BRP/DRP/CM]
- Developing BCP
  - Methodology
  - 8 Phases
    - (1) Preplanning activities
    - (2) Vulnerability Assessment & Genral Definition of Requirmnt
      - Key task (N17)
        - (1) Thorough Security Assessment
        - (2) Improve Existing emergency plan
        - (3) Present finding & recommendation
        - (4) Define scope
        - (5) Analyse, Recommend & purchase
        - (6) Develop Plan framework
        - (7) Assemble project team
    - (3) Biz. Impact Assessment
    - (4) Detailed Defin. of Requirmnt
    - (5) plan Development
    - (6) Testing program
    - (7) Maintenance Program
    - (8) Initial Plan Testing & Implementation
- Component of BCM Process (next Pg)
- Types of Plan
  - Emergency plan
  - Backup plan
  - Recovery plan
  - Test plan
- Types of Back ups
  - Full Backup
  - Incremental Backup
  - Differencial Backup
  - Mirror Backup
- Alternate Processing facility Arrangement
  - Cold Site
  - Hote site
  - Warm Site
  - Reciprocal Arrangement

(Nov17) # Issue to be cover in Third Party site Backup Recovery

HARSHA

Components of BCM Process

(A) Biz. Contⁿ Mgt process
- Major activities to be Carried
- Major Docᵐ of BCM system

(B) Biz. Infoⁿ Collection process
- BIA
- Risk Assessment

(C) BCM strategy Process

(D) BCM Development & Implementation process

(E) BCM Testing & Maint. Process
- BCM Testing
- BCM Maintenance
  - Maintenance Task in Development of BCP
    - (1) Determine ownership & responsibility
    - (2) Identify BCP maintenance triggers
    - (3) Maintenance regime to ensure plan remain uptodate
    - (4) Maintenance process to update the plan
    - (5) Implement version control procedure
  - Audit/self assessment of BCM program
    - (1) Identify & Include key product & services
    - (2) priorities & requirement
    - (3) BCM competence & capability
    - (4) BCM solutions
    - (5) Exercising program & effective implemented
    - (6) Incorporate improvement
    - (7) Ongoing program for training & awareness
    - (8) Effective Commⁿ of prod procedure

(F) BCM Training Process
- Competencies Required by the orgⁿ

Contents of Disaster Recovery Planning Document

(1) Condⁿ for activating plan
(2) Emergency procedure
(3) Fallback Procedure
(4) Resumption procedure
(5) Maintenance schedule
(6) Awareness & education activities
(7) Responsibilities of Individuals

Audit of BCP & DRP

(Read from Book / PM)

HARSHA