IT GOVERNANCE
Suggested Answers
July-August 2022

Answer to the Question# 1(a):

The following are the three action items under the strategic theme, "Promote environmental preservation by adopting environment-friendly green technologies".

i) Mandate energy-saving and low-power-consumption ICT devices for government procurement based on pre-determined, internationally accepted consumption benchmarks.
ii) Set and enforce regulatory standards to control dumping of ICT devices to prevent electronic waste. Establish safe disposal and recycling mechanisms and organizations.
iii) Reduce use of paper in offices by increasing electronic communication, file processing, information sharing and archiving.

Answer to the Question# 1(b):

i) Subject to such conditions and restrictions as may be specified by regulations, the Controller may, with the previous approval of the Government, and by notification in the Official Gazette and additionally optionally in Electronic Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
ii) Where any Certifying Authority is recognized under sub-section i.. of this section, the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
iii) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section i.. of this section, for reasons to be recorded in writing, by notification in the Official Gazette and additionally optionally in Electronic Gazette, revoke such recognition.

Answer to the Question# 1(c):

More and more companies are turning to computerized systems to filter and hire job applicants, especially for lower-wage, service-sector jobs. The algorithms these systems use to evaluate job candidates may be preventing qualified applicants from obtaining these jobs. For example, some of these algorithms have determined that, statistically, people with shorter commutes are more likely to stay in a job longer than those with longer commutes or less reliable transportation or those who haven't been at their address for very long. If asked, "How long is your commute?" applicants with long commuting times will be scored lower for the job. Although such considerations may be statistically accurate, is it fair to screen job applicants this way?

Answer to the Question# 2(a):

Management information systems provide a variety of information products to managers. Four major reporting alternatives are provided by such systems.

Periodic Scheduled Reports. This traditional form of providing information to managers uses a prespecified format designed to provide managers with information on a regular basis. Typical examples of such periodic scheduled reports are daily or weekly sales analysis reports and monthly financial statements.

Exception Reports. In some cases, reports are produced only when exceptional conditions occur. In other cases, reports are produced periodically but contain information only about these exceptional conditions. For example, a credit manager can be provided with a report that contains only information on customers who have exceeded their credit limits. Exception reporting reduces information overload instead of overwhelming decision makers with periodic detailed reports of business activity.

Demand Reports and Responses. Information is available whenever a manager demands it. For example, Web browsers, DBMS query languages, and report generators enable managers at PC workstations to get immediate responses or to find and obtain customized reports as a result of their requests for the information they need. Thus, managers do not have to wait for periodic reports to arrive as scheduled.

Push Reporting. Information is pushed to a manager's networked workstation. Thus, many companies are using Webcasting software to broadcast selectively reports and other information to the networked PCs of managers and specialists over their corporate intranets.

Answer to the Question# 2(b):

Geographic information systems (GIS) and data visualization systems (DVS) are special categories of DSS that integrate computer graphics with other DSS features. A geographic information system is a DSS that uses geographic databases to construct and display maps, as well as other graphics displays that support decisions affecting the geographic distribution of people and other resources. Many companies are using GIS technology along with global positioning system (GPS) devices to help them choose new retail store locations, optimize distribution routes, or analyze the demographics of their target audiences.

Data visualization systems represent complex data using interactive, three dimensional, graphical forms such as charts, graphs, and maps. DVS tools help users interactively sort, subdivide, combine, and organize data while the data are in their graphical form. This assistance helps users discover patterns, links, and anomalies in business or scientific data in an interactive knowledge discovery and decision support process. Business applications like data

mining typically use interactive graphs that let users drill down in real time and manipulate the underlying data of a business model to help clarify their meaning for business decision making.

Answer to the Question# 2(c):

Bitcoin is a digital token whose ownership can be passed from user to user. This token has no real-life tangible representation, and as such is referred to as an "on-chain" asset. That means, it exists on its blockchain, and owning the token reflects nothing else except that you own the token. The role of on-chain assets in traditional financial services is currently uncertain, and remains so unless or until on-chain assets can legally represent sovereign currencies, shares, or other dematerialised assets.

