



Book No. 1 (containing 36 pages)

**THE INSTITUTE OF CHARTERED
ACCOUNTANTS OF INDIA**

C.A - Final

Examination

Group No. *II* Paper No. *2*

Subject *ISCA*

Number of Answer Books used.....

For use by ICAI only

335178



Q. No.	Please put ✓ against the Questions answered	Marks Awarded (to be filled by Examiner)					Total
		a	b	c	d	e	
1		5	2	4	5		16 ✓
2							
3		5	4	4			13 ✓
4		5	5	4			14 ✓
5		2	5	3			10 ✓
6		4	4	3			11 ✓
7		4	4	4	2		14 ✓
8							
9							
10							
Total							78

13 MAY 2015

100228-10468

Use only Blue / Black Ball Point Pen to write and shade the circles.
AVOID RED PEN.
Write the marks in the boxes before shading the respective circles.

Total Marks awarded

078

0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9

Total Marks awarded (in words)

Seventy eight only

Examiner's

Checked
(initial of the)

INSTRUCTIONS TO THE CANDIDATE

Answers are not to be written on this page

number should be written in figures and words in the allotted space at the right hand corner of the cover sheet.

2. Roll number should be written in the box in numbers and darken the appropriate circles of the OMR portion provided in the right hand corner of the cover page with **Black / Blue** ball point pen.
3. Fill particulars such as name of Examination, Group No., Paper No. and subject at the appropriate space at the left hand upper corner.
4. Remove the perforated Bar Code sticker of the particular paper from the Attendance sheet and affix the same on the box provided in the right hand corner of the cover page.
5. Since a machine will read the Roll no., please check and ensure that Roll number written in numbers, words and circles darkened are correct. In case any candidate fills this information wrongly, Institute will not take any responsibility for rectifying the mistake.
6. The answers should be written neatly and legibly
7. The answer to each question must be commenced on a fresh page and question number prominently written at the top of each answer. Alternatively, the question number should be distinctly written in the margin.
8. The answer to each question in all parts should be fully completed in one page, or in a consecutive set of pages, before the next question is taken up.
9. Writing of Roll number in place/s other than the space provided for the purpose or writing distinguishing mark, symbols like "OM", "Sri", "Jesus", "786", etc., will tantamount to adoption of "unfair means"

3. Q3 (a)

Organization fail to achieve its system development objectives because of following reason →

1) User Related Issues: →

a) Shifting of User Needs: → Information requirement in an enterprise changes according to the needs of Personnel / users / managers. Developers after developing information system observe that requirement / needs of user changes.

b) Resistance to Change: →

There is a inbuilt habit of users to resist the changes if changes negatively affect their performance, their capacity, income or increase the workload of user.

c) Lack of User Involvement's

Sometimes in system development users are not actively involved, this raise an hurdle for achieving system development methodologies.

d) Inadequate Testing or User Training.

Inadequate testing of system, sometimes errors not identified, leads to ineffective system.

User Training is also necessary to know how to operate a system.

2) Developer Related Issues

a) Lack of Project Management & System Development Methodologies :->

Sometimes organisation do not formalize their project development. Inadequate System Development methodology lead to ineffective system.

- b) Undertrained or Overworked developing Staff: → Sometimes in organisation we found that developing staff do not have necessary qualification, experience & expertise. In some enterprises developing staff are too overworked that they can't give proper attention.

3) Management Related Issues:

- a) ~~Lack~~ Lack of Management Involvement & Support: →

System developers ~~use~~ use to observe the Management & according change their priorities from one system to another.

Further more management support is imperative, the system which gets lesser support/ involvement may get delayed or abandoned.

b) Strategic System :-)

Developing system for supporting strategic decision require ~~some~~ high technically expertise which may not be available.

4. New Technologies

When organisation wanted to gain competitive advantage by using system, it find that users are not familiar with new technologies

7/03/16

Broad groups of OAS are-

- 1) Text Processing System
- 2) Electronic Message Communication System

ICAI

• Groups of OAS are →

1. Data Collection :- Collecting the data from various resources, to process data into information.
2. Data Capturing :- Capturing the data from internal & external environment to support business activities.
3. Receiving & distribution :-
Receiving data information from sources, mainly external & distribute to end user to perform their basic operations.
4. Calculation :- Calculating various aspects involves in business transactions.
5. Organisation :- Organise various

data & information in a hierarchy so that they can be ~~see~~ accessed easily.

