INTER CA – MAY 2018

Sub : ENTERPRISE INFORMATION SYSTEM

Topic : Automated Business Process, Information System and Its Components, E- Commerce, M-commerce & Emerging Technologies.

Test Code – M17

Branch : MULTIPLE **Date : 07.01.2018**

(50 Marks)

Note: All questions are compulsory.

Question 1 (4 marks)

CBIS is a combination of people, IT and Business Process that helps management in taking important decisions to carry out the business successfully.

CBIS consists of the following elements / components -

Item	Description
1. People	The end – objective of the CBIS is to be useful to people. People cover all type of persons, within and outside the Entity.
2. Hardware	(a) Hardware consists of **Physical Components** including Computer System, i.e. CPU, and all of its support equipment, i.e. peripherals e.g. Input Devices, Storage Devices, and communications Devices. It includes Server or Smart Terminals with different configurations and Processors, etc. (b) **Hardware Resources** refer to – (i) **Machines** – Computers, Video Monitors, Magnetic Disk Drives, Printers, Optical Scanners, and (ii) **Media** – Floppy Disks, Magnetic tape, Optical Disks, Plastic Cards, Paper Forms, etc.
3. Software	(a) Software consists of computer Programs and their User Documentation or Manuals. (b) Programs are machine – readable instructions that direct the CBIS Hardware to produce useful information from data. (c) Software includes – (i) different types of Operating Systems like UNIX, LINUX, WINDOWS, etc. (ii) Applications Software (computer programs designed to perform specific tasks), and (iii) Utility Software (e.g. Tools) . (d) **Software Resources** refer to – (i) **Programs** – Operating System Programs, Spread sheet Programs, Word Processing Programs, Payroll Programs, and (ii) Procedures – Data Entry Procedures, Error Correction Procedures, Pay check Distribution Procedures, etc.
4. Data	(a) Data are **facts** that are used by programs to produce useful information. Like Programs, Data are generally stored in machine – readable form on disk or tape until the Computer needs them. (b) Data may be alphanumeric, text, image, video, audio and other forms. (c) In a CBIS, Data is organized in terms of a Database Management System (DBMS).
5. Network	Network means the **Communication Media** – Internet, Intranet, Extranet, etc.

Question 2 (4 marks)

Point	Description

1. Concept	(a) SoD Concept aims at creating controls, checks and balances such that high – value and high sensitivity activities and transactions involve the coordination of two or more authorized persons in the Entity. (b) SoD Concept seeks to ensure that a single individual does not possess excess privileges, that could result in unauthorized / harmful activities like fraud or the manipulation or exposure of sensitive data. (c) **Example:** In the area of Payment Processing, the activities of – (i) Creation of Vendor Code, (ii) Authorisation of Vendor's Bills, and (iii) Printing of Cheques are handled by separate individuals.
2. Nature of SOD Controls	SoD Controls – (a) Are in the nature of Preventive and Detective Controls place to manage segregation of duties matters. (b) Can be manual or even automated, depending on the nature of transactions – situation, and sometimes required manual intervention in an automated control.
3. Examples of SOD Controls	(a) **Authorisation:** "Maker" (Imitator) of a transaction is different from the "Checker" (i.e. person approving or authorizing the transaction. Sometimes the application program can be configured so as to require two or more persons to "Check" (approve) certain transactions. (b) **Workflow:** Workflow – enabled Applications use a second (or third) level of approval before certain high – value or high – sensitivity activities can take place. [Example: Based on value of the transaction – (i) Loan Processing in a Bank require multiple level approvals.] (c) **Split Custody:** Dual / Multiple Custody of high – Value / sensitive assets is achieved by defining strong Passwords which are split into two halves, one half assigned to two persons, and the other half assigned to two persons, so that no single individual knows the entire password. Sometimes, additionally, personal Identification Criteria like Biometrics, Iris Scan, etc. are used to validate access. (d) **Audit / Review:** IT Personnel or Internal Audit Personnel periodically review User Access Rights to Identify SoD issues. The Access Privileges for each User is compared against a SoD control Matrix.
4. Managing SOD Issues	When SOD issues are encountered during a review / audit, the IT Management should mitigate the SOD Issue by – (a) Reducing the Access Privileges to various Individual Users so that the SOD conflict no longer exists, (b) Introducing new Mitigating (preventive or detective) Controls to prevent or detect unwanted activities, if Access Privileges cannot be reduced. [Examples: (i) Increased logging to record the actions of personnel. (ii) Improved exception reporting to identify possible SoD issues, (iii) periodic reconciliations of Data Assets, (iv) external reviews of high – risk controls, etc.]

