IT GOVERNANCE
Suggested Answers
Nov-Dec 2022

Answer to the Question# 1 (a):

The action items are as follows:

i) Develop a national health network of all medical institutions in the public sector for availability of critical management information.
ii) Develop database of usage, lifespan etc. for important hospital machinery and equipment like X-ray, ultra-sonogram etc. in use in the Governmental Hospitals for proper & timely procurement thereof
iii) Develop infrastructure database for ensuring timely maintenance of governmental facilities
iv) iv)Update and use database for management of doctors, alternative medical care professionals, nurses, paramedics and other health workers for posting, training and promotion
v) Utilize Geographical Information Systems (GIS) to facilitate health sector planning, as well as helping to predict and identify the spread of emerging disease condition
vi) Promote and facilitate the use of ICTs in monitoring health service delivery systems.
vii) Use ICT (mobile) facilities for monitoring, contact & discussions with among field personnel

Answer to the Question# 1 (b):

Hacking is define as follows.

-(1) If any person

(a) with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(b) damage through illegal access to any such computer, computer network or any other electronic system which do not belong to him; then such activity shall be treated as hacking offence

Punishment:

Whoever commits hacking offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka one crore, or with both.

Answer to the Question# 1 (c):

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it. Some of the tools to capture individual activity online. They are

i) Cookies: Cookies are small text files deposited on a computer hard drive when a user visits Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past.

ii) Web beacons: It is a tiny software programs that keep a record of users' online clickstream and report this data back to whomever owns the tracking file invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail.

iii) Other spyware can secretly install itself on an Internet user's computer by piggybacking on larger applications

Technical solution: There are a few technologies that can protect user privacy during interactions with Web sites. Many of these tools are used for encrypting e-mail, for making e-mail or surfing activities appear anonymous, for preventing client computers from accepting cookies, or for detecting and eliminating spyware. For the most part, technical solutions have failed to protect users from being tracked as they move from one site to another. There are Do not track option in some browser.

Answer to the Question# 2 (a):

A DSS model base is a software component that consists of models used in computational and analytical routines that mathematically express relationships among variables. For example, a spreadsheet program might contain models that express simple accounting relationships among variables, such as Revenue 2 Expenses 5 Profit. A DSS model base could also include models and analytical techniques used to express much more complex relationships. For example, it might contain linear programming models, multiple regression forecasting models, and capital budgeting present value models. Such models may be stored in the form of spreadsheet models or templates, or statistical and mathematical programs and program modules.

Answer to the Question# 2 (b):

OLAP is an abbreviation for online analytical processing. The IS industry has responded to the mentioned demands with developments like analytical databases, data marts, data warehouses, data mining techniques, and multidimensional database structures, and with specialized servers and Webenabled software products that support online analytical processing (OLAP). Online analytical processing enables managers and analysts to interactively examine and manipulate large amounts of detailed and consolidated data from many perspectives. OLAP involves analyzing complex relationships among thousands or even millions of data items stored in data marts, data warehouses, and other multidimensional databases to discover patterns, trends, and exception conditions. An OLAP session takes place online in real time, with rapid responses to a manager's or analyst's queries, so that the analytical or decision-making process is undisturbed.

Answer to the Question# 2 (c):

The basic analytical operations involved by online analytical processing (OLAP) are described below:

Consolidation: Consolidation involves the aggregation of data, which can involve simple roll-ups or complex groupings involving interrelated data. For example, data about sales offices can be rolled up to the district level, and the district-level data can be rolled up to provide a regional-level perspective.

Drill-down: OLAP can also go in the reverse direction and automatically display detailed data that comprise consolidated data. This process is called drill-down. For example, the sales by individual products or sales reps that make up a region's sales totals could be easily accessed.

Slicing and Dicing: Slicing and dicing refers to the ability to look at the database from different viewpoints. One slice of the sales database might show all sales of a product type within regions. Another slice might show all sales by sales channel within each product type. Slicing and dicing is often performed along a time axis to analyze trends and find time-based patterns in the data.

Answer to the Question# 2 (d):

The Bitcoin Blockchain is a database file that sits on thousands of computers worldwide, where the individual copies are kept aligned through the rules of the Bitcoin protocol. The Bitcoin Blockchain file (actually it is a series of files, because large files are difficult to manage) contains a list of every single bitcoin transaction that has ever happened: it is the ledger of record for Bitcoin.

The Bitcoin Blockchain is an open or 'permissionless' database. That is, should you wish to write entries to the database you may do so without signing up, logging in or asking permission from anyone in charge. In practice, this is done by downloading some opensource software and running it. By doing so, your computer will connect over the Internet to other computers running similar software. The software lets you start sending and receiving bitcoin transaction data with neighbours, and allow you to add data to the bitcoin blockchain, by playing a computationally intensive lottery known as 'mining'.