Types of OAS are →

- 1) Text Processing System
- 2) Electronic data communication System
- 3) Electronic data Management System.
- 4) Teleconferencing & Video Conference

④

Norms for Selecting an Auditor by SEBI -

- 1) Auditor should have atleast 3rd of experience in security market like stock exchange, depositories, Mutual fund etc.
- 2) Auditor should have experience in direct & indirect ~~to~~ to experienced

SEBI norms for selecting an auditor are-

- 1) Auditor should have at least 3 Years of experience ~~in~~ ^{in secure} of conducting audit of Security Market like stock exchange, Mutual Fund, Depository. Experience should cover experience of various aspects as mentioned in Terms of Reference (TOR)
- 2) The auditor should have experience in indirect access to experienced resources as mentioned in TOR. Auditor should have requisite qualification ~~from~~ prevailing in the Industry like auditor should have ~~any~~ certification ~~from~~ for DISA from ISACA or CISP from ISACA.
- 3) Auditor should have compatible framework or processes prevailing in the industry like COBIT.

4. Auditor should not have any conflict of Interest with Management of auditee.
~~Manager~~ Auditor should not engage itself with any branch/unit of auditee for any consultancy work.
5. Auditor should not have any pending case with previous auditee, which falls within the ambit of SEBI, which disqualifies Auditor.

(4)

Corrective control should be considered as part of Internal Control. Any error or Malicious event which were not detected or prevented ~~etc~~ will adversely affect the organisation if no corrective control are in place. Examples of correcting controls are use default date on invoice when user wanted to alter or remove the date. Business Continuity planning are considered as corrective controls.

Characteristics of Corrective controls are →

1. Minimise the impact of error
2. Identify the cause of problem.
3. Providing remedy to defective controls for problems detected.
4. Getting feedback from Preventive & Corrective controls.
5. Correcting errors cause from problem.
6. Modifying the process to ensure that same error do not occur in future.

Steps involved in Auditing are →

1) Scoping & Preparation :-

In this step scope of audit is defined, which areas deserve more attention & eliminate the areas which are out of the scope. Scope can be determined by reviewing documents, observation, reviewing internet history.

2) Planning :- In this step scope is breaking down into plans & plans will be developed.

3. Field Work :-
Gathering of information through conducting interviews, questionnaires, observing processes.

4. Analyse :- Sorting out, classify & make sense of those collecting in previous

phase by using SWOT (Strength, Weakness, Opportunity, Threat) or PEST (Political, ~~Economic~~ Economical, Social, Technology) analysis.

5) Reporting :- After analysis in previous report will be done to management.

6) Closure :- Documentation will be prepare for future need & follow up to the management if any actions needs to be undertaken by management as per previous audit Report.

(5)

Q4(c) 16

Following categories of test.
performed by programmer ->

- 1) Functional Test
- 2) Structure Test
- 3) Stress Test
- 4) Performance Test.

(4)

- i) Yes, Mr A is punishable for his activities.

As per the provision of IT Act 2008, if any person intends to break/ignore/steal the information which is Nation's Importance, for maintaining integrity, sovereignty or reliability, or maintaining friendly relation with foreign countries are

liable for Imprisonment for whole life.

In the present situation Mr A. hacked the Defence Information System which is useful for maintaining sovereignty, integrity or building friendly relations with foreign country.

Therefore A is liable for imprisonment for whole life.

ii) No, Cyber Vd. It is not liable.

As per provisions of IT Act 2008
if the intermediary

1. provides only access to either person & he does not play any role
2. does not initiate the transmission
3. does not select the receiver
4. does not select the information
5. observing due diligence while discharging his duties

then he will not be liable for any prosecution or penalty.

But we can have another view, if the intermediary is aware about such commitment then he may be held liable, it depends upon facts of the case.

(2)

Key Management practices for achieving IT risk management.

1. Collect Data:-

Data will be collected & given to identify, analyse & reporting of risk associated.

2. Analyse Risk:-

Risk are analysed based on information provided

3. Maintain Risk Profile:-

Crather information of various risk opportunities & ~~there~~ threat to make a risk profile in which risk attributes, its frequency etc. ~~will~~ ^{include}

4. Articulate Risk:-

Provide information on risk opportunities & threats to all stakeholders.

