Hi Everyone,

Following is the master summary of all chapters except 10th of ISCA. It strictly follow module and all points are arranged according to it except some topics where I had tried to do some better work.

I would like suggest following a given methodology to extract best out of it. This is my personal experience and I just wanted to share. Everyone is different and have a different approach to studies.

1. **First of all refer your main study course, preferably module, and go through it completely chapter by chapter.**
2. **After completing each chapter refer this summary and try to recall what you know till now on the topic and how much you can write if it appears in exam.**
3. **Then learn this summary for the time being. You will not remember ISCA for very long so don't panic, something is better than nothing.**
4. **Finally after AMA paper and just look at this summary giving only 2-3 hours.**
5. **Refer module for complete day and then learn this summary on exam day.**

Things do looks easy when said until not done.

IS Concepts

1. System
2. Types of system
    a. Deterministic-Probabilistic
    b. Open-Closed
    c. Manual-Automated
    d. Abstract-Physical
3. System related concepts
    a. Boundary
    b. Environment
    c. Sub-system
    d. Decomposition
    e. Interface
    f. Simplification
    g. Decoupling
    h. Stress
    i. Supra system
    j. Entropy/Maintenance
4. Information
5. Information related concepts
    a. Characteristics of good information
        i. Timeliness
        ii. Purpose
        iii. Mode & format
        iv. Redundancy
        v. Accurate
        vi. Completeness
        vii. Reliability
        viii. Quality
        ix. Value of information
        x. Adequacy
        xi. Rate & frequency
    b. Role in business
        i. Effective DM
        ii. Competitive edge
        iii. Right decision at right time
        iv. Solve critical problems
        v. Information gathered uses in unusual situations
    c. Factors upon which information requirements of executive depends
        i. Operational
        ii. Type of decision making
        iii. Level of management
    d. Types of information (Internal - External)
6. CBIS

a. Components
    i. Hardware
    ii. Software
    iii. Data
    iv. Procedures
    v. People
b. Characteristics
    i. Work towards pre-determined objectives
    ii. Interconnected subsystem & components
    iii. Different subsystem interacts each other
c. Areas of application
    i. Marketing & sales
    ii. Production & manufacturing
    iii. Inventory management
    iv. HRM

7. TPS
    a. Components
        i. Input (Classification & Recording)
        ii. Processing
        iii. Storage (Master/Transaction)
        iv. Output (Financial/Operational)
    b. Features
        i. Large volume of data
        ii. Automation of basic operation
        iii. Benefits are easily measurable
        iv. Source of input for other system
8. MIS
    a. Concept of MIS
    b. Characteristics
        i. Management oriented
        ii. Management directed
        iii. Need based
        iv. Exception based
        v. Integrated
        vi. Common data flows
        vii. Common data base
        viii. Long term planning
        ix. Modularity
        x. Computerized
    c. Misconception
        i. Computerized only
        ii. More data more information
        iii. Accuracy is primary
    d. Pre-Requisites
        i. Database

ii. Qualified staff
iii. Support of top management
iv. Control & maintenance
v. Evaluation of MIS

e. Constraints
i. Non Availability of experts
ii. High turnover of expert
iii. Problem of selecting sub system
iv. Lack of co-operation
v. Difficulty in quantifying benefits

f. Effect of using CB-MIS
i. Fast & timely data processing
ii. More comprehensive information
iii. Better integration
iv. Increase effectiveness
v. Increase scope of analysis
vi. Increase complexity of operation

g. Limitation
i. Quality of output depends on input
ii. Constrained by limitations of TPS
iii. Based on internal data only
iv. No ad-hoc reports on external data
v. Lacks tight integration
vi. Cannot substitute effective mgt
vii. Less useful for structured decision
viii. Does not account non-quantitative factors

9. ERP
a. Objectives
i. Adoption of best business practices
ii. Implement BBP to enhance productivity
iii. Customer & suppliers as integral part

b. Limitations
i. Data quality issues
ii. Only past & current status

10. DSS
a. Characteristics
i. Semi-structured & Unstructured problems
ii. Both internal & external databases
iii. Flexible to respond changing needs
iv. What-if analysis feature
v. Utilizes models for problem solutions
vi. Easy to use
vii. Help end user to construct & modify

b. Components
i. User

1. Managers
2. Staff specialist/analyst

ii. User interface/Planning language
1. General purpose
2. Special purpose

iii. Model base

iv. Other databases (Internal-External)
1. Implementation of databases
a. Physical level
b. Logical level
c. External level

c. Uses
i. Capital budgeting
ii. Cost accounting
iii. Budget variance
iv. General accounting
v. Security analysis & portfolio management

11. EIS
a. Characteristics
i. Top executives
ii. Extract summary data and model complex problems
iii. Very user friendly
iv. Rapid access to timely information
v. Internal & external data both
vi. Easily connected to internet
vii. Extensive online analysis tool
viii. DSS support

b. Executive roles and DM
i. Strategic planning
ii. Tactical planning
iii. Fire –fighting

c. Characteristics of information used
i. Lack of structure
ii. Future orientation
iii. Low level of details
iv. Information from informal sources
v. Lack of certainty

d. Content
i. Meet organization objectives
ii. Generate its content automatically
iii. Performance indicators
iv. Adaptable
v. Available to everyone
vi. Encourage the organization's objectives

12. Expert system

a. Component
    i. User interface
    ii. Inference engine
        1. Backward chaining
        2. Forward chaining
    iii. Explanation facility
    iv. Knowledge base
    v. Knowledge acquisition facility
b. Business application
    i. Accounting & finance
    ii. Marketing
    iii. Manufacturing
    iv. Personnel
    v. General business
c. Need for expert system
    i. Expert labour is expensive & scarce
    ii. Experts cannot handle all factors at a time
d. Benefits
    i. Preserve knowledge
    ii. Information in active form
    iii. Assist novice think as expert
    iv. Not subject to human feelings
    v. Effectively used as business tool
e. Characteristics
    i. Availability
    ii. Complexity
    iii. Domain/Subject area
    iv. Expertise
    v. Structure
f. Business application
    i. Accounting & finance
    ii. Marketing
    iii. Manufacturing
    iv. Personnel
    v. General business

