

Dear Students,

The topics covered in this document are relevant changes for May 15 IPCC-IT exams.

Students referring my notes can link changes with me IPCC-IT book applicable for Nov14 exams.

For any query post your query @ kunalsir.in

Chapter 1 → download notes from kunalsir.in

Chapter 2 (topic 14)

Instruction Set Architecture (ISA): Instruction Set Architecture (ISA) is related to the programming of a computer – that is, how the computer understands what each element in its basic language.

Instructions are translated to machine code. In some architecture, all machine code instructions are the same length i.e. **fixed length**. In other architectures, different instructions may be translated into **variable lengths** in machine code.

Complex Instruction Set Computer (CISC): If the control unit contains a number of micro-electronic circuitry to generate a set of control signals and each micro-circuitry is activated by a micro-code, this design approach is called CISC design. **In this Variable length instructions are commonly used and less space is required.**

Reduced Instruction Set Computer (RISC): To execute each instruction, if there is separate electronic circuitry in the control unit, which produces all the necessary signals, this approach of the design of the control section of the processor is called RISC design. **In this Fixed length instructions are commonly used so job of fetching & decoding instructions is more efficient.**

Chapter 3

Topic 19

Protocols: Protocols are software that performs a variety of actions necessary for data transmission between computers. Protocols are a set of rules for inter-computer communication that have been agreed upon and implemented by many vendors.

Network protocols which are essentially software are sets of rules for-

Communicating timings, sequencing, formatting, and error checking for data transmission.

Providing standards for data communication.

A protocol defines the following three aspects of digital communication:

Aspect	Description
Syntax	Syntax means the format of data being exchanged. It includes the character set used, type of encoding scheme, etc.
Semantics	Semantics means the type and order of messages used to ensure reliable and error-free information transfer.

Timing

Timings define the rate of data transmission or the speed and the correct timing for data transfer.

Different protocols cannot talk to each other hence standard protocols have been structured to resolve the problem.

Network transmission over internet is not actually continuous but is carried out in packets. The entire operation of data transmission over a network is broken down into several systematic steps. Each step has its own rules or protocol. We are now discussing this process in brief.

When transmission begins, Protocol at the sending computer:

- Breaks the data into packets,
- Adds destination address (of the other computer/server) to the packet,
- Prepares and sends data for transmission through Network Interface Card (NIC).

After transmission from sending device, Protocol at the receiving computer–

- Takes data packets off the cable or other medium,
- Brings packets into computer through Network Interface Card (NIC),
- Strips the packets off any transmitting information like address,
- Copies data from packet to a buffer for reassembly,
- Passes the reassembled data to the application program say Internet Explorer.

Topic 25

Network Security Protocols are **primarily designed to prevent any unauthorized user, application, service or device from accessing network data.**

Network security protocols generally **implement cryptography and encryption** techniques to secure data.

Network security **involves four aspects**: Privacy (Confidentiality), Message Authentication, Message Integrity and Non-repudiation.

Privacy: This means that the sender and the receiver expect confidentiality. This is achieved by cryptography and encryption techniques so that the data is secured and can only be decrypted with a special algorithm. [now [Cryptography & Encryption has been made part of this.](#)]

There are two categories of encryption/decryption methods: the Secret Key Method and the Public Key Method.

In **Secret key encryption/decryption** method, the **same key is used by both sender and the receiver**. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In this, for **decryption the algorithm is used in inverse order of the algorithm** used for encryption.

In **Public key encryption**, there are **two keys: a private key and a public key**. The private key is kept by the receiver and the public key is announced to the public.

Authentication: This means that the receiver is sure of the sender's identity and that an imposter has not sent the message.

Integrity: This means that the data must arrive at the receiver exactly as it was sent. There must not be any changes during the transmission – either accidental or malicious.

Non-Repudiation: This means that a receiver must be able to prove that a received message came from a specific sender and the sender must not be able to deny sending it.

These three can be achieved using Digital Signatures. Public key encryption can be used to sign a document. In digital signature, the private key is used for encryption and the public key for decryption.

Topic 26

IDS Technologies: [NNID deleted]

Network Access Control

Network Access Control (NAC) products **enforce security policy** by granting only security policy-compliant devices access to network assets.

Anti – Malware

Anti-malware network tools help administrators identify block and remove malware. Malware is always on the lookout for network vulnerabilities such as in operating systems, browsers, applications etc. that they can exploit.

Topic 27

Network Administration and Management

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security.