5. Develop a Risk Management Portfolio:-

Create portfolio

risk at all risk rates & threats.

6. Respond to Risk → After completion of above practices control measures will be identified to respond to risk.

(5)

ICAI

Tasks performed by an Operating System while allowing users & their applications to share & access resources are →

1. Scheduling Jobs: It will schedule the jobs so that maximum users ~~can~~ can ~~do~~ work on applications.

2. Handling Interrupts: Interrupts are computer technique where processing of one program may be suspended to allow another programme to execute. This happens where operation does not require CPU, input or output.

3. Maintain Multi Sharing: Different users can use share or use single application concurrently. This will enable optimal utilization of resources.

4. Maintaining Usage Records:-
It maintain records on how much user spend his time on CPU network. This is done to charge the user department for using the peripherals.

(3)

ICAI

Principles of COBIT 5.

1. Meeting all Stakeholders needs.
2. Covering enterprise end to end.
3. Apply Single Integrated Framework.
4. Enable Holistic Approach.
5. Separating Governance & Management.

1. Meeting all stakeholder Needs:-

COBIT 5

Focuses on increase value creation through the use of IT by maintaining balance between benefit realisation, risk & control. COBIT-5 provide processes & enablers to achieve value creation.

2. Covering enterprise end to end:-

Focuses on IT^{and} but it also consider other information. COBIT 5 not only

Function & associated activities
It covers everything &
anything in the Organisation.

3) Apply Single Integrated Framework

There are many Framework & processes available in the market which define activities to be undertaken. But COBIT-5 is single integrated Framework which covers all process, enablers, activities etc.

4) Enable Holistic Approach for effective & efficient use of Governance & management, Holistic approach is required. COBIT-5 enable Holistic Approach to be implemented in an organisation

5. Separating Governance & Management:-

CODITE makes clear distinction between Governance & Mgt. Governance & Management involves different activities, rules & responsibilities

(4)

ICAI

Effect of Computer on Evidence Collection For audit are →

Inefficient

1. ^{Capacity} Data Retention & Storage ^{Client's} :-

Computer system may not have sufficient data retention & storage capacity. Like client may store data in hard disk & get the ~~hard~~ hard disk to office.

2. Absence of Input Documents :-

^{Written} input evidence may be substituted by telephonic order.

3. Non-Availability of Audit Trail :-

This makes an auditor's work difficult & make auditor to adopt approach which is ~~an~~ auditing around the computer system.

4. Lack of ~~low~~ Availability of Output:-

Output may not be available in printed form, in such situations, client's used to provide read only access to terminal.

5. Legal issues:- Increase use of computer also increase legal issues related to contracts like where the contract is made, what are the terms of contract etc.

(4)

Backup Option Sites are →

1. Cold Site :- If some down time can be tolerate, cold site backup is suitable. It provides necessary facilities to install mainframe system based - floors, air conditioning, power source etc. Cold site back up ~~is~~ is cheap, it can develop or we can share with others.
2. Hot site :- If fast recovery is required, this back up might be essential. In Hot site backup some hardware & operational facilities are available. Sometimes software, data & servers also available. Hot site back up ^{is expensive} is difficult to maintain it can share with others.

3. Warm Site :- This provide immediate level of Backup. It has software like cold site but it may also contain hardware which is difficult to maintain.

4. ~~Receptor~~

4. Reciprocal Arrangement is when two enterprises mutually agree to provide back to each other. It should be ensure that either enterprise has sufficient capacity.

(4)

Best practices of Green IT →

1. Use LCD in place of CRT (Cathode Ray Display) for conserving energy.
2. Minimise the use of paper & properly recycle paper.
3. Dispose off e-waste as per the guidelines of local authorities.
4. Use laptops or palmtops in place of typical Desktop for conserving energy.
5. Try to do computer related tasks in unambiguous, leaving computer off other time.
6. Power Up & Power down energy consumption resources, like laser printers, when not in use.

(2)

4.

