DO NOT WRITE ANYTHING HERE

H PAPER IS ON THE
ULTIMATE PAGE

o. 1 (containing 28 pages)

NSTITUTE OF CHARTERED
CCOUNTANTS OF INDIA

CA Final Examination

No. II Paper No. VII

: ISCA

er of Answer Books used : Main + 0 additional sheets

For use by ICAI only

183763

INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA
November 2018

13 NOV 2018

80608861-1057

O.	To be ticked (✓) by the candidate against the Questions answered	Marks Awarded (to be filled by Examiner) a	b	c	d	e	Total
	✓		4	1	4		9
	✓	1	5	3			9
	✓	0	5	4			9
	✓	3	3	2			8
6	✓	4	4	0			8
7	✓	4		4	0	3	11
8							
9							
10							
otal							54

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

5 4

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

otal Marks awarded (in words) Fifty four

Examiner's Signature

DO NOT WRITE ANYTHING HERE

STRUCTIONS TO THE CANDIDATE

swers are not to be written on this page

d be written in figures and words in the allotted space at the right hand corner of the and nowhere else including additional answer book/s and graph paper.

should be written in the box in numbers and darken the appropriate circles of the OMR rovided in the right hand corner of the cover page with **Black / Blue** ball point pen.

articulars such as name of Examination, Group No., Paper No. and subject at the appropriate space he left hand upper corner.

4. Remove the 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"

10. Before submission of answer book to the invigilator after completion of the exam, take care to score out (X) blank pages, if any, that you might have left.

Q.3 (a)

Types of Cyber Frauds :-

1. **Financial losses :-**
Hackers may steal the confidential information of orginaziation, which will lead to financial losses.

2. **Legal liabilities :-**
organizations may have to face legal consequences due to cyber frauds

3. **Loss of competitive edge :-**
Due to fraud happened in an organization, the impact of which can lead to destruction of reputation & loss of competitive edge.

4. **Disclosure of confidential / sensitive information :-**
Hackers, after stealing the information, can publish/ disclose the confidential and sensitive information of organization.

5. **Blackmail :-**
Cyber attacks can also result in blackmail & organization will have to face financial crisis because of this.

6. **Sabotage :-**

(1) The objective of Sabotage is not to obtain money but to spoil reputation of entity

Q.3 (b) Following are the objectives of Information Technology Act, 2000 :-

- To grant legal recognition to transactions carried out by means of Electronic Data interchange.
- To give legal sanction to digital signature.
- To give legal sanction to electronic fund transfers between banks and financial institutions.
- To facilitate electronic storage of data.
- To facilitate electronic filing of documents with Government departments.
- To amend Indian penal code, Indian evidence Act, 1872 & RBI Act, 1934.

(5)

Q.3 (c) Ways in ~~syste~~ which system Maintenance can be categorized :-

1. Schedule maintenance :-
The maintenance process should be scheduled so as to avoid any unexpected failure of system.

2. Corrective Maintenance :-
After indulgement of any issue in system, corrective maintenance helps to solve the ~~same~~ in a quick and efficient manner.

3. Preventive Maintenance :-
This type of maintenance helps to prevent the issues in an advanced manner thereby avoiding any future downtime of system.

4. Adaptive maintenance :-
Adaptive maintenance helps the systems to adopt any frequent changes in environment, technologies, etc.

3

5. Rescue maintenance :-
It helps to save the system from unexpected critical issues.

DO NOT WRITE ANYTHING HERE

Q-5 (a) Key management practices for assessing and evaluating the system of Internal Controls in an enterprise :-

- Initially, Scope may be framed by Scope assurance Initiative.
- After framing the scope, the ~~execution~~ planning element is decided by Plan assurance initiative.
- Execution of Scope and plan may be done by Execute Assurance initiative.
- It should be ensured that assurance providers are qualified and independent.
- The Internal Control of an organization should be thoroughly reviewed by exercising due professional care.
- Auditor, after reviewing Internal Control, should report Control deficiency.

(3)

Q.5 (b) Characteristics required for a good coded programme / application software :-

1. Usability :-
The usability of a coded application software must be identified and communicated and the same should be easy to understand.

