

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

ISCA-2

Answer **all** questions.

Each question carries 20 marks.

Marks

- 1)
- a) Explain the following terms :
- i) Preventive controls
 - ii) Detective controls
 - iii) Corrective controls
 - iv) Compensatory controls
- 2.5x4=10
- b) "Decision support systems are widely used as part of an organisation's AIS". Give examples to support this statement. 5
- c) Describe the audit tools for a disaster recovery testing. 5
- 2)
- a) As an internal auditor of an enterprise, which has acquired and implemented an ERP system in its headquarters and five regional branch offices, how will you perform the testing of general and automated controls on the following issues:
- [i] The flow of data and information between the headquarters and the five branch offices,
 [ii] The concurrent usage of 1000 employees on an average across the offices at anytime,
 [iii] The data processing and report generation is in tune with the management objectives.
- 4x3=12
- b) What are the Type I and Type II reports under SAS70? 8
- 3)
- a) How does one assess insurance coverage? 5
- b) What are the four domains identified under COBIT for high level classification.?can you establish their inter-relationship? 10
- c) Composition of cyber appellate tribunal as per section 49 of ITAA2008. 5

4)



- a) Explain the Business Process Reengineering [BPR] process along with business management [BE] concept. 10
- b) You are to conduct an IS audit for an organisation. Identify what all you would include in the audit plan ? 5
- c) Explain the following definitions as per ITAA-2008:
- i) Affixing electronic signature
 - ii) Intermediary
 - iii) Cyber cafe
 - iv) Computer network
 - v) Communication device

1x5=5

5)

- a) Preparation of RFP
- b) What is a data flow diagram[DFD]? Give an example of DFD.
- c) What is a data dictionary? What are its uses?
- d) Explain the RAD [Rapid Application Development] approach .

5x4=20

 All the best 

SUGGESTED ANSWERS / HINTS

1)

a) Chap -3. Explain the following terms :

- i) Preventive controls
- ii) Detective controls
- iii) Corrective controls
- iv) Compensatory controls

2.5x4=10

b) chap- 1 ."Decision support systems are widely used as part of an organisation's AIS".

Give examples to support this statement.

5

c) chap -6. Describe the audit tools for a disaster recovery testing.

5

2)

a) Chap -4 To test the flow of data and information between the headquarters and the five branch offices where an enterprise-wide application is implemented to process the business cycle, the testing method used is called the **Inter System Testing**.

This test method ensures that the data flow and interconnection between the application systems function correctly.

The objectives of this test are:

- Proper parameters and data are correctly passed between the applications
- Documentation for involved system is correct and accurate.
- Proper timing and coordination of functions exists between the application systems.

The method of testing involves:

- Operations of multiple systems are tested.
- Multiple systems are run from one another to check that they are acceptable

and processed properly.

- The testing also ensures synchronization when there is a change in the parameters of the application system.
- The parameters, which are erroneous and the risk associated to such parameters decide the extent of testing and type of testing.
- Intersystem parameters are checked and verified after the change or when a new application is placed in the production.

(b) To test if concurrent usage of 1000 employees on an average across the offices at anytime is feasible on the implemented ERP system, the **Volume testing method** is followed.

The test method checks the behaviour of the enterprise-wide system when the maximum number of users are logged concurrently and when the database contains the greatest data volume.

This test method involves:

- Creation of a large volume test environment.
- It tests the level of complexity in terms of the data within the database and the range of transactions and data used by the users.
- The test tries to reliably reflect the production environment.
- Volume tests offer much more than simple service delivery measurement.

The test answers the following questions:

- What service level can be guaranteed? How can it be specified and monitored?
- Are changes in user behaviour likely? What impact will such changes have on resource consumption and service delivery?
- Which transactions/processes is resource hungry in relation to their tasks?
- What are the resource bottlenecks? Can they be addressed?
- How much spare capacity is there?
- The volume testing brings out the weaknesses in the system with respect to its handling of large amount of data during extended time periods

(c) **Control testing**, ensures if the data processed and report generation done by the implemented ERP is in tune with the management objectives. It is a management tool to ensure that processing is performed in accordance to management desires or intent. This testing method is used in parallel with the other system tests.

The testing ensures that:

- the data is accurate and complete.
- the transactions are authorized.
- there is adequate maintenance of audit trail information.
- the data processing facilities are efficient, effective and economical.
- the processing tasks meet the needs of the user.

In performing the control testing:

- the system risks are identified.
- the testers determine or anticipate what can go wrong in the application system with a negative approach.
- the risk matrix is developed to identify the risks, controls; segments within Application system in which control resides.

12

b) What are the Type I and Type II reports under SAS70?

8

3)

a) Chap -5 How does one assess insurance coverage?

5

b) Chap -8 What are the four domains identified under COBIT for high level classification.?can you establish their inter-relationship?

10

c) Chap-10 Composition of cyber appeallate tribunal as per section 49 of ITAA2008

5

4)

a) Chap -7. Explain the Business Process Reengineering [BPR] process along with business management [BE] concept.

10

b) Chap -9 .You are to conduct an IS audit for an organisation. Identify what all you would include in the audit plan ?

5

c) Chap -10 Explain the following definitions as per ITAA-2008:

5

5)

- a) Chap-2 Preparation of RFP
- b) Chap-2 What is a data flow diagram[DFD]? Give an example of DFD.
- c) Chap-2 What is a data dictionary? What are its uses?
- d) Chap-2 Explain the RAD [Rapid Application Development] approach .

😊 GOOD LUCK 😊

5x4=20