By studying The Bitcoin Blockchain file it is easy to see which bitcoin account has how many bitcoins and which accounts are sending bitcoins to whom. This transparency is needed so that the validators of the transactions determine whether a transaction is legitimate or not. For example, a bitcoin transaction that pays someone using bitcoins that don't exist would not be considered valid.

Answer to the Question# 2 (e):

The robo-advice subsegement refers to portfolio management systems that provide algorithm-based and largely automated investment advice, sometimes also making investment decisions. Robo advisers' algorithms are generally based on passive investing and diversification strategies. They consider the investor's risk tolerance, the preferred duration of the investment, as well as other goals.

Answer to the Question# 3 (a):

Most IT governance frameworks are designed to help you determine how your IT department is functioning overall, what key metrics management needs and what return IT is giving back to the business from its investments. Where COBIT and COSO are used mainly for risk, ITIL helps to streamline service and operations. Although CMMI was originally intended for software engineering, it now involves processes in hardware development, service delivery and purchasing. As previously mentioned, FAIR is squarely for assessing operational and cyber security risks.

When reviewing frameworks, consider your corporate culture. Does a particular framework or model seem like a natural fit for your organization? Does it resonate with your stakeholders? That framework is probably the best choice.

But you don't have to choose only one framework. For example, COBIT and ITIL complement one another in that COBIT often explains why something is done or needed where ITIL provides the "how." Some organizations have used COBIT and COSO, along with the ISO 27001 standard (for managing information security).

Answer to the Question# 3 (b):

People in organizations occupy different positions with different specialties, concerns, and perspectives. As a result, they naturally have divergent viewpoints about how resources, rewards, and punishments should be distributed. These differences matter to both managers and employees, and they result in political struggle for resources, competition, and conflict within every organization.

Political resistance is one of the great difficulties of bringing about organizational change—especially the development of new information systems. Virtually all large information systems investments by a firm that bring about significant changes in strategy, business objectives, business processes, and procedures become politically charged events. Managers who know how to work with the politics of an organization will be more successful than less-skilled managers in implementing new information systems.

Answer to the Question# 3 (c):

The growing use of sensors in industrial and consumer products, often called the Internet of Things (IoT), is an excellent example of how the Internet is changing competition within industries and creating new products and services. Many other sports and fitness companies are investing into wearable health trackers and fitness equipment that use sensors to report users' activities to remote corporate computing centers where the data can be analyzed. Farm tractors from several manufacturers are loaded with field radar, GPS transceivers, and hundreds of sensors keeping track of the equipment. One leading organization is creating a new business out of helping its aircraft and wind turbine clients improve operations by examining the data generated from the many thousands of sensors in the equipment.

The result is what are referred to as "smart products" — products that are a part of a larger set of information-intensive services sold by firms. The impact of smart, Internet-connected products is just now being understood.

Smart products offer new functionality, greater reliability, and more intense use of products while providing detailed information that can be used to improve both the products and the customer experience. They expand opportunities for product and service differentiation. When you buy a wearable digital health product, you not only get the product itself, you also get a host of services available from the manufacturer's cloud servers. Smart products increase rivalry among firms that will either innovate or lose customers to competitors. Smart products generally raise switching costs and inhibit new entrants to a market because existing customers are trapped in the dominant firm's software environment. Finally, smart products may decrease the power of suppliers of industrial components if, as many believe, the physical product becomes less important than the software and hardware that make it run.

Answer to the Question# 4 (a):

Internet vulnerability has increased from widespread use of e-mail, instant messaging (IM), and peer-to-peer (P2P) file-sharing programs. E-mail may contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use e-mail messages to transmit valuable trade secrets, financial data, or confidential customer information to unauthorized recipients.

Some of the popular IM applications for consumers do not use a secure layer for text messages, so they can be intercepted and read by outsiders during transmission over the Internet. Instant messaging activity over the Internet can in some cases be used as a back door to an otherwise secure network. Sharing files over P2P networks, such as those for illegal music sharing, may also transmit malicious software or expose information on either individual or corporate computers to outsiders.

Answer to the Question# 4 (b):

We tend to think the security threats to a business originate outside the organization. In fact, company insiders pose serious security problems. Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace.

Studies have found that user lack of knowledge is the single greatest cause of network security breaches. Many employees forget their passwords to access computer systems or allow coworkers to use them, which compromises the system. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information. This practice is called social engineering.

Both end users and information systems specialists are also a major source of errors introduced into information systems. End users introduce errors by entering faulty data or by not following the proper instructions for processing data and using computer equipment. Information systems specialists may create software errors as they design and develop new software or maintain existing programs.

Answer to the Question# 4 (c):

Spyware has a variety of characteristics, beyond its potential for stealing valuable private information, which make it undesirable to most computer users.