"Off-chain" assets, by contrast, are real-world items (such as gold, shares, currency) that are digitally represented on a ledger by a token or tokens issued by an issuer. The issuer will safe-keep the real-world item and issue tokens on a ledger against them. The token represents a title deed for that asset and can be passed from user to user. Ultimately a user will return the digital token to the issuer and make a claim on the real-world asset. One current idea for blockchains-as-asset-ledgers is to facilitate faster and more efficient settlement of off-chain assets.

Answer to the Question# 2(d):

Technological impediments, that may limit the scope of the activities of the crowd investing platforms, include bad Internet connections in rural areas.
Regulatory hindrances that may impedes their operations include the following:

i) Limits imposed by act regarding subscription limits for investors.
ii) Unequal treatment of different investments with respect to the prospectus requirement.
iii) Issues related to silent partnerships and non-securitized participation rights.
iv) Difficulty in issuing of securities in crowd investing.
v) Difficulty in the transfer of shares in a limited liability company in crowd investing platforms.
vi) Cross-border activity is difficult.

Answer to the Question# 3(a):

Use information systems to enable a specific market focus, and serve this narrow target market better than competitors. Information systems support this strategy by producing and analyzing data for finely tuned sales and marketing techniques. Information systems enable companies to analyze customer buying patterns, tastes, and preferences closely so that they efficiently pitch advertising and marketing campaigns to smaller and smaller target markets.

The data come from a range of sources—credit card transactions, demographic data, purchase data from checkout counter scanners at supermarkets and retail stores, and data collected when people access and interact with Websites. Sophisticated software tools find patterns in these large pools of data and infer rules from them to guide decision making. Analysis of such data drives one-to-one marketing that creates personal messages based on individualized preferences. For example, Hilton Hotels' OnQ (pronounced "On Cue") system analyzes detailed data collected on active guests in all of its properties to determine the preferences of each guest and each guest's profitability. Hilton uses this information to give its most profitable customers additional privileges, such as late checkouts. Contemporary customer relationship management (CRM) systems feature analytical capabilities for this type of intensive data.

Credit card companies are able to use this strategy to predict their most profitable cardholders. The companies gather vast quantities of data about consumer purchases and other behaviors and mine these data to construct detailed profiles that identify cardholders who might be good or bad credit risks.

So, this strategy, Focus on Market Niche that I will follow to provide special services to the most profitable customers.

Answer to the Question# 3(b):

Use information systems to achieve the lowest operational costs and the lowest prices. The classic example is Walmart. By keeping prices low and shelves well stocked using a legendary inventory replenishment system, Walmart became the leading retail business in the United States. Walmart's continuous replenishment system sends orders for new merchandise directly to suppliers as soon as consumers pay for their purchases at the cash register. Point-of-sale terminals record the bar code of each item passing the checkout counter and send a purchase transaction directly to a central computer at Walmart headquarters. The computer collects the orders from all Walmart stores and transmits them to suppliers. Suppliers can also access Walmart's sales and inventory data using Web technology. Because the system replenishes inventory with lightning speed, Walmart does not need to spend much money on maintaining large inventories of goods in its own warehouses. The system also enables Walmart to adjust purchases of store items to meet customer demands. Competitors, such as Sears, have been spending 24.9 percent of sales on overhead. But by using systems to keep operating costs low, Walmart pays only 16.6 percent of sales revenue for overhead. (Operating costs average 20.7 percent of sales in the retail industry.) Walmart's continuous replenishment system is also an example of an efficient customer response system. An efficient customer response system directly links consumer behavior to distribution and production and supply chains. Walmart's continuous replenishment system provides such an efficient customer response.