Fault Management → The goal of fault management is to recognize, isolate, correct and log faults that occur in the network. Fault management identifies and isolates network issues, proposes problem resolution, and subsequently logs the issues and associated resolutions.

Configuration Management → Monitors network and system configuration information so that the impact on network operations can be tracked and managed.

Accounting Management → Accounting management is concerned with tracking network utilization information etc. so business units can be appropriately billed or charged for accounting purposes. For non-billed networks, accounting refers to administration whose primary goal is to administer the set of authorized users

Performance Management - Measures and makes network performance data available so that performance can be maintained and acceptable thresholds. The network performance addresses the throughput, network response times etc.

Security Management - Controls access to network resources as established by organizational security guidelines. Security management functions include managing network authentication, authorization, and auditing.

Topic 43

Information Systems and Telecommunication

Telecommunication give an opportunity to move data at distant location and to collaborate between employees, customers and to capture high competitive ground in the marketplace.

Telecommunications helps in

An increase in the efficiency of operations;

Improvements in the effectiveness of management; and

Innovations in the marketplace.

Telecommunications may provide these values through the following impacts:

Time compression

Chapter 4

Topic 2 [table added]

People Resources	Specialists - systems analysts, software developers End Users—anyone else who uses information systems
Hardware Resources	Machines - computers, monitors, disk drives, printers, optical scanners. Media - floppy disks, magnetic tape, optical disks, plastic cards, paper forms.
Software Resources	Programs - operating system programs, spreadsheet programs etc. Procedures - data entry procedures, paycheck distribution procedures.
Data Resources	Product descriptions, customer records, employee files, inventory databases.
Network Resources	Communications media, communications processors, network access, control software.
Information Products	Management reports and business documents using text and graphics displays, audio responses, and paper forms.

Topic 6 [one topic added]

Typical Transaction Processing Cycle

Data Entry: The first step of the transaction processing cycle is the capture of business data. The recording and editing of data has to be quickly and correctly captured for its proper processing.

Transaction Processing: Transaction processing systems process data in two basic ways: (i) batch processing, and (ii) real-time processing (also called online processing). All online TPS depend on the capabilities of fault tolerant computer systems that can continue to operate even if parts of the system fail.

Database Maintenance: An organization's databases must be updated by its transaction processing systems so that they are always correct and up-to-date.

Document and Report Generation: Transaction Processing Systems produce a variety of documents and reports. Examples - purchase orders, paychecks, sales receipts etc.

Topic 7 [following addition]

Examples of Office Automation Applications

Word Processing → Use of a computer to perform automatically many of the tasks necessary to prepare typed or printed documents.

Electronic mail → Use of a computer network that allows users to send, store and retrieve messages using terminals and storage devices.

Electronic Calendaring → Use of a networked computer to store and retrieve a manager's appointment calendar. Allows other managers' calendars to be accessed and facilitates scheduling.

Video Conferencing → Use of television equipment to link geographically dispersed conference participants.

FAX → Uses special equipment that can read a document at one end of a communication channel and make a copy at the other end.

Desktop Publishing → Uses a computer to prepare output that is very close in quality to that produced by a typesetter.

Topic 18 [following added]

Some of the commercial applications of AI are as follows

Decision Support → Intelligent human–computer interface (HCI) systems that can understand spoken language and gestures, and facilitate problem solving by supporting organization wide collaborations to solve particular problems.

Information Retrieval → Natural language technology to retrieve any sort of online information, from text to pictures, videos, maps, and audio clips, in response to English questions. Database mining used for marketing trend analysis, financial forecasting etc.

Virtual Reality → X-ray–like vision enabled by enhanced-reality visualization that allows brain surgeons to “see through” intervening tissue to operate.

Robotics → Machine-vision inspections systems for gauging, guiding, identifying, and inspecting products and providing competitive advantage in manufacturing.

Chapter 5

One first page, table replaced with following

Types	Nature of processing	Source of application	Size and Complexity of business	Nature of Application
Type I	Batch Processing	Custom built	Small business	Accounting application
Type II	Online Processing	Packaged software	Medium business	Cash Management
Type III	Real-time Processing	Leased	Large business	Manufacturing Applications
More types	No	Yes	No	Yes

Applications based on Nature of Processing

Batch Processing: It is defined as a processing of large set of data in a specific way, automatically, without needing any user intervention. The data is first collected, during a work day, for example, and then batch-processed, so all the collected data is processed in one go.

Online Processing: Data is processed immediately while it is entered, the user usually only has to wait a short time for a response. Interactive or online processing requires a user to supply an input.