13. OAS – Activities
    a. Document capture
    b. Document creation
    c. Receipts and distribution
    d. Filling, search, retrieval and follow-up
    e. Calculations
    f. Recording utilization of resources
14. OAS – Benefits
    a. Improve communication
    b. Reduce cycle time

c. Reduce cost of office communication
d. Ensure accuracy

15. OAS – types
    a. Text processors
        i. Most commonly used
        ii. Automate document creation
        iii. Quick production of multiple documents
        iv. Supported with printers
    b. EDMS
        i. Capture, store and communicate
        ii. Linked with text processor & E-mail
        iii. Remote access of document
        iv. Location become irrelevant
    c. EMCS
        i. E-mail
            1. Electronic transmission
            2. Online development & editing
            3. Reply & multiple forward
            4. Integration with other OAS
            5. Portability
            6. Economical
        ii. Facsimile
            1. Uses special software and fax servers
            2. To send & receive fax message
            3. Using communication resources
            4. Server automatically re-route
        iii. Voice mail
            1. Variation of email
            2. Transmit as digitized voice
            3. Dial a voice mail box service
            4. Receiver hear spoken voice
    d. Teleconferencing
        i. Conduct business meeting
        ii. Reducing time and cost
        iii. Audio or video
        iv. Flexibility
        v. Use digital camera, visual communication software, lines, etc
        vi. Quite expensive

SDLC methodology

1. Introduction
2. System development process
3. Why SD objectives fail
    a. Lack of senior management support

b. Shifting user needs
c. Development of strategic system
d. New technologies
e. Lack of standard SD methodologies
f. Resistance to change
g. Lack of user participation
h. Inadequate testing & user training

4. SD approaches
    a. Waterfall
        i. Divided into sequential phases
        ii. Emphasis on planning, time schedules, etc at one time
        iii. Tight control by excessive documentation
    b. Prototyping
        i. Identify IS requirement
        ii. Develop initial plan
        iii. Test & revise
        iv. Obtain user approval
    c. Incremental
    d. Spiral
        i. Define system requirement
        ii. Planning & designing system to identify all risks & alternatives (use prototyping to select)
        iii. Develop prototype
        iv. Evaluate first prototype & repeat above
    e. RAD
        i. Fast development
        ii. High quality
        iii. Active user involvement
        iv. Iterative prototyping
        v. Computerized development tools
        vi. Emphasis on fulfilling business needs
        vii. Defining delivery deadlines
        viii. Includes JAD
    f. Agile
5. SDLC
    a. Advantages
        i. Better planning
        ii. Compliance to prescribed standards
        iii. Documentation
        iv. Phases as milestones
    b. ISA perspective
        i. Clear understanding
        ii. State compliance in his report
        iii. Guide if having technical knowledge
        iv. Provide evaluation of methods & techniques

   c. Risks
      i. Cumbersome
      ii. End product not visible
      iii. Rigidity approach
      iv. Not suitable for small & medium projects
6. Preliminary investigation
   a. Identification of problem
   b. Identification of objective
   c. Delineation of scope
      i. Functional requirements
      ii. Control requirements
      iii. Performance requirements
      iv. Reliability requirements
      v. Constraints
      vi. Interfaces
      vii. Data to be processed
   d. Feasibility study
      i. Technical
      ii. Economical
      iii. Behavioral
      iv. Financial
      v. Time
      vi. Resource
      vii. Operational
      viii. Legal
   e. Reporting results
7. System requirement analysis
   a. Fact finding techniques
      i. Documents
      ii. Questionnaires
      iii. Interviews
      iv. Observation
   b. Analysis of present system
      i. Review historical aspects
      ii. Analyze inputs
      iii. Review data files maintained
      iv. Review methods, procedures & data communications
      v. Analyze outputs
      vi. Review internal controls
      vii. Model existing physical system & logical system
      viii. Undertake overall analysis of present system
   c. Analysis of proposed system
      i. Emphasis on output
      ii. Database maintenance
      iii. Input from original source

iv. Methods, procedures & data communications
v. Work volumes & timings

d. SRS
i. Information
ii. Information description
iii. Functional description
iv. Behavioral description
v. Validation criteria
vi. Appendix
vii. SRS review

8. System development tools
a. Categories
i. System components & flow (SFC, DFD, SCM)
ii. User interface (LFS, DFD)
iii. Data attributes & relationship (DD, ERD, FLF, GC)
iv. Detailed system process (DT, DT, SC)
b. Tools
i. Pseudo code
ii. Flowcharts
1. Types
2. Benefits
3. Limitations
iii. Data flow diagrams
iv. Decision tree
v. Decision table
vi. CASE tools
vii. System component matrix
viii. Data dictionary
ix. Layout form & screen generator

9. Roles involved in SDLC
a. Steering committee
b. Project manager
c. Project leader
d. System analyst
e. Module/team leader
f. Programmer/Coder/Developer
g. DBA
h. Quality assurance
i. Tester
j. Domain specialist
k. ISA

10. System design
a. Architectural design
b. Design of data/information flow
c. Design of database

d. Design of user interface (Input/output)
    i. Factors
        1. Content
        2. Timeliness
        3. Format
        4. Media
        5. Form
        6. Volume
e. Physical design
f. Design of hardware/software platform

11. System acquisition
    a. Acquisition standards
    b. Acquiring systems components
        i. Hardware acquisition
        ii. Software acquisition
        iii. Contracts, software licenses & copyright violations
        iv. Validation of vendors' proposals
            1. Checklist
            2. Point-scoring analysis
            3. Public evaluation reports
            4. Bench marking problem
            5. Test problems
12. Program development
    a. Characteristics
        i. Reliability
        ii. Robustness
        iii. Accuracy
        iv. Efficiency
        v. Usability
        vi. Readability
    b. Program coding standards
    c. Programming language
    d. Program debugging
    e. Test the program
    f. Program documentation
    g. Program maintenance
13. System testing
    a. Unit testing
        i. Categories
            1. Functional tests
            2. Performance tests
            3. Stress tests
            4. Structural tests
            5. Parallel tests
        ii. Types

1. Static analysis testing
    a. Desk check
    b. Structures walk through
    c. Code inspection
2. Dynamic analysis testing
    a. Black box
    b. White box
    c. Gray box

b. Integration testing
    i. Bottom up
    ii. Top down
    iii. Regression
c. System testing
    i. Recovery
    ii. Security
    iii. Stress or volume
    iv. Performance
d. Final acceptance testing
    i. Quality assurance
    ii. User acceptance
        1. Alpha
        2. Beta

