IT GOVERNANCE

Suggested Answers

July-August 2024

Answer to the Question# 1 (a):

i. Ensure availability of electricity supply all over the country according to current demand and ensure fulfilling future demand.

ii. Government funded replacement programme of conventional light with energy saving light in 10 years.

iii. Provide incentives for use of alternative energy sources such as solar, wind, bio-fuel, etc.

iv. Ensure uninterrupted power supply in Incubator/Hi-tech Park/Software Technology Park/IT Park.

v. Reduce tax on power generator, solar panel, IPS, UPS/Online UPS, battery used in IPS/UPS.

vi. Encourage private investment in power generation and provide same facilities and benefits as the govt.

vii. Encourage R&D for efficient power consumption.

viii. Minimize system loss.

ix. Introduce prepaid meter.

Answer to the Question# 1 (b):

Here are the issues in brief:

Predictive Policing

Some police departments sent officers to visit individuals identified by a computer system as likely to commit a crime, with the intent of preventing crime by providing information about job training programs or increased penalties. This practice was protested by many community groups as racial profiling.

Insurance Rates

Auto insurance companies use devices to analyze driving habits to offer better rates, but criteria such as avoiding late-night driving and short commutes can be discriminatory against poorer individuals. Predictive modeling systems that use data about buying habits and medical histories to predict life expectancy and disease likelihood can potentially affect health insurance rates.

Computerized Hiring

Companies use computerized systems to filter job applicants, potentially preventing qualified candidates from obtaining jobs based on factors like commute length. This method can be statistically accurate but raises fairness concerns.

Targeting Financially Vulnerable Individuals Data brokers sell reports highlighting financially vulnerable individuals to companies offering high-risk financial products. Few regulations exist to prevent the targeting of these groups, and privacy laws have not kept pace with big data technology.

The challenges of big data to privacy described show that technology can be a double-edged sword. It can be the source of many benefits, including the ability to combat disease and crime and to achieve major cost savings and efficiencies for business. At the same time, digital technology creates new opportunities for invading your privacy and using information that could cause you harm.

Answer to the Question# 2 (a):

Business analytics (BA) refers to the skills, technologies, applications, and practices applied to a continuous iterative exploration and investigation of a business's historical performance to gain insight and drive the strategic business planning process. Business analytics focuses on developing new insights and understanding of business performance based on data and statistical methods. In contrast, business intelligence traditionally focuses on using a consistent set of metrics to both measure past performance and guide business planning, which is also based on data and statistical methods.
Business Analytics (BA) focuses on predicting future trends and providing actionable recommendations using advanced techniques like AI and machine learning. In contrast, Business Intelligence (BI) emphasizes analyzing historical data for reporting and operational monitoring through visualization and dashboards.

Answer to the Question# 2 (b):

Cognitive science is based on research in biology, neurology, psychology, mathematics, and many allied disciplines. It focuses on researching how the human brain works and how humans think and learn. The results of such research in human information processing are the basis for the development of a variety of computer-based applications in artificial intelligence. Applications in the cognitive science area of AI include the development of expert systems and other knowledge-based systems that add a knowledge base and some reasoning capability to information systems. Also included are adaptive learning systems that can modify their behaviors on the basis of information they acquire as they operate. Chess-playing systems are primitive examples of such applications, though many more applications are being implemented. Fuzzy logic systems can process data that are incomplete or ambiguous, that is, fuzzy data. Thus, they can solve semi structured problems with incomplete knowledge by developing approximate inferences and

answers, as humans do. Neural network software can learn by processing sample problems and their solutions. As neural nets start to recognize patterns, they can begin to program themselves to solve such problems on their own. Genetic algorithm software uses Darwinian (survival of the fittest), randomizing, and other mathematics functions to simulate evolutionary processes that can generate increasingly better solutions to problems. In addition, intelligent agents use expert system and other AI technologies to serve as software surrogates for a variety of end-user applications.

Answer to the Question# 2 (c):

Transparency is maintained in blockchains via a real time view of the trades and computer coded "smart" contracts. With trade data published to a common platform, regulators or other interested parties can plug into this and get a real time view of the trades. This gives regulators oversight into one common source, rather than receiving reports in different formats at different times from each institution. The transparency offered by blockchains could help regulators detect systemic risks sooner.