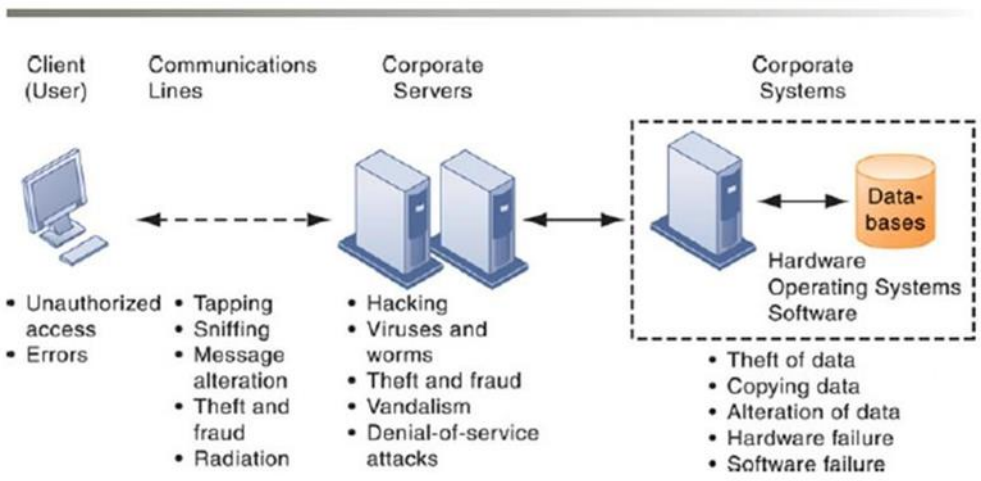
Using such kind of strategy, Low-Cost Leadership, it is possible to develop unique services for our restaurant to attract customers

Answer to the Question# 3(c):

Agency theory- economic theory that views the organization as a nexus of contracts among self-interested individuals who must be supervised and managed.

Information technology reduces the costs of acquiring and analyzing information, which allows organizations to reduces agency costs because it becomes easier for managers to oversee a greater number of employees. This, overall, lowers agency costs. In the long run, organizations should have fewer middle managers and higher revenue per employee, if they've invested in IT.

Answer to the Question# 4(a):



Answer to the Question# 4(b):

Name: **Storm**
Type: Worm/ Trojan horse

Description: First identified in January 2007. Spreads via e-mail spam with a fake attachment. Infected up to 10 million computers, causing them to join its zombie network of computers engaged in criminal activity.

Name: **I Love You**
Type: Virus

Description: First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.

Answer to the Question# 4(c):

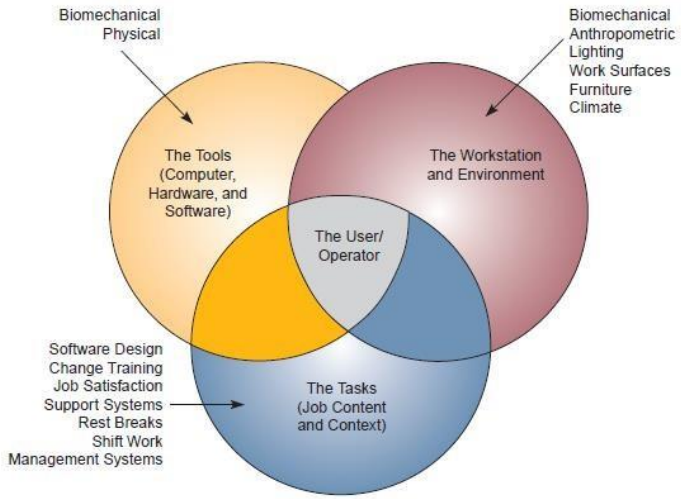
Proportionality. The good achieved by the technology must outweigh the harm or risk. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk.
Informed Consent. Those affected by the technology should understand and accept the risks.
Justice. The benefits and burdens of the technology should be distributed fairly. Those who benefit should bear their fair share of the risks, and those who do not benefit should not suffer a significant increase in risk.
Minimized Risk. Even if judged acceptable by the other three guidelines, the technology must be implemented so as to avoid all unnecessary risk.

Answer to the Question# 4(d):

Computer profiling and mistakes in the computer matching of personal data are other controversial threats to privacy. Individuals have been mistakenly arrested and jailed and people have been denied credit because their physical profiles or personal data have been used by profiling software to match them incorrectly or improperly with the wrong individuals. Another threat is the unauthorized matching of computerized information about you extracted from the databases of sales transaction processing systems and sold to information brokers or other companies. A more recent threat is the unauthorized matching and sale of information about you collected from Internet Web sites and newsgroups you visit, as we discussed previously. You are then subjected to a barrage of unsolicited promotional material and sales contacts as well as having your privacy violated.