14. System implementation
    a. Equipment installation
        i. Site preparation
        ii. Installation of new hardware/software
        iii. Equipment check point
    b. Training personnel
    c. Conversion strategies
        i. Direct
        ii. Phased
        iii. Pilot
        iv. Parallel
    d. Conversion activities
        i. Procedure
        ii. File
        iii. System
        iv. Scheduling personnel & equipment
15. Post implementation review
    a. Development evaluation
    b. Operation evaluation
    c. Information evaluation
16. System maintenance
    a. Scheduled
    b. Rescue

c. Corrective
d. Adaptive
e. Perfective
f. Preventive

17. Operation manuals
18. Organizational structure of IT department
    a. Line management
    b. Project management

Control Objective

19. Introduction
20. Need for controls
    a. Cost of data loss
    b. Incorrect DM
    c. Cost of computer abuse
    d. Cost of hardware, software & personnel
    e. Cost of error
    f. Maintenance of privacy
    g. ISA
    h. Data integrity objectives
    i. System effectiveness& efficiency
21. Effect of computers on ICS
    a. Personnel
    b. Segregation of duties
    c. Record keeping
    d. Authorization
    e. Concentration of programs & data
    f. Access to assets & data
    g. Management supervision & review
    h. Components of IC
        i. Control environment
        ii. Risk assessment
        iii. Control activities
        iv. Information & communication
        v. Monitoring
22. Effect of computer on audit
    a. Changes to evidence collection
        i. Data retention & storage
        ii. Absence of input documents
        iii. Lack of visible audit trial
        iv. Lack of visible output
        v. Audit evidence
        vi. Legal issues
    b. Changes to evidence evaluation

i. System generated transactions
ii. Systematic errors

23. Responsibility of controls
    a. Develop & implement cost – effective controls
    b. Assess adequacy
    c. Separately assess & document IC consistent with ISP
    d. Identify needed improvements
    e. Take corrective actions
    f. Report annually
24. ISA process
    a. Responsibility of IS auditor
        i. Sound knowledge of business operations
        ii. Knowledge of standards & best practices
        iii. Requisite technical qualification
        iv. Knowledge of IT strategies, policies
        v. Understanding of risk & controls
        vi. Understand technical controls
    b. Functions – Check whether
        i. Security is inadequate
        ii. Adequate IT related policies
        iii. IT related frauds
        iv. Resources efficiently utilized
        v. Controlled SDMP
    c. Categories of ISA
        i. System & applications
        ii. IPF
        iii. System development
        iv. IT management structure
        v. Telecommunications, intranets, extranets
    d. Steps
        i. Scoping/Pre – Audit survey
        ii. Planning
        iii. Fieldwork
        iv. Analysis
        v. Reporting
        vi. Closure
    e. Standards
    f. Cost effectiveness of control procedures
        i. Initial cost
        ii. Execution
        iii. Failure
        iv. Correction
        v. Maintenance
25. Information system control techniques
    a. Objectives of control

b. Based on objective
    i. Preventive
        1. Understanding vulnerabilities
        2. Understanding probable threats
        3. Provision of necessary controls
    ii. Detective
        1. Understanding of lawful activities
        2. Established mechanism to report unlawful act
        3. Interaction with preventive control
        4. Surprise checks
    iii. Corrective
        1. Minimize impact
        2. Identify cause and correct problems discovered
        3. Get feedback
        4. Modify processing system to minimize future occurrences
    iv. Compensatory
c. Based on functions/Component of IC
    i. Accounting
    ii. Operational
    iii. Administrative
d. Based on nature
e. Control techniques
    i. Organisational controls
        1. Responsibilities & objectives
        2. Policies, standards, practices
        3. Job description
        4. Segregation of duties
    ii. Management controls
        1. Responsibility
        2. Official IT structure
        3. IT steering committee
    iii. Financial controls
        1. Authorization
        2. Budgets
        3. Cancellation of documents
        4. Documentation
        5. Dual control
        6. Safekeeping
        7. Segregation of duties
        8. Sequentially numbered documents
        9. Supervisory review
        10. I/O verification
    iv. Data processing
    v. Physical access
    vi. Logical access

vii. SDLC
viii. BCP
ix. Application control
x. Audit trials
xi. Audit trial objectives
    1. Detecting unauthorized access
    2. Reconstructing events
    3. Personnel accountability

26. User controls
    a. Boundary
        i. Cryptography
        ii. Password
        iii. PIN
        iv. Identification cards
    b. Input
        i. Errors
            1. Addition
            2. Truncation
            3. Transcription
            4. Transposition
            5. Double Transposition
        ii. Factors affecting input errors
            1. Length
            2. Alphanumeric mix
            3. Special character
            4. Mixing uppercase/lowercase
            5. Sequence of characters
    c. Processing
        i. Run – to – run totals
        ii. Reasonableness verification
        iii. Edit checks
        iv. Field initialization
        v. Exception reporting
        vi. Existence/recovery controls
    d. Output
        i. Storage & logging of sensitive/critical forms
        ii. Logging of output program execution
        iii. Spooling
        iv. Controls over printing
        v. Report distribution & collection controls
        vi. Retention controls
        vii. Existence/recovery controls
    e. Database
        i. Update controls
            1. Sequence check in transaction & mater files

2. Ensure all records are processed
3. Process multiple transaction from single record in correct order
4. Maintain suspense account

ii. Report controls

1. Standing data
2. Print run – to – run totals
3. Print suspense account
4. Existence/recovery controls

27. SD & acquisition controls
    a. Problem definition
        i. Need for IS in business
        ii. Support & priority by management
        iii. Level of acceptance by stakeholders
        iv. Investigation & strategy
    b. Change management process
        i. Prepare & promote for unrestricted change
        ii. Complete changeover
        iii. Help user to adapt new system
        iv. Review periodically for potential conflicts
    c. Entry & feasibility assessment
        i. Technical
        ii. Operational
        iii. Economical
        iv. Behavioral
    d. Existing system analysis
        i. Study of history of systems
        ii. Using formal methodology
    e. System design (formulation of strategic requirements)
        i. Align business requirement with objectives and goals
    f. Organizational & job design
        i. Defined roles & responsibilities
        ii. Clear design of organisation structure
    g. IS processing design
        i. Requirement elicitation
        ii. User interface design
        iii. Dataflow design
        iv. Database design
        v. Platform design
        vi. Physical design
    h. Application software acquisition
        i. IS requirement needs to meet business goals
        ii. Feasibility analysis to define constraints
        iii. Detailed RFP specifying acceptable requirements
        iv. Vendor evaluation process
28. Control over system & program changes

a. Change management process
b. System change controls
c. Program change controls
d. Authorization controls
e. Document controls
f. Testing & quality controls