Traditionally for trade payoffs, entities had to rely on heavy legal documentation, such as International Swaps and Derivatives Association (ISDA) master agreements. But computer code, by its very nature, is far more readable and predictable than legal language. By writing payoff structures onto a common platform in computer code which can be tested against, a smart contract on a blockchain provides for much higher levels of transparency over outcomes.

Non-financial parties could also stand to benefit from the transparency offered by blockchain applications as they allow multiple parties to have access to the same data, where traditionally, data held by third parties can be obfuscated or withheld.

Blockchain achieves transparency by combining decentralization, immutable ledgers, and open verification processes. This ensures that all transactions and activities are visible, trustworthy, and resistant to manipulation, fostering accountability in various applications.

Answer to the Question# 2 (d):

Crowdfunding portals can be subdivided into four further subsegments on the basis of the kind of consideration given to investors for their investments, donation-based crowdfunding, reward-based crowdfunding, crowdinvesting and crowdlending.

Investors participating in donation-based crowdfunding receive no remuneration for their contributions (though they may derive indirect personal benefits through the act of donation), in reward-based crowdfunding they receive some form of non-monetary consideration. Such consideration can take the form of the right to pre-order a product or some other form of prestige, such as having the investor's name included in the credits of a funded film. Generally, there are no costs to individuals for initiating projects in the reward-based and donation-based crowdfunding subsegments. Some portals charge a certain percentage of the fee of the total amount of funding in

the case of a successful campaign. Other portals gain revenue through voluntary donations from investors and the initiators of the projects.

In the third subsegment, crowdinvesting, investors receive a share of equity, debt or hybrid ownership. The contracts used in crowdinvesting often simulate certain aspects of equity participation using a mezzanine instrument As a rule, crowdinvesting platforms profit from the fees they receive from successfully financed companies. Recently crowdinvesting portals have also gained revenue from the future success of financed companies by requiring investors to deduct a certain share of a company's potential profits, its enterprise value and exit proceeds (carried interest).

The fourth subsegment, crowdlending, contains platforms that enable private individuals and businesses to secure loans from the crowd. In return for the provision of the loan, investors receive a pre-determined interest rate. In Germany, the market leaders in the crowdlending industry are financed by two types of fees. On the one hand, borrowers are charged a fee that depends on their creditworthiness and the duration of the loan. On the other hand, lenders are required to pay a certain percentage of the amount invested or one percentage point of the interest rate.

Answer to the Question# 3 (a):

Factor Analysis of Information Risk (FAIR) helps organizations quantify risk. The focus is on cyber security and operational risk, with the goal of making more well-informed decisions. By quantifying risks in financial terms, it empowers organizations to adopt a practical, business-focused approach to IT governance.

Answer to the Question# 3 (b):

According to transaction cost theory, firms and individuals seek to economize on transaction costs, much as they do on production costs. IT affects the cost and quality of information and changes the economics of information. Information technology helps firms contract in size because it can reduce transaction costs—the costs incurred when a firm buys on the marketplace what it cannot make itself. Using markets is expensive because of costs such as locating and communicating with distant suppliers, monitoring contract compliance, buying insurance, obtaining information on products, and so forth. Traditionally, firms have tried to reduce transaction costs through vertical integration, by getting bigger, hiring more employees, and buying their own suppliers and distributors.

Information technology, especially the use of networks, can help firms lower the cost of market participation (transaction costs), making it worthwhile for firms to contract with external suppliers instead of using internal sources. As a result, firms can shrink in size (numbers of employees) because it is far less expensive to outsource work to a competitive marketplace rather than hire employees.

Answer to the Question# 3 (c):

Here the business value chain model is helpful. The value chain model highlights specific activities in the business where competitive strategies can best be applied and where information systems are most likely to have a strategic impact. This model identifies specific, critical leverage points where a firm can use information technology most effectively to enhance its competitive position.

