FINAL – November 2017

INFORMATION SYSTEMS CONTROL AND AUDIT

Test Code – FNJ 0012
Branch (MULTIPLE) (Date : 11.06.2017)

(50 Marks)

Note: All questions are compulsory.

Answer 1 (5 Marks)

The principles to guide the design of measures and indicators to be included in an EIS are given as follows:

- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.**(1 Mark)**
- EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service. **(1 Mark)**
- Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers. **(1 Mark)**
- EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff, people feel that they, as individuals, can contribute to improving the performance of the organization. **(1 Mark)**
- EIS information must be available in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential be part of EIS. **(1/2 Mark)**
- EIS measures must evolve to meet the changing needs of the organization. **(1/2 Mark)**

Answer 2 (5 Marks)

Expert System: An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in investment portfolio management might ask its user several specific questions relating to investments for a client like – how much can be invested. Does the client have any preferences regarding specific types of securities? **(2 marks)**

Major properties that an application should possess to qualify for Expert System development are given as follows: **(3 Marks)**

- **Availability:** One or more experts can communicate 'how they go about solving the problems to which the Expert System will be applied'.
- **Complexity:** Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing
- **Domain:** The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.

- **Expertise:** Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure:** The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem -solving situation.

Answer 3 (4 Marks)

The main characteristics of the corrective controls are given as follows:

- Minimizing the impact of the threat; **(1 mark)**
- Identifying the cause of the problem; **(1 mark)**
- Providing remedy to the problems discovered by detective controls; **(1/2 mark)**
- Getting feedback from preventive and detective controls; **(1/2 mark)**
- Correcting error arising from a problem; and **(1/2 mark)**
- Modifying processing systems to minimize future occurrences of incidents. **(1/2 mark)**

Answer 4 (6 Marks)(1 mark each)

Major Data Integrity Policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage:** Backups must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

Answer 5 (4 Marks)

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongful withdrawal of money from bank accounts.**(1 mark)**
- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These enti ties need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities. **(1 mark)**
- **Loss of credibility or Competitive Edge:** News that an organization's database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to loss of credibility. There have been instances where share prices of such companies went down, when the news of such attach percolated to the market. **(1 mark)**
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, instances of individuals leaking information about government's secret programs. **(1/2 mark)**

- **Sabotage:** The above situation may lead to misuse of such information by enemy country. **(1/2 mark)**

Answer 6 (6 Marks)(1 mark for each point)

While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:

- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.

- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.

- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.

- Define the scope of the planning effort.

- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.

- Develop a Plan Framework.

Answer 7 (5 Marks)

During a BCP/DRP Audit of Information Technology, Information Systems auditor is expected to follow these steps:

- Determine if the plan reflects the current IT environment.**(1 mark)**
- Determine if the plan includes prioritization of critical applications and systems. **(1 mark)**
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable. **(1 mark)**
- Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications? **(1 mark)**
- Is there plan for alternate means of data transmission if computer network is interrupted? Has the security of alternate methods been considered? **(1/2 mark)**
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weakness identified in the last test were corrected**. (1/2 mark)**

Answer 8 (5 Marks)

Major strengths of prototyping model are given as follows:

- It improves both user participation in system development and communication among project stakeholders.**(1 Mark)**
- It is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface. **(1/2 Mark)**
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed. **(1/2 Mark)**
- It helps to easily identify, confusing or difficult functions and missing functionality. It enables to generate specifications for a production application. **(1/2 Mark)**
- It encourages innovation and flexible designs . **(1/2 Mark)**
- It provides for quick implementation of an incomplete, but functional, application. **(1/2 Mark)**
- It typically results in a better definition of users' needs and requirements than traditional systems development approach. **(1/2 Mark)**
- A very short time is normally required to develop and start experimenting with a prototype. This short period allows system users to immediately evaluate proposed system changes. **(1/2 Mark)**
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. Thus, the information system ultimately implemented should be more reliable and less costly to develop than when traditional systems development approach is employed. **(1/2 Mark)**

Answer 9 (5 Marks)(1 Mark for each point)

Major aspects that need to be kept in mind while eliciting information to delineate scope are given as follows:

- Different users may represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project (alternately called champion or executive sponsor of the project). Addressing his concerns should be the basis of the scope.
- While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
- While presenting the proposed solution for a problem, the development organization must clearly quantify the economic benefits to the user organization. The information required must be gathered at this stage. For example, when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.

- It is also necessary to understand the impact of the solution on the organization - its structure, roles and responsibilities. Solutions, which have a wide impact, are likely to be met with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle it may have a very poor ERP implementation record with disastrous consequences.
- While economic benefit is a critical consideration when deciding on a solution, there are several other factors that must be given weightage too. These factors are to be considered from the perspective of user management and resolved. For example, in a security system, how foolproof it is, may be a critical factor.

Answer 10 (5 Marks)

Maintaining the system is an important aspect of System Development. Maintenance can be categorized in the following ways:

- Scheduled Maintenance: Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- Rescue Maintenance: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- Corrective Maintenance: Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- Adaptive Maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating sys tem. The term environment refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- Perfective Maintenance: Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- Preventive Maintenance: Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

****

****

FINAL – November 2017

INFORMATION SYSTEMS CONTROL AND AUDIT

Test Code – FNJ 0012
Branch (MULTIPLE) (Date : 11.06.2017)

(50 Marks)

Note: All questions are compulsory.