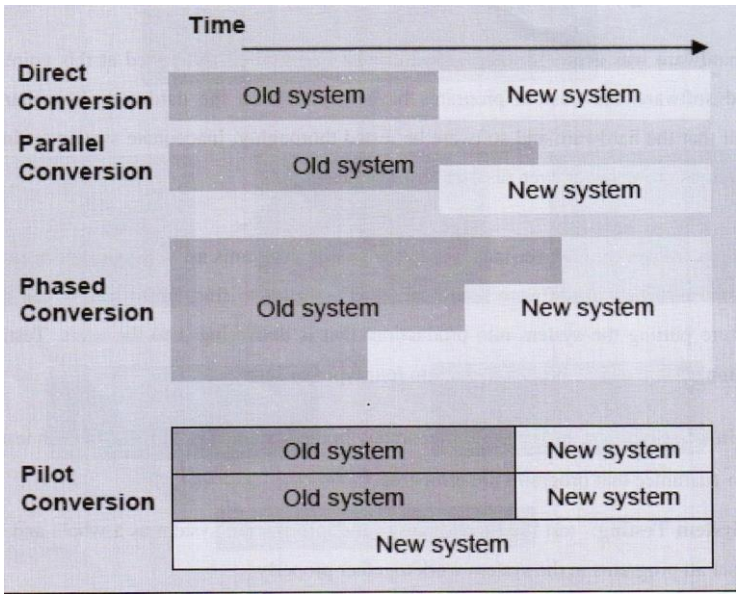
Answer to the Question# 4(e):

Ergonomic factors in the workplace. Note that good ergonomic design considers tools, tasks, the workstation, and the environment.



Answer to the Question# 5(a):

Conversion entails the method used to change from an old accounting information system (AIS) to new AIS. There are several methods for achieving this goal.



System conversion strategies

One is to run the new and old systems in parallel for a specified period. A second method is to directly cut over to the new system at a specified point. A third is to phase in the system, either by location or system function. A fourth is to pilot the new system at a specific site before converting.

For this case, parallel strategy is the most appropriate.

Parallel Strategy:
Both the old system and its potential replacement are running together for a specified time period until it is assured that the new one functions correctly.

Parallel strategy

The advantage of this strategy is that any problems with the new system can be solved before the old system is terminated. The disadvantage is that it is very expensive since additional staff or resources may be required to run the extra system.

Answer to the Question# 5(b):

The goal of the feasibility study is to consider alternative information systems solutions, evaluate their feasibility, and propose the alternative most suitable to the organization. The feasibility of a proposed solution is evaluated in terms of its components. These components are:

Economic Feasibility—the economic viability of the proposed system. The proposed project's costs and benefits are evaluated. Tangible costs include fixed and variable costs, while tangible benefits include cost savings, increased revenue, and increased profit.

A project is approved only if it covers its cost in a given period of time. However, a project may be approved only on its intangible benefits such as those relating to government regulations, the image of the organization, or similar considerations.

Technical Feasibility—the possibility that the organization has or can procure the necessary resources. This is demonstrated if the needed hardware and software are available in the marketplace or can be developed by the time of implementation.

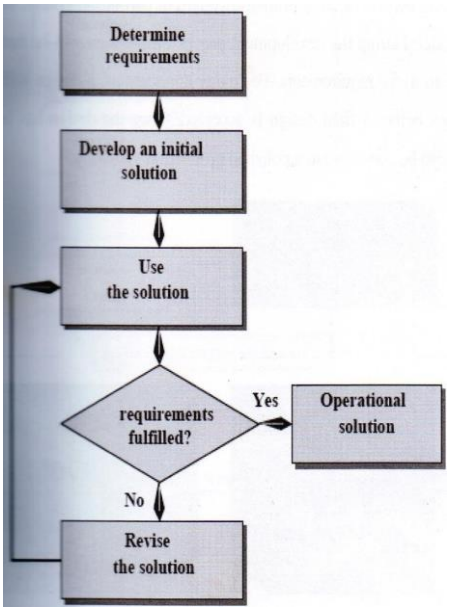
Operational Feasibility—the ability, desire, and willingness of the stakeholders to use, support, and operate the proposed computer information system. The stakeholders include management, employees, customers, and suppliers. The stakeholders are interested in systems that are easy to operate, make few, if any, errors, produce the desired information, and fall within the objectives of the organization.

