



Book No. 1 (containing 36 pages)

**THE INSTITUTE OF CHARTERED
ACCOUNTANTS OF INDIA**

C.A - Final

Examination

Group No. *II* Paper No. *6*

Subject *ISCA*

Number of Answer Books used.....

For use by ICAI only

383690



17 NOV 2014

400270-46118

Q. No.	Please put ✓ against the Questions answered	Marks Awarded (to be filled by Examiner)					Total
		a	b	c	d	e	
1	✓	0	0	0	2		2
2	✓	2	1	0			3
3	✓	0	3	2			5
4	✓	3	2	0			5
5	✓	1	0	1			2
6							
7	✓	0	1	2	0	3	
8							
9							
10							
Total							20

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

020

0 1 2 3 4 5 6 7 8 9

Total Marks awarded (in words)

Twenty

Examiner's

Checked
(initial of the)

INSTRUCTIONS TO THE CANDIDATE

Answers are not to be written on this page

Roll 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"

Following data integrity policies we will suggest:-

1) ~~Valid Signature Updation~~ :-

1) Automatic Valid Signature Updation :- When the software are purchased from the Vendors, it should have capacity to automatically update It itself.

2. System Testing :- System has to thoroughly test before its implement.

3. Store backups to offsites :- After a some period backup data should be shifted to some offsite.

4. Quarterly or Monthly Backup :- Take the quarterly or monthly backup in addition to regular backup to secure the integrity data integrity.

5. Recovery Tasks :- There should have recovery planning or task which.

can invoke in case of
data loss, to secure the
data integrity.

0

ICAI

5 Q1(b)

The following categories of test are performed ~~for~~ by programmer.

1. Structural test.
2. Performance test.
3. Stress test.
4. Functional Test
5. Operational Test.
6. Durability Test.

0

ICAI

Critical controls required in a computerized environment are-

1. Control regarding the use of environmental protecting equipment. The use of these equipment must be restricted to authorized users only.
2. Controls regarding consumables eatables ~~consumable~~ eating should be prohibited in computerized environment.
3. Controls regarding Fire Extinguisher / water detector / fire suppression system.
4. Employees are aware about these ~~set~~ equipment & how to use these equipment.

0

✓

Recommendations for efficient use of computer ----- Green Computing -----

1. Use LCD display in place of CRT (i.e. use Liquid Crystal display in place of Cathode Ray Tube).
2. Minimum use of paper & proper recycling of wastage.
3. Dispose off e-waste as per local rules & regulations.
4. Do the work ~~on~~ with computer when you are using it don't put it idle.
5. Use of laptops in place of desktop.
6. Use power saving measures to keep control on power use by computer equipment.
7. Put off the computer & systems when not in use.
8. Use latest technology inbuilt equipment such as laser printers which consume less power.

②

Q2(q) 8

Relevant Requirement with respect to annual system mandated by SEBI are -

System Audit:-

1. Every depository / stock exchange have require to audit its Books of Accounts as per guidelines terms of Reference (TOR) & Framework issued by SEBI
2. Depository can negotiate Board of directors shall ask for proposals from auditors. Auditors proposal shall be submit to SEBI.
3. Audit schedule have to be submitted before 2 months from starting the audit. They also have to submit the scope of audit to SEBI.
4. SEBI can extend the scope of audit on the basis of previous audit requirement.

or if any ~~discrepancies~~ discrepancies found in previous audit.

5. Auditor shall submit the audit report with its observation or Non-Conformities on some ~~given~~ activities to Depository & SEBI.

6. Depository have to reply to SEBI within ~~3 months~~ on Non-Conformities or with 3 months for each non-conformity.

2

Q.2 (b)

Pertinent objectives are-

1. Service as pay-per-use :-
Cloud computing provides various facilities on the network, in case of Service Level Agreement, the user & provider need to clearly define the services will be provided. Application Program Interface can be ~~providing~~ provided to the user so that he can access from anywhere by using this interface.
2. Maintenance :- Maintenance of ~~clouding~~ cloud computing is very easy, as cloud computing need not ~~to~~ install in every computer & it can access from anywhere.
3. Cloud ~~so~~ computing enable storage devices to maximum utilisation of application by migrating from one place to another.

4. High reliability & scalability :-
To cloud computing providing
various services with consistent
reliability & scalability as there are
minimum chance of system failure.