Implications of Information Systems are-

1. It helps managers in effective decision making for achieving strategic goals.
 2. Enterprise is able to survive & thrive in competitive environment because of its well defined information system.
 3. Information system helps managers to take right decision on right time i.e. just on time.
 4. A good information system can generate innovative ideas to help in decision making.
 5. Information gained by manager can be use in critical situations.
 6. Information system is a process, it can be integrated with strategy to form action.
- (5)

Tasks undertake to ensure
DCM programme is in place
are →

1. Assess the critical activities that will effect the enterprise.
 2. Assess the impact of disruption on the functioning of ~~critical and~~ critical activities & its magnitude.
 3. ~~Assess~~ Identify the "Pain Threshold" i.e. the ~~enterprise~~ time during which enterprise can survive without accoring to critical functions.
- (2)

1. Confidentiality :- It refers to unauthorized modification of data. As information are put on cloud it is subjected to risk. We can overcome from this by encrypting the data & isolating the system.
2. Availability :- Availability refers to unauthorized withholding of data. Availability should be considered to ensure Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP) operates effectively. Availability is critical. As one of the organisation AWS's ~~server~~ server goes down for several hrs.
3. Privacy :- Privacy is embedded in each phase of cloud computing. There should be ensure legal compliance & building trust. Privacy should be considered in cloud computing to reduce project risk.

4. Data Theft Stealing :- Both public & private can be access the data on cloud. Sometime cloud provider hires database from some other organisations, in this situation chances of data stealing ~~will~~ is higher.

5. Application Risk :- Risk associated with application not decreases when application moves to cloud. Cloud service provider should have access to ~~monitor~~ of database to monitor ~~application~~ application & correct if something wrong in application.

(4)

Q. 61)

Following are the ways →

- 1) Remote access to computer & data across network should be implemented.
- 2) Terminal Lock ✓ can ensure physical security to the same extent.
- 3) Applications & operations which can remotely access via modem & other devices should monitor frequently ✓
- 4) To protect the unauthorised access to system, proper control mechanism should be placed at system documentation & manual.
- 5) Data communication between remote location, sender of the data should attach some informatⁿ so that receiver ~~the can~~ can know the genuineness of information.
- 6) Replicated copies at remote location should be controlled & it should be ensured the both data ~~to~~ are identical.

Q 6 (c)

- ⇒ Business Manager should possess the following knowledge →
1. Foundation Concept :- He should know what is the Foundation of Informatic System.
 2. Information Technologies :- He should have knowledge of various technologies, its benefits & weaknesses.
 3. Business Application :- He should know what application support the business.
 4. Development :- He should involve in development process of informatic system.
 5. Management Position :- He should have knowledge regarding the Management position.

(3)



Addl. Book No. 1

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA
ADDL. BOOK

DO NOT WRITE ROLL NUMBER ANYWHERE IN THIS
ADDITIONAL ANSWER BOOK

Q.6(a)

Key Management practices are

- 1) Overall Management direction :-
Get the informed of various business processes, external & internal environment (including technical, etc. technical, social etc)
- 2) Assess enterprise environment, capacity & competence :- Assess enterprise capacity so that corrective actions can be implemented for improving from deficiencies.
3. Conduct Gap vs Analysis.
Conduct Gap vs analysis to know the gap between existing & target computing environment.

4. Define Target Capabilities
Define target capabilities on the basis of business process, environment & gap analysis.
5. Define Strategic Plan & Road Map :- Define the plan to align IT strategy with enterprise strategy & prepare a road map.
6. Communication of Strategy & direction :-
Communicate strategies & direction to stakeholders so they can aware of enterprise's position.

(4)

Major Boundary Controls techniques are.

1. Cryptology. → It is a technique of transforming basic data in another form of data. To decipher a text a password is required. Strength of cryptology depends upon the time to decipher the text. Sender cipher the text which can decipher by receiver if he has ^{valid} authority.
- 2.) Password. Passwords are like name, date of birth, account numbers. Passwords in combination with identification cards can be a strong boundary ctrl. Use of common dictionary words should be avoided, number of wrong attempts etc.
3. PIN. → PIN (Personal identifi. number) can be assigned to individual to gain the access. PIN are ~~genero~~ random number generated from database.

4) Identification Badges :-
These are the badges which
can information of users.
They can be use as broadband
connects.

5) Biometrics :- Use of body's
part like voice, retina,
finger print etc.

(4)