Answer to the Question# 5(c):

Meeting or exceeding stakeholder needs and expectations invariably involves balancing competing demands among:

- Scope; time, cost, and quality.
- Stakeholders with differing needs and expectations.
- Identified requirements (needs) and unidentified requirements (expectations).

Developing a Solution to Fulfill Requirements



Developing a solution

Answer to the Question# 6(a):

Risk is the combination of the probability of an event and its consequence. Risk signifies the adverse impacts that could occur to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations. . . due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

IS auditors must be able to identify and differentiate risk types and the controls used to mitigate the risk. They must have knowledge of common business risk, related technology risk and relevant controls. They must also be able to evaluate the risk assessment and management techniques used by business managers, and to make assessments of risk to help focus and plan audit work. In addition to an understanding of business risk and control, IS auditors must understand that risk exists within the audit process.

Answer to the Question# 6(b):

The assessment of countermeasures should be performed through a cost-benefit analysis where controls to mitigate risk are selected to reduce risk to a level acceptable to management. This analysis process may be based on any of the following:

- The cost of the control compared to the benefit of minimizing the risk.

- Management's appetite for risk (i.e., the level of residual risk that management is prepared to accept).
- Preferred risk-reduction methods (e.g., terminate the risk, minimize probability of occurrence, minimize impact, transfer the risk via insurance).

Answer to the Question# 6(c):

The risk assessment process is characterized as an iterative life cycle that begins with identifying business objectives, information assets, and the underlying systems or information resources that generate, store, use or manipulate the assets (hardware, software, databases, networks, facilities, people, etc.) critical to achieving these objectives. Because IT risk is dynamic, it is strategic for management to recognize the need for and establish a dynamic IT risk management process that supports the business risk management process. The greatest degree of risk management effort may then be directed toward those considered most sensitive or critical to the organization. After sensitive and/or critical information assets are identified, a risk assessment is performed to identify vulnerabilities and threats, and determine the probability of occurrence and the resulting impact and additional safeguards that would mitigate this impact to a level acceptable to management.

Answer to the Question# 6(d):

From the IS auditor's perspective, risk analysis serves more than one purpose:

- It assists the IS auditor in identifying risk and threats to an IT environment and IS system— risk and threats that would need to be addressed by management—and in identifying system- specific internal controls. Depending on the level of risk, this assists the IS auditor in selecting certain areas to examine.
- It helps the IS auditor in his/her evaluation of controls in audit planning.
- It assists the IS auditor in determining audit objectives.
- It supports risk-based audit decision making.

Answer to the Question# 7(a):

The IS auditor should understand the various types of audits that can be performed, internally or externally, and the audit procedures associated with each:

Compliance audits: Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards. These audits often overlap traditional audits but may focus on particular systems or data. Examples include Payment Card Industry Data Security Standard (PCI DSS) audits for companies that process credit card data and Health Insurance Portability and Accountability Act (HIPAA) audits for companies that handle health care data.

Financial audits: The purpose of a financial audit is to assess the accuracy of financial reporting. A financial audit will often involve detailed, substantive testing, although increasingly, auditors are placing more emphasis on a risk- and control-based audit approach. This kind of audit relates to financial information integrity and reliability.

Operational audits: An operational audit is designed to evaluate the internal control structure in a given process or area. IS audits of application controls or logical security systems are some examples of operational audits.

Integrated audits: An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance. An integrated audit can be performed by external or internal auditors and would include compliance tests of internal controls and substantive audit steps.

Answer to the Question# 7(b):

Effective risk-based auditing is driven by two processes:

i) The risk assessment that drives the audit schedule.
ii) The risk assessment that minimizes the audit risk during the execution of an audit.

A risk-based audit approach is usually adapted to develop and improve the continuous audit process. This approach is used to assess risk and to assist an IS auditor in making the decision to perform either compliance testing or substantive testing. It is important to stress that the risk-based audit approach efficiently assists the auditor in determining the nature and extent of testing.

Business risk includes concerns about the probable effects of an uncertain event on achieving established business objectives. The nature of business risk may be financial, regulatory or operational and may also include risk derived from specific technology. For example, an airline company is subject to extensive safety regulations and economic changes, both of which impact the continuing operations of the company. In this context, the availability of IT service and its reliability are critical.

---The End---