Question 3 (4 marks)

1. Input Controls are responsible for ensuring the accuracy and completeness of data and Instruction input into an application system, sometimes using data codes.
2. Input Controls are important since substantial time is spent on input of data, involve human Intervention and are therefore prone to error and fraud.
3. Input Controls Include Existence / Recovery Controls, since it might be necessary to re-process input data in case the Master Files are lost, corrupted, or destroyed.
4. Sources Documents or Transaction Listings are generally stored securely for longer periods for reasons like statutory requirements, change verification, audit trail, etc.
5. Input Controls are further classified into – (a) Source Document Control, (b) Data Coding Controls, (c) Batch Controls, and (d) Validation Controls.

Question 4 (6 marks)

Computer Crimes: Computer Systems can be used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made. The effects of Computer Crimes on the Entity are –

1. Financial Loss: Financial Losses may be – (a) direct, e.g. loss of electronic funds, or (b) indirect, e.g. expenditure towards repair of damaged electronic components.

2. Legal Battles: Organizations will be exposed to lawsuits from Inventors and Insurers, if there are no proper security measures. The IS Auditor should obtain legal counsel while reviewing the issues associated with computer security.

3. Loss of Credibility or Competitive Edge: To maintain competitive edge, organisations need credibility and public trust. This credibility will be shattered resulting in loss of business and prestige, if there is a security violation. Crimes can damage the reputation, morale and very existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations.

4. Blackmail / Industrial Espionage: By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

5. Disclosure of Confidential, Sensitive or Embarrassing Information: These events can spoil the reputation of the organization. Legal or regulatory actions against the Company are also a result of disclosure.

6. Sabotage: This is done by people who may not be interested in financial gain, but who want to spoil the credibility of the Company. They do it because of their dislike towards the organization or for their intemperance.

7. Spoofing: Spoofing is considered a Technical Exposure / Computer Crime Exposure.

Question 5 (4 marks)

1. Audit Hooks are audit routines that flag or mark suspicious transactions.

2. When audit hooks are employed, the Auditors are Informed of questionable transactions immediately on their occurrence by displaying a message on the Auditors terminal. This immediate notification is called real – time notification.

3. Example: The Internal Auditor of a Bank, envisaged that Pensioner's Accounts, Where the pension is directly credited to the pensioner's account, is vulnerable to fraud, useless a life Certificate is obtained each year from the individual concerned. They devised a system of Audit Hooks to tag records where Life Certificate was not obtained. The Internal Audit Department will be notified / informed when a transaction takes place in a tagged record. The Audit Department can take steps to investigate fraud, if any

Question 6 (4 marks) (1/2 mark each)

Control Objectives in e – Commerce include the following –

1. To recognize the significance of Information as a Critical Asset to the Entry,
2. To prevent loss from incorrect decision making.
3. To recognize the criticality and value of all IT Resources, viz. Hardware, Software and Personnel,
4. To prevent Cost of Data Loss.
5. To avoid Computer Abuse and its related costs.
6. To maintain privacy and integrity of data shared through the Network amongst various Participants.
7. To safeguard IT Assets from un – authorized access.
8. To ensure System Effectiveness, i.e. the ability to meet substantial User requirements, and
9. To ensure System Efficiency, i.e. to optimize the use of various IS Resources (machine time, Peripherals, system software and labour).

Question 7 (6 marks) (1 mark each, students are not expected to write much detail)

A. Develop a sustainable Green Computing Plan:

1. Involve Stakeholders to include checklists, Recycling Policies, Recommendations for disposal of used equipment, Government and recommendations for purchasing green computer equipment in the organizational Policies and Place.
2. Encourage the IT Community for using the best practices, to consider green computing practices & guidelines.
3. On – going communication about and Firm's commitment to Green IT best practices to produce notable results. This includes power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organisational policies and plans, and.
4. Use Cloud Computing so that multiple organizations share the same computing resources, thus increasing the utilization by making more efficient use of hardware resources.

B. Recycle:

1. Dispose e – waste according to Central, State and Local Regulations.
2. Discard used or unwanted electronic equipment in a convenient and environmental attributes.
3. Manufacturers must offer safe end – of – life management and recycling options when products become unusable, and
4. Recycle Computers through Manufacturer's Recycling Services.