29. Quality controls
    a. Quality standards
    b. Quality reviews
    c. Copyright violations
    d. Contract/Warranties
    e. SLA
30. Controls over system implementation
    a. Procedures development
    b. Conversion
        i. Direct
        ii. Parallel
        iii. Phased
        iv. Pilot
    c. User final acceptance testing
        i. Performance
        ii. Volume
        iii. Stress
        iv. Security
        v. Clerical procedures checking
        vi. Back-up and recovery
    d. User training
31. System maintenance
    a. Maintenance
        i. Corrective
        ii. Adaptive
        iii. Perfective
    b. Performance measurement
32. Post implementation review
    a. Achievement of objectives
        i. Business
        ii. User expectation
        iii. Technical requirements
    b. Balance between period of PIR
    c. PIR team
    d. Activities to be undertaken
33. Control over data integrity, privacy, security
    a. Information classification
        i. Top secret
        ii. Highly confidential

iii. Propriety
iv. Internal use only
v. Public documents

b. Data integrity
   i. Source data control
   ii. Input validation routines
   iii. On-line data entry controls
   iv. Data processing and storage controls
   v. Output controls
   vi. Data transmission controls

c. Data integrity policies
   i. Virus signature updating
   ii. Software testing
   iii. Division of environments
   iv. Version zero software
   v. Offsite backup
   vi. Quarter or Year end backup
   vii. Disaster recovery

34. Logical access controls
   a. Logical access paths
      i. Online terminals
      ii. Batch job processing
      iii. Dial-up ports
      iv. Telecommunication network
   b. Logical access exposure
      i. Technical
         1. Data diddling
         2. Logic bomb
         3. Time bomb
         4. Trojan horse
         5. Worms
         6. Rounding down
         7. Salami techniques
         8. Trap doors
      ii. Computer crime
         1. Financial loss
         2. Legal repercussions
         3. Loss of credibility
         4. Blackmail
         5. Disclosure of confidential information
         6. Sabotage
         7. Spoofing
      iii. Asynchronous attacks
         1. Data leakage
         2. Wire – tapping

3. Piggybacking
4. Denial of service

iv. Remote and distributed data processing controls
1. Remote access through network should be implemented
2. Having terminal lock
3. Applications to be controlled and remotely accessed via modem
4. Monitored carefully
5. Proper control over documentation and manuals
6. Data transmission to be controlled, verify accuracy, genuineness and integrity
7. Replicated copies contain same information, no duplication

v. Physical and environmental protection

c. Logical access controls (also in chapter 8 under ISMS)
i. User access management
1. User registration
2. Privilege management
3. User password management
4. Review of user access rights

ii. User responsibility
1. Password use
2. Unattended user equipment

iii. Network access control
1. Policy on use network services
2. Enforced path
3. Segregation of networks
4. Network connection and routing control
5. Security of network services

iv. Operating system access control
1. Automated terminal identification
2. User identification and authentication
3. Password management system
4. Use of system utilities
5. Alarms system
6. Terminal time out
7. Limitation of connection time

v. Application and monitoring system access control
1. Information access restriction
2. Sensitive information isolation
3. Event logging
4. Monitor system use
5. Clock synchronization

vi. Mobile computing

d. Role of IS auditor
i. Review the relevant documents and RAE techniques
ii. Evaluate potential access paths

iii. Identify deficiencies and redundancies
iv. Verify test control over access paths
v. Analyze test results and verify that objective are achieved
vi. Compare security policy

35. Physical access controls
    a. Issues and exposure
    b. Access control mechanism
        i. Identification
        ii. Authentication
        iii. Authorization
    c. Physical access control
        i. Locks on doors
            1. Cipher lock
            2. Bolting door lock
            3. Electronic door lock - Card entry
            4. Biometric door lock
        ii. Physical identification mechanism
            1. PIN
            2. Plastic cards
            3. Cryptographic controls
            4. Identification badges
        iii. Logging on utilities
            1. Manual logging
            2. Electronic logging
        iv. Others
            1. Video camera
            2. Security guards
            3. Controlled visitor access
            4. Dead man doors
            5. Controlled single point entry
            6. Alarm system
            7. Perimeter fencing
            8. Control on employees Out-of-office during office hours
        v. Accounting and audit trial
    d. Audit and evaluation technique
    e. Role of IS auditor
        i. Risk assessment
        ii. Control assessment
        iii. Planning for review of PA controls
        iv. Testing
            1. Tour of facilities
            2. Physical inventory
            3. Interview personnel
            4. Observation of safeguards (including special consideration)
            5. Review of PA procedures

6. Examination of physical logs

36. Environmental controls
    a. Categorization
        i. Hardware and media
        ii. IS supporting infrastructure
        iii. Documentation
        iv. Supplies
        v. People
    b. Issues and exposures
    c. Controls
        i. Water detectors
        ii. Fire extinguishers
        iii. Manual fire alarms
        iv. Smoke detectors
        v. Fire suppression system (dry, water, halon)
        vi. Strategic location of computer room
        vii. Regular inspection by fire department
        viii. Fireproof walls, floors, ceilings
        ix. Electric surge protectors
        x. UPS
        xi. Power lead from two stations
        xii. Emergency power-off switch
        xiii. Wiring placed in fire resistant panels
        xiv. Prohibitions on eatables
        xv. Fire resistant office material
        xvi. Documented and emergency evacuation plans
    d. Audit and evaluation technique
    e. Role of IS auditor
        i. Audit planning and assessment
            1. Risk profile should include kinds of risk exposure and periodic updating
            2. Controls assessment to ascertain adequacy
            3. Security policy review to assess policies and procedures
            4. Building and wiring plans needs to be reviewed
            5. Interview relevant personnel (awareness, role, incident handling)
            6. Administrative procedures like reporting and plans
        ii. Audit of technical controls
            1. IPF and its construction
            2. Activities in the IPF
            3. Presence of water and smoke detectors
            4. Location of fire extinguishers
            5. Evacuation plans and emergency exit markings
            6. Documents for compliances of various requirements
            7. Power sources and test to assure its quality
            8. Environmental control equipment like AC, heater, etc
            9. Complaint logs