Real-time Processing: Real time processing is a subset of interactive or online processing. Input is continuously, automatically acquired from sensors. This system doesn't need a user to control it, it works automatically. Whenever there is a rapid reaction required due to some sort of change, real time processing can take action without the need of a user.

Applications based on Source of Application

Custom-built Application: Whether they are for one function or integrate processes across the company like an ERP – these are the easiest ones to customize. Customization involves additional coding as per business requirements and style. Example – Billing, Inventory etc.

Packaged Software: These are the standard applications which are not free but are licensed. Customization to suit business requirements may or may not be allowed. For Example -Tally, Oracle 9i, etc.

Leased application: A new method for getting applications is being used today, i.e. leased applications, where user pays fixed rent for using the application for agreed terms.

In topic 6 BPA, now all benefits of ch 1& 2 added and total benefits are now 9

Topic no. 14 'Info. System control changed'

Information Systems' Controls

Controls divided into 2 categories i.e. Managerial Controls & Application Controls.

Usually auditors cannot examine and evaluate all the data processing carried out within an organization. They need guidelines that will direct them toward those aspects of the information systems function in which material losses or account misstatements are most likely to occur.

Controls reduce expected losses from unlawful events by -

Decreasing the probability of the event occurring in the first place, or

Limiting the losses that arise if the event occurs.

Following newly added

Managerial Controls

These are controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner.

Types of Management Subsystem

Top Management → Top management must ensure that information systems function is well managed.

Information Systems Management → IS management has overall responsibility for the planning and control of all information system activities.

Systems Development Management → Systems Development Management is responsible for the design, implementation, and maintenance of application systems.

Programming Management → It is responsible for programming new system; maintain old systems and providing general systems support software.

Data Administration → Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.

Security Administration → It is responsible for access controls and physical security over the information systems function.

Quality Assurance Management → It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.

Operations Management → It is responsible for planning and control of the day-to-day operations of information systems.

Managerial Functions Based Controls

Top Management and Information Systems Management Controls: The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior manager must perform are Planning, Organizing, Leading, Controlling.

Systems Development Management Controls: Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining

information systems. Three different types of audits may be conducted during system development process as discussed below:

Concurrent Audit: Helps in improving the quality of systems development.

Post-implementation Audit : Auditors seek to help an organization learn from its experiences in the development of a specific application system

General Audit: Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion.

Programming Management Controls: Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. The program development life cycle comprises six major phases as follows:

Phase	Controls
Planning	Techniques like Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan
Design	A systematic approach to program design
Coding	Programmers must choose a module implementation and integration strategy.
Testing	Three types of testing can be undertaken: • Unit Testing – which focuses on individual program modules; • Integration Testing – Which focuses in groups of program modules; and • Whole-of-Program Testing – which focuses on whole program.
Operation And Maintenance	Three types of maintenance can be used – Repair maintenance – in which program errors are corrected; Adaptive Maintenance – in which the program is modified to meet changing user requirements; and Perfective Maintenance - in which the program is tuned to decrease the resource consumption.
Control	Monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

Data Resource Management Controls: Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. If data repository system is used properly, it can enhance data and application system reliability.

Quality Assurance Management Controls: Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software. Organisations are becoming more concerned about their liabilities if they produce and sell defective software.

Security Management Controls: Information security administrators are responsible for ensuring that information systems assets are secure. Major threats and their control measures are as follows:

Fire: Well-designed, reliable fire-protection systems must be implemented.

Water: Facilities must be designed and sited to mitigate losses from water damage

Structural Damage: Facilities must be designed to withstand structural damage.

Unauthorized Intrusion: Physical access controls can be used.

Viruses and Worms: Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.

Operations Management Controls: Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions like Computer Operations, Communications Network Control etc. Operations management control must continuously monitor the performance of the hardware/software platform to ensure that systems are executing efficiently.

Under application controls, input control simplified and same is given under

Input Controls:

These are responsible for ensuring the accuracy and completeness of data that are input into an application system.

Input controls are important since substantial time is spent on inputting data which involves human intervention and are therefore chances of errors and fraud are more here.

Type of Input Controls:

Source Document Control: In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments.

Data Coding Controls: Data Coding Controls are put in place to reduce user error during data feeding.

Batch Controls: These controls are put in place at locations where batch processing is being used. The objective is to ensure accuracy and completeness of the content and that they are not lost during transportation.

Validation Controls: These controls validate the accuracy/correctness of input data. Input Validation Controls are intended to detect errors in transaction data before the data are processed.