2. Readability :-
Coded application software must be easy to read and make conclusions.

3. Reliability :-
Data and information possessed by coded application software must be from reliable sources.

4. Efficiency :-
The programme should be efficient so as to undertake critical functions during system development phase.

5. Accuracy :-
Data, information and process flow of programme should be accurate.

(3 6.) Robustness :-
Application software should be made robust so as to avoid any inherent limitations.

Q5 (C)

Advantages of private cloud :-

- Security level is highest in private cloud as compared to public, hybrid or community cloud.

- Service level Agreement (SLA) is very strong in private cloud.

Q

Advantages of public cloud :-

- Cost of public cloud services is very much cheap as compared to other cloud service because of its multi-sharing feature.

2- Scalability is very high in public cloud services.

(2)

Q.6 (a)

Factors influencing on organization towards control and audit of computers and the impact of the Information Systems :-

1. **Data loss :-**
Organizations face the need for control and audit due to its most sensitive and confidential part - Data. Loss of data can lead to destruction of reputation, finance, etc. factors.

2. **Incorrect decision making :-**
The decision making process should be accurate & reliable. Incorrect decision making generates the need for control and audit.

3. **Computer Abuse :-**
Few inherent limitations of using computers are reasons of control and audit.

4. **Software and hardware resources :-**
Organizations maintain sufficient software and hardware resources therefore the security and safety of the same is of top priority which leads to need of audit of those resources.

5. System effectiveness :-
To ensure system effectiveness, periodic verification and testing is required of computer systems.

6. System efficiency :-
Keeping control and having audited the computer systems make those systems work in an efficient manner.

(4)

Q.6 (b)

Following issues must be covered in the contract if company uses a third party site for backup and recovery process :-

- How soon the site will be made available in the event of disaster.
- The period for which site will be made available.
- Conditions under which site can be used by the organization.
- How the site will be made available if two or more organizations have to use the site concurrently in the event of disaster.

- Clear-cut understanding of Backup and recovery process should be obtained.

- Any other pre-requisites that should be known to the organization before entering into contract with provider of this kind of services.

4

0.6
CO

Asynchronous attack :-
These type of attacks affect the systems in a way not known to the organization and which may lead to critical loss to the organization.

The Subversive Threats to an Information Systems are as follows :-

1. Wire-tapping :-
The information can be stolen by tapping the physical wire through which data is transmitted online and electronically.

2. Data-leakage :-
Inadequate security, absence of updated antivirus, etc factors are responsible for threat of data leakage.

3. Denial of Service :-
Service providers sometimes deny the provision because of less secure cyber systems thereby affecting the chain data transmission in an information system.

4. Piggy - backing :-
Information systems are vulnerable to the threat of piggy - backing from outsiders.

Q.7 (a) Benefits of Expert System :-

- Expert systems preserve knowledge that might be lost due to death, resignation of employees.

- Expert system keeps information in an active form.

- Expert system assists novice in thinking.

- Expert systems are not subject to Human fallings.

(4)

Q.7 (c) Advantages of BYOD :-

1. Happy employees :-
Because of using their own devices in the environment of organization, employees feel good during working hours.

2. Lower IT budgets :-
Since the organizations don't have to incur much cost in purchasing electronic devices, the budget for information technology keeps low.

3. Reduced IT support requirement :-
The back-end support that should be provided to employees in relation to IT is becoming much lower after introduction of Bring your Own device (BYOD) concept.

4. Early adoption of new technologies :-
Employees can adopt the changes in technologies very much speedily. Therefore the latest technologies are rapidly adopted across the organization.

5. Increased Employee Efficiency :-
The employees can work in a more effective and efficient ways because of working with their own familiar devices thereby increasing employee efficiency.

(4)

0.7
(d)

Role of IS auditor in physical Access Control :-

- IS Auditor should verify the security whether it is secured by Personal Identification Number (PIN)
- whether the password protection is in place to ensure security.

- Whether cryptosystem / cryptography system is in place.
- Lastly, auditor should check whether Biometric devices are installed since they provide highest level of security.

(6)

Q.7 (e)

Limitations of Management Information Systems :-

- Quality of output of MIS depends upon the quality of inputs and processes.
- Traditional limitation of Transaction processing systems (TPS) still exists in MIS.
- MIS is less useful for solving the unstructured problems.
- If culture is of hoarding information, MIS becomes ineffective.
- If management of the entity changes, MIS becomes ineffective.