37. Security concepts and techniques
    a. Cryptosystem
    b. DES
    c. PKI
    d. PKI policies
38. Data security and public networks
    a. Firewall
        i. Packet filter
        ii. Stateful inspection
        iii. Proxy server
        iv. Application – level
39. Unauthorized intrusion
    a. Why use IDS
    b. Types of IDS
        i. Network based
        ii. Host based
40. Hacking
    a. What damage is done
    b. How do they hack
        i. NetBIOS
        ii. ICMP ping
        iii. FTP
        iv. RPC statd
        v. HTTP
41. Controlling against virus
    a. What is virus
    b. Antivirus software
        i. Scanner
        ii. Active monitor and heuristic scanner
        iii. Integrity checkers
    c. Recommended policy and procedure controls
42. Data privacy
    a. Protecting data privacy in IS
        i. Policy communication
        ii. Policy enforcement
    b. Data privacy policies
        i. Copyright notice
        ii. E-mail monitoring
        iii. Customer information sharing
        iv. Encryption of data backups
        v. Data access

Testing – General & automated controls

1. Introduction

   a. Methods
      i. Substantive
      ii. Compliance
   b. Phases
2. Audit planning
   a. Use M/S concepts for effective plan
   b. Underlying principle is optimum utilization of resources
   c. Determine areas of little/no attention
   d. M/S include both qualitative & quantitative factors
   e. Occurs throughout audit as iterative process
3. Audit testing
   a. Devise testing plan & methodology
   b. Perform necessary testing
   c. Use of GAS for testing
4. ISCA process
   a. Obtain understanding of entity, its operations & key business processes
   b. Obtain understanding of structure on entity's networks
   c. Identifying key areas of audit interest
   d. Assessment of IT risk
   e. Identify critical control points
   f. Obtain understanding of ISC
   g. Performing other audit planning procedures
5. Factors to determine NTE of audit procedures
   a. Extent to which significant IC depend on reliability of information processed
   b. Availability of evidence from sources other than IS
   c. Relationship of ISC to data reliability
   d. Assessing effectiveness of ISC
6. Identify key areas of audit interest
7. Obtain preliminary understanding of IS
8. Performing ISCA test
   a. Types
      i. Test of design
      ii. Test of effectiveness
   b. Levels
      i. Entity wide level
      ii. System level
         1. Network
         2. OS
         3. Infrastructure
      iii. Business process application level
9. Testing critical control points
10. Test effectiveness of ISC
   a. Test on tiered basis
      i. Test of general controls at entity & system level
      ii. Test of general controls at BPAL

iii. Test of BPAC/UC

b. Evaluate & determine D/I/O
   i. Identify general controls
   ii. Determine how controls function and actually placed
   iii. Evaluate operating effectiveness

11. Appropriateness of controls
    a. Inquiry
    b. Questionnaire
    c. Inspection
    d. Observation
    e. Re-performance
    f. Review documents
    g. Analysis of system
    h. Data review & analysis of output
12. Multiyear testing plans
13. Documentation
    a. Understanding IS
    b. ISC objectives & activities
    c. Control techniques
    d. NTE of test
    e. Specific test performed
    f. Evidence of effective controls or lack thereof
    g. Conclusions about effectiveness
    h. If control objective not achieved, compensatory controls
    i. For each weakness, material/significant/deficiency
14. Reporting
    a. Basic
       i. Summarize results
       ii. Draws conclusion out of I+A effect of identified ISC weaknesses
       iii. Reports results
    b. Audit objectives
    c. Report audit result
    d. Substantive resting
    e. Documenting results
       i. Audit findings
    f. Analysis
       i. Reexamination
       ii. Standards
       iii. Facts
       iv. Verification
       v. Cause
       vi. Materiality & exposure
       vii. Recommendations
15. Continuous Audit & embedded modules
    a. Types

i. Snapshots
ii. ITF
    1. Methods of entering
        a. Tagged transaction
        b. Specially prepared test data
    2. Methods of removing
        a. Programmed to ignore apart from test purpose
        b. Reversal additional inputs
        c. Submit Trivial entries
iii. SCARF
    1. Application system errors
    2. Policy & procedural variances
    3. Profiling data
    4. Performance measurement
    5. System exception
    6. Snapshots & extended records
    7. Statistical sample
iv. CIS

b. Benefits
    i. Examine data faster & efficiently
    ii. Reduce time & cost
    iii. Near 100% testing possible
    iv. Testing throughout the year
    v. Increase quality of audits
c. Advantages
    i. Timely, comprehensive & detailed audit
    ii. Surprise test capability
    iii. Information to system staff on meeting objectives
    iv. Training new users
d. Disadvantages
    i. Must obtain required resource
    ii. Usable if auditors involved in development of system
    iii. Knowledge & experience of auditor
    iv. Usable where audit trial is less visible & cost of errors are high
    v. Stable application system required

16. Hardware testing
17. Review of hardware – Review
    a. Capacity management & performance evaluation
    b. Hardware acquisition plan
    c. Change in management controls
    d. Preventive maintenance
18. OS review
    a. Interview personnel
    b. Review cost-benefit analysis
    c. SS installation

d. SS change controls
e. SS implementation
f. SS security
g. System documentation
h. Authorization documentation
i. Database supported ISC

19. Reviewing network

Risk assessment methodologies and applications

20. Introduction
21. Risk concepts
    a. Risk
    b. Threat
    c. Vulnerability
    d. Exposure
    e. Likelihood
    f. Attack
    g. Residual risk
22. Threats to computerized environment
    a. Power failure
    b. Communication failure
    c. Technology failure
    d. Disgruntled employees
    e. Theft or destruction of asset
    f. Abuse of access privileges
    g. Fire
    h. Natural disaster
    i. Error
    j. Malicious code
23. Threats due to cyber crime
    a. Fraud
    b. Embezzlement
    c. Theft of propriety information
    d. Sabotage
    e. Virus
    f. Denial of service
24. Risk assessment
    a. Prioritization
    b. Identify critical applications
    c. Assess the impact on organization
    d. Determine recovery time frame
    e. Assess insurance coverage
        i. Hardware facilities
        ii. Software reconstruction

iii. Extra cost
iv. Business interruption
v. Valuable records and documents
vi. Media transportation
vii. Error and omission
viii. Fidelity coverage

f. Identification of exposures and implications
g. Develop a recovery plan

25. Risk management
    a. Types
        i. Systematic risk
        ii. Unsystematic risk
    b. Risk management process
        i. Identify technology related risk
        ii. Assess identified risk in terms of probability and exposure
        iii. Classify into systematic and unsystematic
        iv. Identify various managerial actions that can reduce systematic risk and cost of it
        v. Look out for technological solution to mitigate unsystematic risk
        vi. Identify the contribution of technology across the organization in reducing overall risk exposure
        vii. Evaluate technology risk premium and compare with possible value of loss
        viii. Match analysis with management policy
    c. Risk management cycle
        i. Risk identification
        ii. Risk assessment
        iii. Risk mitigation
26. Risk identification
    a. Purpose
        i. Identify probability
        ii. Calculate exposure
        iii. Make control recommendations
    b. Techniques
        i. Judgment and intuition
        ii. Delphi approach
        iii. Scoring technique
        iv. Quantitative
        v. Qualitative
27. Risk ranking
28. Risk mitigation
    a. Common techniques
        i. Insurance
        ii. Outsourcing
        iii. Service level agreements
29. Risk and controls