The value chain model views the firm as a series or chain of basic activities that add a margin of value to a firm's products or services. It focuses on analyzing internal activities identifying areas to optimize for cost reduction, quality improvement, and efficiency, thereby enhancing competitive advantage through better operational performance.

Answer to the Question# 3 (d):

Primary activities are most directly related to the production and distribution of the firm's products and services, which create value for the customer. Primary activities include inbound logistics, operations, outbound logistics, sales and marketing, and service. Inbound logistics includes receiving and storing materials for distribution to production. Operations transforms inputs into finished products. Outbound logistics entails storing and distributing finished products. Sales and marketing includes promoting and selling the firm's products. The service activity includes maintenance and repair of the firm's goods and services.

Support activities make the delivery of the primary activities possible and consist of organization infrastructure (administration and management), human resources (employee recruiting, hiring, and training), technology (improving products and the production process), and procurement (purchasing input). One can ask at each stage of the value chain, "How can we use information systems to improve operational efficiency and improve customer and supplier intimacy?" This will force one to critically examine how one performs value-adding activities at each stage and how the business processes might be improved. One can also begin to ask how information systems can be used to improve the relationship with customers and with suppliers who lie outside the firm's value chain but belong to the firm's extended value chain where they are absolutely critical to one's success. Here, supply chain management systems that coordinate the flow of resources into one's firm and customer relationship management systems that coordinate one's sales and support employees with customers are two of the most common system applications that result from a business value chain analysis.

Answer to the Question# 4 (a):

Not safe. Wi-Fi networks are susceptible to hacking by eavesdroppers. It can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae, and hacking software. Wi-Fi transmission technology was designed to make it easy for stations to find and hear one another. The service set identifiers (SSIDs) that identify the access points in a Wi-Fi network are broadcast multiple times and can be picked up fairly easily by intruders' sniffer programs. Wireless networks in many locations do not have basic protections against war driving, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic. An intruder who has associated with an access point by using the correct SSID is capable of accessing other resources on the network. For example, the intruder could use the Windows operating system to determine which other users are connected to the network, access their computer hard drives, and open or copy their files.

Answer to the Question# 4 (b):

Zero-day attack: A zero-day attack is an attack that uses a vulnerability or security hole in a computer system unknown to its owners, developers, or anyone capable of mitigating it. The term "zero-day" refers to the fact that the vendor has had zero days to address or patch the vulnerability. These types of attacks can be especially dangerous because they occur before a patch or fix is available, leaving systems vulnerable.

No, the wannaCry ransomware attack was not a zero-day attack as Microsoft released the required security patches before the attack. Users who didn't update their operating systems were responsible for the success of the attack. So, one should keep the systems updated. Especially the security updates should be incorporated as soon as possible. To prevent attacks like WannaCry, regularly update software, segment networks, deploy firewalls and endpoint protection, maintain backups and train users.

Answer to the Question# 4 (c):

Computer Forensics: Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law.

It deals with the following problems.

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data
- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

X needs to perform a risk assessment to determine the level of risk to the company if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but X will be able to acquire some understanding of the risks they face.

X needs to perform disaster recovery planning for the restoration of disrupted computing and communications services. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

Answer to the Question# 4 (d):

Deep packet inspection (DPI) helps solve this problem. DPI examines data files and sorts out low-priority online material while assigning higher priority to business-critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds.

Answer to the Question# 4 (e):

Sniffer: Programs that covertly search individual packets of data as they pass through a network, capturing passwords or the entire contents.
Spoofing: Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers.
Logic Bombs: An instruction in a computer program that triggers a malicious act when a specific trigger condition is met.
Social Engineering: A tactic used by attackers to manipulate or deceive employees into revealing sensitive information, like passwords, by building trust or using psychological tactics.

Answer to the Question# 5 (a):

An organizational analysis is an important first step in systems analysis. How can people improve an information system if they know very little about the organizational environment in which that system is located? They can't. That's why the members of a development team have to know something about the organization, its management structure, its people, its business activities, the environmental systems it must deal with, and its current information systems. Someone on the team must know this information in more detail for the specific business units or end-user workgroups that will be affected by the new or improved information system being proposed. For example, a new inventory control system for a chain of department stores cannot be designed unless someone on a development team understands a great deal about the company and the types of business activities that affect its inventory. That's why business end users are frequently added to systems development teams.