(3)

Q.4 (a) Electronic signature, as per IT Act, 2000, means a digital online signature which provides a high level of safety and security to signature transactions. Electronic signature can be considered reliable if,

- Types of electronic signatures are specified
- The manner and format in which electronic signature shall be affixed is specified.
- Control procedures and processes are identified to ensure confidentiality, integrity and security.
- Other relevant matters are specified to give legal effect to electronic signature.

Q.4 (b) Key management practices for aligning IT strategy with Enterprise Strategy :-

1. Understand Enterprise Direction :-
The first and foremost step to align IT strategy with Enterprise Strategy is to understand and have a good knowledge of Enterprise direction.

2. Assess Current Environment :-
Auditor should assess the current

environment of the organization to set the future goals and corresponding requirements.

3. Define target IT capabilities :-
Target Information technology requirements and capabilities should be set and thoroughly understood to avoid any misconception in execution.

4. Conduct gap analysis :-
The limitations and difficulties that may arise during execution should be identified by conducting gap analysis.

5. Define strategy plan and roadmap :-
How to execute the plan should be framed by defining strategy plan and roadmap thereby avoiding any pitfalls in future.

6. Communicate to stakeholders :-

The defined strategy plan and roadmap must be communicated to the stakeholders of the organization so as to ensure the accuracy of plan

of aligning IT strategy with business strategy. (5)

Q.4 (c)

Important characteristics of Computer Based Information systems (CBIS) :-

- Every system works with a sub-system & therefore no system works in isolation.
- Systems and sub-systems perform interactions. They are called interfaces.
- If one sub system fails, entire System may fail.
- Every sub-system must follow the goal set by main system. Therefore, the goal of individual sub system is of lower priority than the goal set by entire System.

(4)

Q-1 (b) Means of achieving Network Access Controls :-

1. Firewall :-
Implementing latest firewall helps in maintaining a robust control during access to computer network.

2. Encryption :-
Data and information kept in computer system should be encrypted at any point of time so as to prevent any unauthorized access to the same.

3. Call-back devices :-
If any communication is interrupted or avoided to be handled, Call back devices help to assure whether the communication is in a secure manner and through a secured gateway.

4. Recording transaction logs :-
Transactions which are being passed through network of device must be recorded in detail. This may help in resolving any future contingencies and issues.

5. Updated antivirus :-
Antivirus implemented in the organization on a periodic basis thereby securing the overall transmission of data and information through Internet and Intranet. (4)

8-1
(c)
(i) The enterprise uses Training process as a tool to initiate a culture of Bcm in all the stakeholders because the training process provides a nimble source of understanding to have a good knowledge and idea as to why an organization should implement Business Continuity Management (BCM) culture.

Moreover, to improve its IS performance and availability of services, to minimize its loss in terms of revenue loss, loss of reputation and to improve customer satisfaction, organizations must initiate a culture of Bcm by providing training.

(ii) The supports which are needed for the development of a Bcm culture :-

- Incident management plan (IMP) and

Business continuity plans (BCP) are required to support BCM culture.

- The processes related to BCM collection of information, strategy, development and implementation, training, maintenance, testing should be clearly understood to develop a BCM culture.

Q-1
(d) The types of information that can be collected by System control Audit Review file (SCARF) are explained below :-

1. Statistical Samples :-
SCARF helps in providing the statistical samples thereby providing continuous assurance about the population of data and reports.

2. System Exceptions :-
Exception reports can be generated to monitor periodically the processing of transactions through system network.

3. Snapshots / Extended records :-
Snapshots which are inbuilt in system provides a great source of collecting the rare information.

4. Profiling data :-
SCARF helps to profile the data
arranging the data in a structur
manner so as to make easy the
collection process.

5. Performance Measurement :-
Analysis and measurment of syste
performance can be identified easi
with utmost accuracy by using S
technique as a continuous auditi
technique.

6. Policy and procedure Variance :-
Data related to variances i.e. diffe
identified between policy and act
implementation thereof can be obtai
with the aid of SCARF technique.

(4)

DO NOT WRITE ANYTHING HERE

DO NOT WRITE ANYTHING HERE

DO NOT WRITE ANYTHING HERE