BCP/DRP

1. BCP
    a. Concept
    b. Areas/Components
        i. Business resumption planning
        ii. Disaster recovery planning
        iii. Crisis management
    c. Objectives
        i. Provide for the safety and well-being of people
        ii. Continue critical business operations
        iii. Minimize the duration of serious disruptions to operations and resources (G)
        iv. Minimize immediate damage and losses
        v. Establish management succession and emergency powers
        vi. Facilitate effective co-ordination of recovery tasks (G)
        vii. Reduce complexity of recovery effort (G)
        viii. Identify critical lines of business & support functions
        ix. Identify weakness and implement disaster prevention program (G)
2. Developing a BCP
    a. Methodology
        i. Provide comprehensive understanding of total efforts required
        ii. Obtain commitment to support
        iii. Define recovery requirements from business perspective
        iv. Document the impact of extended loss
        v. Focus on disaster prevention and impact minimization equally
        vi. Select BC teams
        vii. Develop understandable, easy to use and maintain BCP
        viii. Define BCP must be integrated to ongoing business planning & SD
    b. Phases
        i. Preplanning activities
            1. Understanding present & projected system
            2. Defining overall scope of BCP
            3. Develop policy to support BCP
            4. Establish steering committee
            5. Launch BCP awareness program
        ii. Vulnerability assessment
            1. Identify critical business processes
            2. Identify all threats and vulnerabilities
            3. Evaluate existing security measure and control
            4. Evaluate existing emergency plan
            5. Document findings
        iii. Business impact analysis
            1. Identify organisational risk
            2. Quantify risk to critical BP in terms of financial and goodwill loss
            3. Identify interdependencies of critical BP and time order to restore

4. Maximum allowable downtime
5. Identify type and quantity of resources required
6. Submit BIA report

iv. Detailed definition of requirement
1. Identify recovery alternatives for short, medium, and long term
2. Estimate and determine resources required for critical functions in terms of hardware, software, personnel, facilities, outside support
3. Develop scope, objectives and assumption of BCP

v. Plan development
1. Formulate overall recovery plan and strategy categorized in business and technical
2. Define & document recovery plan and components
3. Define changes to user procedures, data processing procedures
4. Define roles and duties of recovery teams
5. Determine changes made to vendor contracts

vi. Testing program
1. Recovery procedures are complete and workable
2. Staff is adequately trained
3. Resources (H/S/P/F) are adequate
4. Manual recovery and back-up procedures are also working

vii. Plan implementation
1. Implement individual components of plan
2. Assigning job roles and duties to staff
3. Providing emergency guidelines
4. Scheduling test activities

viii. Maintenance program
1. Determine responsibility to maintain BCP
2. Continuous monitoring to look for desired changes
3. Designing change management process

3. Types of plans
   a. Emergency plan
   b. Backup plan
      i. Hardware
      ii. Application software
      iii. System software
      iv. Documentation
      v. Data/Information
      vi. Personnel
      vii. Facilities
      viii. Supplies
   c. Recovery plan
   d. Test plan
4. Threats and risk management
   a. Lack of integrity
   b. Lack of confidentiality

c. Lack of system availability
d. Unauthorized user attempt to gain access
e. Hostile software
f. Disgruntled employees
g. Hacker and computer crimes
h. Terrorism
i. Minimizing risk in organisation infrastructure
j. Single point of failure analysis
    i. Objectives
        1. Identify IT risks
        2. Determine level of risk
        3. Identify risk factors
        4. Determine risk mitigation strategies
    ii. Benefits
        1. Business driven process to identify, manage and quantify risk
        2. A framework that governs technological choice and delivery processes
        3. Interpretation and communication of potential risk impact and risk reduction
        4. Implementation of strict disciplines for active risk management

5. Software and data back-up techniques
    a. Full
    b. Incremental
    c. Differential
    d. Mirror
6. Alternate processing facility arrangements
    a. Hot site
    b. Cold site
    c. Ware site
    d. Reciprocal arrangements
    e. Contract issues
        i. How soon
        ii. Number of user allowed concurrently
        iii. Priority to be given to concurrent users
        iv. Period
        v. Condition
        vi. Facilities and services
        vii. Controls in place and working
7. Back-up redundancy
    a. Importance
        i. Multiple backup media
        ii. Off site backup
        iii. Where to keep backup
        iv. Media rotation tactics
    b. Types of media
        i. Floppy disk

ii. DVD/CD
iii. Tape drives
iv. Digital audio tape
v. Optical juke box
vi. Autoloader tape system
vii. Disk drives
viii. Removable disk
ix. USB flash drive
x. ZIP drive

c. Fundamental factors
i. Speed
ii. Reliability
iii. Cost
iv. Capacity
v. Extensibility

d. Backup tips
i. Draw simple and easy to understand plan
ii. Keep a record of what, when, which media used
iii. Put proper labels on media
iv. Use software utilities for automatic backup scheduling
v. Verify backup files after process
vi. Create reference points
vii. Restore privilege to administrator only
viii. Create step-by-step guidelines

8. DRP
a. Procedural plan
b. Insurance
i. Coverage
ii. Kinds
1. First party – property damages
2. First party – business interruptions
3. Third party – general liability
4. Third party – errors and omission

9. Testing methodology
a. Types of test
i. Hypothetical
ii. Component
iii. Module
iv. Full

b. Methodology
i. Setting objectives
ii. Defining boundaries
iii. Scenario
iv. Test criteria
v. Assumption

vi. Test prerequisites
vii. Briefing
viii. Checklist
ix. Analysing test
x. Debriefing

10. Audit tools and techniques
    a. Automated tools
    b. Internal control auditing
    c. Disaster and security checklists
    d. Penetration testing