C. Make environmentally sound purchase decisions:

1. Purchase of Desktop Computers, Notebooks and Monitors based on environmental attributes.
2. Provide a dear, consistent set of performance criteria for the design of products.
3. Recognize Manufacture's efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials, and
4. Use Server and Storage Virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

D. Reduce Paper Consumption:

1. Reduce paper consumption by use of e – mail and electronic archiving.
2. Use of "track changes" features in electronic documents, rather than redline corrections on paper.
3. Use online marketing rather than paper – based marketing, use e – mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail, free and low – cost online invoicing solutions that help cut down on paper waste, and
4. While printing documents make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

E. Conserve Energy:

1. Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
2. Develop a Thin – Client strategy wherein Thin Clients are smaller, cheaper, simpler for Manufactures to build than Traditional PCs or Notebooks and most importantly use about half the power of a Traditional Desktop PC.
3. Use Notebook Computers rather than Desktop Computers whenever possible.

4. Use the power - management features to turn off Hard Drives and display after several minutes of inactivity.
5. Power – down the CPU and all Peripherals during extended periods of inactivity.

6. Try to do computer – related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
7. Power – up and power – down energy – intensive peripherals such as Laser Printers according to need.
8. Employ alternative energy sources for Computing Workstations, Servers, Networking and Data Centres, and
9. Adapt more of web – Conferencing offers instead of travelling to meetings in order to go green and save energy.

F. Green Security:

1. Identify IT Solution Providers who offers green security services, along with green computing technologies.
2. Identify how to increase the energy savings through green security services and assess that "how sustainable computing technology can immediately help the environment".
3. Identify the role of security tools, methods and practices that reduce a Company's environment impact.

Question 8 (4 marks)

Point	Description
Concept **(1/2 mark)**	The Internet of Things (IoT) is a system of inter – related computing devices, mechanical and digital machines objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human – to – human or human – to – computer interaction.
Examples **(1/2 mark)**	1. A Wi-Fi enabled Water Purifier, installed at a Customer's home, automatically connects to the Home Wi-Fi, and generates a Service Request with the Manufacturing Company, when the purifying agents deplete in the Machine. 2. A Wi-Fi enabled Car Engine System connects to the Car Dealer's Portal and logs on to generate a Routine Maintenance Services Request after running of a certain number of Kilometres.
Applications **(1/2 mark)**	1. Home Appliances are connected to create a "virtual home", so that all activities at home can be monitored through the Mobile Phone / Hand – held devices held by the Owner while s/he is at office. 2. Office Appliances are connected through intranet, so that many statistical information on Resource Usage can be obtained effectively, e.g. Number of Pages printed in Office Printer, etc.
Risks **(1 1/2 mark)**	1. **Environmental Risks:** All Home / Office Devices connected through Wi-Fi, use heavy earth metals and have an impact on the house air quality. 2. **Technology Risk:** There are hardware variations and differences in the software running on various devices, Leading to platform fragmentation and lack of technical standards. The task of developing common applications is very tough. **3. Obsolescence:** (a) Manufactures that bring in a new product may focus Users to dump the old products, by disabling the Operating Software of the old product. (b) An Entity (X) is taken over / acquired by another Entity (Y),and the latter does not support the old products sold. **4. Manufactures:** (a) Those Entities which do not have IoT devices have to ensure their

	confidentially and Integrity. (b) Entities which collect huge data from IoT devices have to ensure their Confidentially and Integrity. 5. **Internet Risk:** If all Home / Office Devices are connected to the Internet, they are subject to all Network – related risks, including hacking, virus attacks loss of confidential data, etc. 6. **Privacy:** Individuals may lose control over their personal life, which can be hacked and made public.

Question 9 (6 marks)

Risk Concept in BPA: (1 mark)

(a) Risk is any event that may result in a significant deviation form a planned objective resulting in an unwanted negative consequence. Thus, Risk is the possibility that an event will occur and adversely affect the achievement of objectives.

(b) The planned Objective may be any aspect of an Entity's strategic, financial, regulatory and operational processes, products or services.

(c) The degree of risk associated with an event is determined by – (i) the likelihood (uncertainty, probability) of the event occurring, (ii) the consequences (impact) if the event were to occur, and (iii) its timing.

3. Risk Types in BPA: BPA – related Risks include the following – **(1/2 mark each)**

(a) Input: Risks that all Input transaction data may not be accurate, complete and authorized.

(b) Transmission: Risk that all the Files and Data transmitted may not be processed accurately and completely, due to Network error or system failure.

(c) Processing: Risk that valid input data may not be processed properly due to program errors or other reasons.

(d) Output: Risk that output is not complete and accurate, or risk that output is distributed to Unauthorized Personnel.