Answer to the Question# 5 (b):

In a traditional systems development cycle, the role of a business end user is similar to that of a customer or a client. Typically, business end user make a request for a new or improved system, answer questions about the specific information needs and information processing problems, and provide background information on the existing business systems. IS professionals work with the business end user to analyze the problem and suggest alternative solutions. When the business end user approves the best alternative, it is designed and implemented. Here again, the business end user may be involved in a prototyping design process or be on an implementation team with IS specialists.

In end-user development, however, IS professionals play a consulting role while the business end user does its own application development. Sometimes, user consultants may be available to help and other end users with the application development efforts. This may include training in the use of application packages; selection of hardware and software; assistance in gaining access to organization databases; and, of course, assistance in analysis, design, and implementation of the business application of IT that is needed.

Answer to the Question# 5 (c):

In the parallel conversion strategy, the old and new systems are run simultaneously until the end users and project coordinators are fully satisfied that the new system is functioning correctly and the old system is no longer necessary.

Using this approach, a parallel conversion can be effected with either a single cutover, where a predetermined date for stopping the parallel operation is set, or a phased cutover, where some predetermined method of phasing in each piece of the new system and turning off a similar piece of the old system is employed.

Although clearly having the advantage of low risk, the parallel approach also brings with it the highest cost. To execute a parallel approach properly, the end users must literally perform all daily functions with both systems, thus creating a massive redundancy in activities and literally double the work. In fact, unless the operational costs of the new system are significantly less than the old system, the cost of parallel operation can be as much as three to four times greater than the old system alone. During a parallel conversion, all outputs from both systems are compared for concurrency and accuracy, until it is determined that the new system is functioning at least as well as the one it is replacing. Parallel conversion may be the best choice in situations where an automated system is replacing a manual one. In certain circumstances where end users cannot cope with the often-confusing redundancy of two systems, the parallel conversion strategy may not be viable. Also, parallel conversion may not be possible if the organization does not have the available computing resources to operate two systems at the same time.

Answer to the Question# 6 (a):

- Identify those government or other relevant external requirements dealing with:
  - Electronic data, personal data, copyrights, e-commerce, e-signatures
  - The manner in which computers, programs, and data are stored
  - The organization or the activities of information technology services
  - IS audits

- Document applicable laws and regulations.
- Assess whether the management of the organization and the IT function have considered the relevant external requirements in making plans and in setting policies, standards, and procedures, as well as business features.
- Review internal IT department/function/activity documents that address adherence to laws applicable to the industry.
- Determine adherence to established procedures that address these requirements.
- Determine if there are procedures in place to ensure contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

Answer to the Question# 6 (b):

Answer to the Question# 6 (c):

- Principle 1: Meeting Stakeholder Needs
- Principle 2: Covering the Enterprise End-to-End
- Principle 3: Applying a Single, Integrated Framework
- Principle 4: Enabling a Holistic Approach
- Principle 5: Separating Governance from Management

Answer to the Question# 6 (d):

Compliance Testing	Substantive Testing
• Focus: To test compliance with control procedures. • Objective: To determine if controls are applied according to management policies. • Example: Checking if production program library controls are functioning by verifying if the source and object program versions match. • Purpose: Provides reasonable assurance that controls are operating as expected.	• Focus: To evaluate the integrity of individual transactions, data, or information. • Objective: To verify the validity and accuracy of financial statement balances and supporting transactions. • Example: Testing the accuracy of tape library inventory records by conducting an inventory count or statistical sample. • Purpose: Provides evidence of the validity and integrity of financial data and balances.

Answer to the Question# 6 (e):

- Detect problems before they arise.
- Monitor both operation and inputs.
- Attempt to predict potential problems before they occur and make adjustments.
- Prevent an error, omission, or malicious act from occurring.
- Segregate duties (deterrent factor).
- Control access to physical facilities.
- Use well-designed documents (prevent errors).

---The End---