ERP

1. Introduction
2. ERP – Definition
    a. Evolution
        i. Aggressive cost cutting
        ii. Need to analyze costs/revenue
        iii. Flexibility to respond to changes
        iv. Changes in ways to do business
    b. Enabling technologies
    c. Characteristics
        i. Flexibility
        ii. Modular & open
        iii. Comprehensive
        iv. Beyond the company
        v. BBP
    d. Features
        i. Multi-platform, lingual, currency, facility
        ii. Function effectively integrated for flow and update by single entry
        iii. Company-wide integration
        iv. Integration of companies under same management
        v. Perform core activities and increase customer services
        vi. Eliminates most business problems
        vii. Bridge information gap
        viii. SCM to optimize demand and supply data
        ix. Allow automatic introduction of latest technologies
        x. Provides intelligent business tools like DSS, EIS, Data mining
    e. Why ERP
        i. Integrate financing
        ii. Integrate customer order processing
        iii. Standardize and speed up manufacturing
        iv. Reduce inventory
        v. Standardize HR information

f. Benefits
    i. Improved business processes
    ii. Improves productivity
    iii. Improved resource utilization
    iv. Reduce inventory levels
    v. Improves financial controls
    vi. Helps in reducing operating cost
    vii. Fast and accurate reports
    viii. Unified customer database
    ix. Better follow-up on customers
    x. Supports strategic planning
    xi. Improved decision making capability
    xii. Better information access throughout management

3. BPR
    a. What is BPR
        i. Fundamental rethinking
        ii. Radical redesign
        iii. Dramatic improvement
    b. Business engineering
    c. Business management
    d. Business modeling
4. ERP implementation
    a. Hindrances/Impediments
        i. Working together to achieve overall objectives
        ii. Properly managed implementation, Workload may not decrease
        iii. Customization
        iv. Roles and responsibilities
        v. Expandable and adaptable
    b. Implementation decision
        i. ERP or no ERP
        ii. Follow software processes or customization
        iii. In-house or outsourced
        iv. Bing – bang or phased implementation
    c. Methodology
        i. Identify the needs for implementing ERP
        ii. Evaluate "As is" situation
        iii. Decide "Would be" situation
        iv. BPR
        v. Evaluate various ERP packages
            1. Flexibility
            2. Modular & open
            3. Comprehensive
            4. Beyond the company
            5. BBP
            6. Integrates

7. New technologies

vi. Finalise most suitable package
vii. Install required hardware and network
viii. Finalise implement consultants
ix. Implement ERP

d. Guidelines
i. Understand the corporate needs
ii. BPR
iii. Good communication network
iv. Strong and effective leadership
v. Capable project manager
vi. Balanced team of consultants
vii. Good implementation methodology
viii. Training to user
ix. Adapting new system

5. Post implementation
a. Expectation
b. Fears
6. Risk and governance issues
a. Single point failure
b. Structural changes
c. Job roles changes
d. Online real time
e. Change management
f. Broad system access
g. Data content quality
h. Privacy and confidentiality
i. Single sign on
j. Distributes computer experience
k. Program interfaces and data conversion
l. Dependence on external assistance
m. Audit expertise
7. Why ERP fails
a. Resistance in adoption of work methods outlined in ERP
b. Customization of standard software
c. Changing habits is more difficult than customizing
8. ERP and E-commerce
a. Complex and not intended for public use
b. Two new channels – For customers and for supplies/partners
c. Careful planning needed
9. Life after implementation
a. Tasks to performed
i. Develop new job description and organisation structure
ii. Identify skills gap
iii. Assess training requirements and implement training plan

iv. Develop and amend HR, financial and operational policies

b. Post implementation blues
   i. Change in business environment – Change in CSF – Change in KPI
   ii. A review may indicate change in some processes
   iii. New processes require extra business functionality
   iv. Continuous improvement in technology and hardware require change in ERP

ISA standards, guidelines, best practices

1. Introduction
   a. Common features
      i. Every organization using IT, uses set of controls
      ii. Set of controls depend on business objective, budget, etc
      iii. Set of control objective should be constant
      iv. Everyone uses same control framework
2. ISO 27001
   a. General
      i. Asset to be protected
      ii. Approach to risk management
      iii. Control objective and control (3)
      iv. Degree of assurance required
   b. Establishing management framework (1)
      i. Define SP (2)
      ii. Make appropriate risk assessment
      iii. Identify areas of risk
      iv. Select appropriate control (4)
      v. Prepare SoA (5)
   c. Implementation
      i. Verification procedures
      ii. Review procedures
   d. Documentation
      i. Management control
      ii. 12345
      iii. Procedures under implementation control
      iv. ISMS control procedure
      v. Document control
      vi. Records
   e. Areas of focus
      i. Security policy
         1. Definition of information security
         2. Statement of management intention
         3. Allocation of responsibility
         4. Explanation of standards and compliance requirements
         5. Defined review procedures and means of assessing
         6. Nomination of policy owner

ii. Organizational security
    1. IS infrastructure
    2. Security to 3rd party access
    3. Outsourcing
iii. Asset classification and control
    1. Accountability of assets
        a. Inventory, ownership, IAR
    2. Information classification
        a. Classification guidelines
        b. Information labeling and handling
iv. Personnel security
    1. Security requirement in job definition and employee resourcing
    2. User training
    3. Responding to security incidents
v. Physical & environmental security
    1. Secure areas
    2. Equipment security
    3. General controls
vi. Communication and operations management
    1. Operational procedures & responsibilities
    2. Protection against malicious software
    3. Housekeeping
    4. Network management
    5. Media handling & security
    6. Exchanges of information & software
vii. Access control
    1. Business requirement for access control
    2. Monitoring system access & use
    3. (Same as in chapter 3 under logical control)
viii. System development and maintenance
    1. Security requirement of system
    2. Security in application systems
    3. Security of system files
    4. Security in development & support process
    5. Cryptographic control
ix. BC management
x. Compliance
    1. Compliance with legal requirement
    2. Review of SP and technical Compliance
    3. System audit consideration

3. CMM
    a. Fundamental concept
    b. Software process capability
    c. Software process performance
    d. Software process maturity

    e. Phases
        i. Initial
        ii. Repeatable (disciplined)
        iii. Managed (standard, consistent)
        iv. Defined (predictable)
        v. Optimizing (continuous improving)
4. COBIT
5. COCO
6. ITIL
7. Systrust & webtrust
    a. Principles
        i. Security
        ii. Availability
        iii. Processing integrity
        iv. Online privacy
        v. Confidentiality
    b. Broad areas
        i. Policies
        ii. Communication
        iii. Procedures
        iv. Maintenance
8. HIPPA
    a. Title I and Title II
    b. Security rules
        i. Administrative
        ii. Physical
        iii. Technical
9. SAS 70
    a. Type of reports
    b. Benefits to SO
    c. Benefits to UO