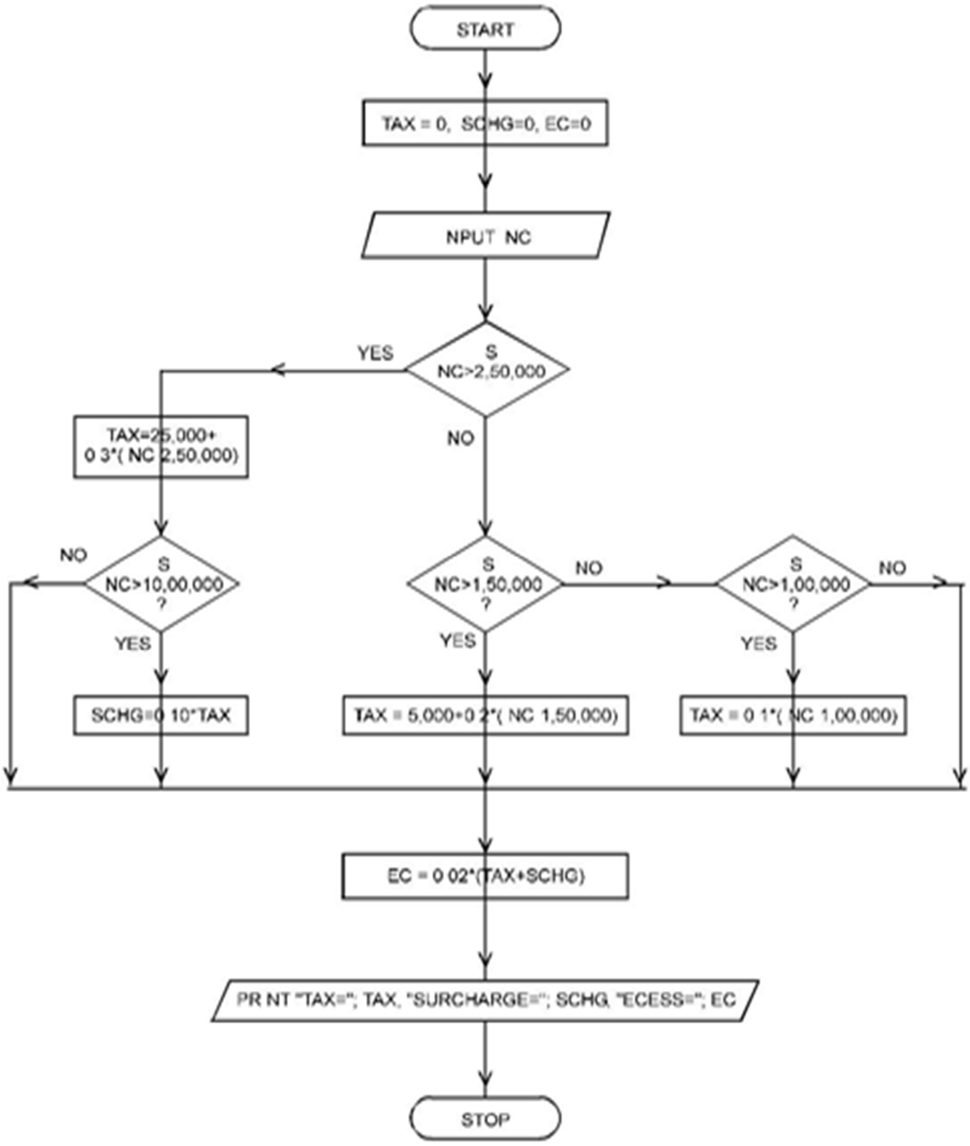
(e) Access: Risk that the Entity's Master Data and / or Transaction Data may be changed by Unauthorized Personnel due to weak access controls.

(d) Backup: Risk that all data & programs may be lost if there is no proper backup in the event of a disaster and the Entity's Operations could come to a standstill due to lack of adequate infrastructure settings.

Question 10 (8 marks)

We shall define the variables first:

SCHG: Surcharge; TAX: Income Tax; EC: Education Cess; INC: Income


START
TAX = 0, SCHG=0, EC=0
NPUT NC
S
NC>2,50,000
YES
NO
TAX=25,000+
0 3*(NC 2,50,000)
NO
S
NC>10,00,000
?
YES
SCHG=0 10*TAX
S
NC>1,50,000
?
NO
YES
TAX = 5,000+0 2*(NC 1,50,000)
S
NC>1,00,000
?
NO
YES
TAX = 0 1*(NC 1,00,000)
EC = 0 02*(TAX+SCHG)
PR NT "TAX="; TAX, "SURCHARGE="; SCHG, "ECESS="; EC
STOP

****