Answer 1 (5 Marks)

The principles to guide the design of measures and indicators to be included in an EIS are given as follows:

- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.**(1 Mark)**
- EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service. **(1 Mark)**
- Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers. **(1 Mark)**
- EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff, people feel that they, as individuals, can contribute to improving the performance of the organization. **(1 Mark)**
- EIS information must be available in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential be part of EIS. **(1/2 Mark)**
- EIS measures must evolve to meet the changing needs of the organization. **(1/2 Mark)**

Answer 2 (5 Marks)

Expert System: An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in investment portfolio management might ask its user several specific questions relating to investments for a client like – how much can be invested. Does the client have any preferences regarding specific types of securities? **(2 marks)**

Major properties that an application should possess to qualify for Expert System development are given as follows: **(3 Marks)**

- **Availability:** One or more experts can communicate 'how they go about solving the problems to which the Expert System will be applied'.
- **Complexity:** Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing
- **Domain:** The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.

- **Expertise:** Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure:** The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem -solving situation.

Answer 3 (4 Marks)

The main characteristics of the corrective controls are given as follows:

- Minimizing the impact of the threat; **(1 mark)**
- Identifying the cause of the problem; **(1 mark)**
- Providing remedy to the problems discovered by detective controls; **(1/2 mark)**
- Getting feedback from preventive and detective controls; **(1/2 mark)**
- Correcting error arising from a problem; and **(1/2 mark)**
- Modifying processing systems to minimize future occurrences of incidents. **(1/2 mark)**

Answer 4 (6 Marks)(1 mark each)

Major Data Integrity Policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage:** Backups must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

Answer 5 (4 Marks)

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongful withdrawal of money from bank accounts.**(1 mark)**
- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These enti ties need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities. **(1 mark)**
- **Loss of credibility or Competitive Edge:** News that an organization's database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to loss of credibility. There have been instances where share prices of such companies went down, when the news of such attach percolated to the market. **(1 mark)**
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, instances of individuals leaking information about government's secret programs. **(1/2 mark)**

- **Sabotage:** The above situation may lead to misuse of such information by enemy country. **(1/2 mark)**

Answer 6 (6 Marks)(1 mark for each point)

While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:

- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.

- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.

- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.

- Define the scope of the planning effort.

- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.

- Develop a Plan Framework.

Answer 7 (5 Marks)

During a BCP/DRP Audit of Information Technology, Information Systems auditor is expected to follow these steps:

- Determine if the plan reflects the current IT environment.**(1 mark)**
- Determine if the plan includes prioritization of critical applications and systems. **(1 mark)**
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable. **(1 mark)**
- Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications? **(1 mark)**
- Is there plan for alternate means of data transmission if computer network is interrupted? Has the security of alternate methods been considered? **(1/2 mark)**
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weakness identified in the last test were corrected**. (1/2 mark)**

Answer 8 (5 Marks)

Major strengths of prototyping model are given as follows:

- It improves both user participation in system development and communication among project stakeholders.**(1 Mark)**
- It is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface. **(1/2 Mark)**
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed. **(1/2 Mark)**
- It helps to easily identify, confusing or difficult functions and missing functionality. It enables to generate specifications for a production application. **(1/2 Mark)**
- It encourages innovation and flexible designs . **(1/2 Mark)**
- It provides for quick implementation of an incomplete, but functional, application. **(1/2 Mark)**
- It typically results in a better definition of users' needs and requirements than traditional systems development approach. **(1/2 Mark)**
- A very short time is normally required to develop and start experimenting with a prototype. This short period allows system users to immediately evaluate proposed system changes. **(1/2 Mark)**
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. Thus, the information system ultimately implemented should be more reliable and less costly to develop than when traditional systems development approach is employed. **(1/2 Mark)**

Answer 9 (5 Marks)(1 Mark for each point)

Major aspects that need to be kept in mind while eliciting information to delineate scope are given as follows:

- Different users may represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project (alternately called champion or executive sponsor of the project). Addressing his concerns should be the basis of the scope.
- While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
- While presenting the proposed solution for a problem, the development organization must clearly quantify the economic benefits to the user organization. The information required must be gathered at this stage. For example, when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.

- It is also necessary to understand the impact of the solution on the organization - its structure, roles and responsibilities. Solutions, which have a wide impact, are likely to be met with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle it may have a very poor ERP implementation record with disastrous consequences.
- While economic benefit is a critical consideration when deciding on a solution, there are several other factors that must be given weightage too. These factors are to be considered from the perspective of user management and resolved. For example, in a security system, how foolproof it is, may be a critical factor.

Answer 10 (5 Marks)

Maintaining the system is an important aspect of System Development. Maintenance can be categorized in the following ways:

- Scheduled Maintenance: Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- Rescue Maintenance: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- Corrective Maintenance: Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- Adaptive Maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating sys tem. The term environment refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- Perfective Maintenance: Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- Preventive Maintenance: Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

****

****