~~5. Compliance of legislative & legal~~
5. Easy compliance with legislative
& legal regulations.

6. Agility :-

L

ICAI

The following risks will be reviewed -

1. Risk for ^{not} attaining the desired objective.
2. Risk regarding system processes produce reliable, accurate & consistent information.
3. Risk regarding # that is the system is working as planned or it deviates.

3

Operating System Security :-

Security of operating system is very essential for overall informatⁿ system. If intruder able to crack the network security, it is last security which will stop him from unauthorised ~~access~~ access. Following security measures can be used to protect Operating System.

1. Identification of User.
2. Automatic identification of terminal.
3. Terminal log on procedures.
4. Password management system.
5. Automatic terminal log out.

User can access various applications because of Operating System. Operating system enables user to perform various tasks & to use various applications. From the above importance of Operating System there will may happen an unauthorised

access of data / stealing of data etc.

- 1.) Vulnerability :- It is an weakness in system which can be exploits to gain the unauthorised access. Vulnerability may be in system, its sub components, its design. In brief vulnerability allow the user to conduct unauthorized operations.
2. Threat :- It is a condition or event that have a capability to destroy, alter, steal the information. Asset, is anything which have value to organization. Threat is exist ~~to~~ because of asset. If there is no asset, no threat threat will be there. They are inter connected with each other.

- 3- Risk $\Rightarrow$ Risk is the probability of loss that may materialise if particular vulnerability exploits. Risk assessment is necessary to be done to identify the various risk attached to the system & the ~~same~~ respective remedial ~~measures~~ means to eliminate or reduce it.

L

ICAI

Types of Backup:->

1. Full Backup:- In this type of backup all the files in the folder will be copied to hard disk, floppy disk etc. It is economically & practically very less used as it requires ~~high~~ involves sufficient cost & high cost & sufficient time.

2. Incremental:- Back up of those files that have created or changed from the last backup. The files which changed or created will be backed up regardless of backup type.

To restore this type of backup, first we have to install the full backup & then this backup.

It is economically viable as it uses very less storage / cost & less time.

3. Differential Backup:- In this type of backup, file & folder ~~will be~~ which changes from last full backup will be ~~be~~ copied.

This type of backup also require two steps to ~~get~~ restore it. First restore the original backup & then restore the differenced backup.

4. Mirror Backup:- It is just like full Backup but with two exceptions. 1st backed up files are not compressed in zip file & there is no facility of protection with password.

2

Design of Database:-

Design of database ~~will~~ should be such that it will fulfill the user needs & objectives of system development. Design should be such that it can ~~create~~ facilitate easy access of data to users. When designing the database the System Developers can choose design from various alternatives which is best suitable for system as well as database.

3

Risk related to use of PC's are-

1. PC's are small equipment/system which can easily move from one place to another which increase the risk.
2. Pen drives are the small equipment which may contain sensitive information. As Pen drives can also be movable from one place to another. Now a day even hard disk can also be moved.
3. PC's are small system which don't have inbuilt data protection application which ~~enables~~ can enforce security PC's from malware, viruses, unauthorized access.
4. Segregation of duty not possible because of lower number of staff.
5. Because of no. of installations,

at different locations
information leakage can be
possible.

6. Inadequate awareness & staff training.
7. Log-on Access Control is. PCs don't have inbuilt log on applications. But now a day ~~log on~~ then applications have been developed. but there application activated only after system is activated & ~~booted~~ from hard disk.

There are other control application also which prohibits the use of USB ports from unauthorized access.

- Security Measures are-
1. Purchase software from registered dealer only.
 2. Use only updated antivirus.
 3. Thoroughly tested before ~~implemented~~ implementation.

IT Governance: IT governance is sub part of corporate governance. & it implement the necessary framework as per objectives of Corporate governance. firstly it identifies the requirement of corporate governance & then it uses various principles, procedures, guidelines & method to achieve it.

Benefits of IT Governance:

1. It provides consistent approach, integrated & align with enterprise corporate governance approach.
2. It verifies whether IT related decision are in line with enterprise corporate objective.
3. Facilitates

0

✓

IT Governance :- IT governance refers to evaluating the ~~corporate~~ stakeholder need, expectation from IT perspectives. Converting these needs into enterprise goals & try to achieve them. Moral behaviour in IT departments ~~from~~ for completion of enterprise's objective. IT governance now a days is very popular because everything is surrounded by IT.