IS Security policy, Audit policy and Audit Reporting

1. Introduction
2. Importance of IS security
    a. Widespread use of technology
    b. Interconnectivity
    c. Unevenness of technology
    d. Unconventional electronic attacks
    e. Devolution of management and control
    f. Legal and regulatory requirement
3. IS security
    a. Security objective (CIA)
    b. Sensitive information

   i. Strategic plans
   ii. Business operations
   iii. Financial information
c. Establishing better protection
   i. Not all data has same value
   ii. Know where the critical data resides
   iii. Develop an access control methodology
   iv. Protect information stored on media
   v. Review hard copy output

4. Protecting information
   a. Rules
      i. What the IS are and where these are located
      ii. Value of the information held and how difficult it would be to recreate if it were damaged or lost
      iii. Who are authorized to access the information and what they are permitted to do
      iv. How quickly information needs to be made available if it become unavailable for whatever reason
   b. Types
      i. Preventive
      ii. Restorative
      iii. Holistic
5. ISP
   a. Issues to address
      i. Definition of information security
      ii. Why information security is important
      iii. Brief explanation of security policies
      iv. Definition of all relevant roles and responsibilities
      v. Reference to supporting documents
   b. Members of SP
      i. Management members
      ii. Technical group
      iii. Legal experts
6. Types of ISP and hierarchy
   a. ISP
   b. User SP
   c. Acceptable usage policy
   d. Organisational ISP
   e. Network & system SP
   f. Information classification SP
   g. Condition of connection
7. Components
   a. Security organization structure
   b. Document maintenance and compliance
   c. Monitoring and audit requirements

d. Purpose and scope
    i. Ensure CIA
    ii. Restrict and deny access to unauthorized users
    iii. How far, to whom and the period of SP
e. Security organisation structure
f. Responsibility allocation
    i. Appoint owner
    ii. Aware staff the need and responsibility
    iii. Task completion and satisfied owner
    iv. Contact list if security incident
    v. Controlled & Risk assessment for 3rd party access
    vi. Condition of connection agreement
    vii. New network link to be approved
    viii. Outsourcing contract details
g. Asset classification and security classification
    i. Maintain inventory
    ii. Formal & documented classification scheme
    iii. Classification by owner
    iv. Protective marking
    v. Controlled exchanges of data
    vi. Information labeling and handling
    vii. Classified waste disposed securely
h. Access control
    i. Prevent unauthorized access
    ii. Owner responsible for approving, maintain log
    iii. Grant access if business requirement
    iv. Access upto level required
    v. Registration, de-registration, deletion of users
    vi. Separate User ID, no sharing
    vii. Password policy
    viii. PC and terminal not left unattended
    ix. Mobile computing
i. Incident handling
    i. Consistent reporting approach
    ii. Procedure to ensure recording
    iii. Reoccurrence analysis to identify weakness
    iv. Procedures for collection of evidence
    v. Adequate records for inspection
j. Physical and environmental security
    i. Maintain check to identify vulnerable area
    ii. IT infrastructure physically protected
    iii. Secured access
    iv. Sensitive information & valuable assets locked away
    v. PC and terminal not left unattended
    vi. Supplies delivered & loaded at separate place

vii. Equipment, information not taken off-site without authorization
viii. Premises (equipment, data) located away from threats

k. Business continuity management
   i. BCP maintained, tested, updated
   ii. BIA conducted annually

l. System development and maintenance controls
   i. Controls identified prior to development
   ii. Controls to ensure CIA

8. Audit policy
   a. Purpose
      i. Unauthorized access to confidential data and information
      ii. Password disclosure
      iii. Virus infections
      iv. Denial of service attacks
   b. Objectives
      i. Safeguard IS asset & resources
      ii. Ensure data integrity
      iii. Ensure system efficiency and effectiveness
      iv. Compliance with SP, guidelines, etc
   c. Scope
      i. Adequacy & effectiveness of ICS
      ii. Quality of performance by IS
      iii. POD to reasonable assurance for achievement of objectives and goals
      iv. Provide information to appraise ICS
   d. What audit policy should do
      i. Periodicity and authority of reporting
      ii. Minimum professional proficiency required
      iii. Declaration of fidelity & secrecy
      iv. Extent of testing to be done
      v. Documented audit program
         1. Objectives & scope
         2. Nature and degree of testing required
         3. Identification of technical aspects, risks, processes
         4. Document procedures of audit
         5. Prior preparation and subsequent modification of procedures
      vi. Define access rights
         1. User level or system level access to devices
         2. Access to information
         3. Access to work areas
         4. Access to reports/documents
         5. Monitor and log network traffic
      vii. Compliance testing
         1. Organizational and operational control
         2. Security management control
         3. Application control

4. Access control
5. Physical and environmental security
6. Business continuity management
7. System development control

viii. Substantive testing
1. Observe weakness
2. High risk exposure
3. Gather additional information

9. Audit working papers
   a. Form and content affected by
      i. Nature of engagement
      ii. Form of audit report
      iii. Complexity of client's business
      iv. Condition of records and degree of reliance
   b. Permanent audit file
      i. Organization structure
      ii. IS policies
      iii. Historical background
      iv. Important legal documents
      v. Study and evaluation ICS
      vi. Old audit reports
      vii. MRL
   c. Current audit file
      i. Acceptance letter and scope
      ii. Evidence of planning process
      iii. Record of NTE of procedures and results
      iv. Letter and notes concerning audit matters and material weaknesses
      v. MRL and confirmation
      vi. Conclusion reached on significant aspects and how exceptional matters resolved
      vii. Copies of data and system and related audit reports
10. Documentation
   a. Planning key factors
      i. Knowing your resources
      ii. Defining scope
      iii. Knowing your audience
   b. Rules
      i. Gathering information
         1. About reader
         2. About subject
      ii. Organizing
         1. Selecting information
         2. Dividing into sections and subsections
      iii. Writing
         1. Writing in active voice
         2. Giving consequences

3. Writing from general to specific
4. Consistency

iv. Finalizing

1. Review and test
2. Generating glossary and index
3. Formatting and production

11. IS audit reports
    a. Cover and title page
    b. Table of content
    c. Summary
    d. Introduction
        i. Context
        ii. Purpose
        iii. Scope
        iv. Methodology
    e. Findings
    f. Opinion
    g. Appendices
    h. Level of detail
    i. Commentary