Objectives of IT Governance are

1. For compliance with legal & legislative regulation.
2. Improve user satisfaction through IT services.
3. Better cost benefit of IT services.

(R)

Output controls required to be reviewed are-

1. Logging of sensitive forms & information is Sensitive forms & information must be stored & logged so that unauthorised action against them can be prevented.
2. Logging of output programme execution is Logging of those programme which creates the output is necessary to prevent from ~~unauthorised~~ unauthorised changes in programme.
3. Training to employees regarding printing :- Proper training must be given to employees on which printer they have to proceed. Otherwise employees may print to another printer, of which, he don't know the location or he needs some time to reach there. In between, several copies of such printed output can

be taken.

4. Print distribution & Collection of Reports
 When distribution of some important / sensitive information takes place, it should be directly delivered to person who is authorized to receive.

In case of collection of reports, authorized person must reach at such place in time otherwise someone may make copy of it.

5. Data Retention Control :-
 Data retention refers to time for which data has to store. In various situation unnecessary data retention will raise the chances of unauthorized access to such information. Data should be retain for a particular time period after which it has to destroy.

6. Spooling is In short Spool is Simultaneous Peripheral Operatⁿ Online is technique ~~who~~ through which data can be accessed. It is ~~a~~ a technique of through which user continue to do work while he is printing. ~~Printing~~ The instructions for printing have to wait for clearance for such time it will store in some device, by spooling technique these data can be accessed. ~~can~~

3
/

Four Phases of ISMS prescribed by ISO 27001 are -

1. Plan Phase :- In this planning is done & a plan will prepare for securing the information system.
2. Do Phase :- In this phase whatever has planned in the above phase will do practically.
3. Check Phase :- This phase checks whether there is any ~~discrepancy~~ discrepancies arise in function as per plan & what has done actually.
4. The Act Phase :- Whatever has explained in above three phases this phase will do it.

2

✓

5

Expert System is Expert system is a system which have like capabilities of decision maker. It enables to answer the problems like a human being. It will ask few questions regarding problem to be solve. Like problems related to investment, it will ask, how much you would invest, fixed or floating income etc. & on the basis of the conditions it will provide a solution on how much you should invest, what you will ~~earn~~ earn, type of income fixed & floating etc.

Properties that potential application should possess are:-

1. It possess knowledge of various human being, their judgement, their experience.
2. It should have the capacity to hold such data (information).

3. ~~It is able to provide requis-~~
~~ite~~

1. Human Resource: In this application expert system stores the data regarding its qualification & recommend which job is suitable to its profile.

2. Production: At what level production will be optimise & profit also. To fix the inventory level.

3. Marketing: It helps in raising the no. of customers.

Repercussions of Cyber Fraud are as follows :->

1. Cost of data Abuse.
2. Cost of computer error.
3. Loss of sensitive & credible information.
4. Blackmailing.
5. Loss of computer, hardware & software.
6. Loss of Credibility or Competitive Strength.

0/

The matters to be verified while auditing the BCP program are -

1. Evacuation procedure, Emergency Plan & Contingency Plan.
2. Proper fire extinguisher or fire suppression system are addressed in such programme.
3. Is the BCP solution ~~not~~ are effective as per risk faced by organisation?
4. ~~Steps~~ Are proper BCP plan, procedures are identified in BCP programme?
5. Is BCP programme is prepared in a line with achieving Business objectives
6. Awareness & training programme are conducted to aware employees ~~from~~ the regarding use of their equipment.

7. BCP programme is prepared by keeping in any various risk attached to the organisation & the impact on organisation.
8. BCP programme should be authorised by senior level management.
9. Is BCP programme includes any any Back up procedure or restore procedure.

✓

(2)

Key Management practices are -

1. Scope's first determines the scope of internal control.
2. Identify the personnel involve in Internal control & their capabilities.
3. Identify ^{which type of} ~~whether~~ internal control is sufficient for such type of organization.
4. Whether Internal control have any support from Top level management.
5. Run the test approach & compare whether systems generate the ~~same~~ same result or not. If there is ^{any} deviations means Internal control is not proper.

⑥ Identify the risk faced by the organization.

ICAI



ICAI

ICAI

Virus Sign Ordal
Software testing
Offshore Back
Chaid was orkan
Recovery, tasks.

ICAI