At the very least, it plagues the user of the infected machine with unwanted advertising. More often, it watches everything a user does online and sends that information back to the marketing company that created the spyware. Often, spyware applications add advertising links to Web pages owned by other people, for which the Web page owner does not get paid, and may even redirect the payments from legitimate affiliate-fee advertisers to the makers of the spyware. Other undesirable characteristics include setting an infected system's browser home page and search settings to point to the spyware owner's

Web sites (generally loaded with advertising), often in a manner that prevents you from changing back the settings (referred to as home-page hijacking).

In the extremes, spyware can make a dial-up modem continually call premiumrate phone numbers, thus causing large telephone charges (and usually fees to the spyware owner) or leave security holes in an infected system allowing the makers of the spyware—or, in particularly bad cases, anyone at all—to download and run software on the infected machine (such downloads are called Trojans).

In almost all cases, spyware severely degrades system performance. As you can see, spyware doesn't have any redeeming features except for the benefits to its owner. Its use is pervasive, and failing to protect against it virtually ensures that your system will eventually become infected.

Answer to the Question# 4 (d) (i):

Cyber law is the term used to describe laws intended to regulate activities over the Internet or via the use of electronic data communications. Cyber law encompasses a wide variety of legal and political issues related to the Internet and other communications technologies, including intellectual property, privacy, freedom of expression, and jurisdiction.

Answer to the Question# 4 (d) (ii):

The intersection of technology and the law is often controversial. Some feel that the Internet should not (or possibly cannot) be regulated in any form. Furthermore, the development of sophisticated technologies, such as encryption and cryptography, make traditional forms of regulation extremely difficult. Finally, the fundamental endto-end nature of the Internet means that if one mode of communication is regulated or shut down, another method will be devised and spring up in its place. In the words of John Gilmore, founder of the Electronic Frontier Foundation, "the Internet treats censorship as damage and simply routes around it."

Answer to the Question# 4 (d) (iii):

Cyber law is a new phenomenon, having emerged after the onset of the Internet. As we know, the Internet grew in a relatively unplanned and unregulated manner. Even the early pioneers of the Internet could not have anticipated the scope and Computer Libel and Censorship far-reaching consequences of the cyberspace of today and tomorrow. The debate continues regarding the applicability of analogous legal principles derived from prior controversies that had nothing to do with cyberspace. As we progress in our understanding of the complex issues in cyberspace, new and better laws, regulations, and policies will likely be adopted and enacted.

Answer to the Question# 4 (e):

Data classification as a control measure should define:

- The importance of the information asset.
- The information asset owner.
- The process for granting access.
- The person responsible for approving the access rights and access levels.
- The extent and depth of security controls.

Data classification must take into account legal, regulatory, contractual and internal requirements for maintaining privacy, confidentiality, integrity and availability of information.

Data classification is useful to identify who should have access to the production data used to run the business versus those who are permitted to access test data and programs under development. For example, application programmers or system development programmers should not have access to production data or programs.

Answer to the Question# 5 (a):

The essence of systems thinking is as follows.

- Seeing interrelationships among systems rather than linear cause-and-effect chains whenever events occur.
- Seeing processes of change among systems rather than discrete "snapshots" of change, whenever changes occur.

The sales process of a business can be viewed as a system. We could then ask: Is poor sales performance (output) caused by inadequate selling effort (input),out-of-date sales procedures (processing), incorrect sales information (feedback), or inadequate sales management (control)

Answer to the Question# 5 (b):

i) System Investigation: Determine how to address business opportunities and priorities. Conduct a feasibility study to determine whether a new or improved business system is a feasible solution. Develop a project management plan and obtain management approval.
ii) System Analysis: Analyze the information needs of employees, customers, and other business stakeholders. Develop the functional requirements of a system that can meet business priorities and the needs of all stakeholders. Determine how to address business opportunities and priorities. Conduct a feasibility study to determine whether a new or improved business system is a feasible solution. Develop a project management plan and obtain management approval. Develop logical models of current system
iii) System Design: Develop specifications for the hardware, software, people, network, and data resources, and the information products that will satisfy the functional requirements of the proposed business information system. Develop logical models of new system
iv) Systems Implementation: Acquire (or develop) hardware and software. Test the system, and train people to operate and use it. Convert to the new business system. Manage the effects of system changes on end users.
v) Systems Maintenance: Use a post implementation review process to monitor, evaluate, and modify the business system as needed.

Answer to the Question# 5 (c):

Software Evaluation Factors

i) Quality: Is it bug-free, or does it have many errors in its program code?
ii) Efficiency: Is the software a well-developed system of program code that does not use much CPU time, memory capacity, or disk space?
iii) Flexibility: Can it handle our business processes easily, without major modification?
iv) Security: Does it provide control procedures for errors, malfunctions, and improper use?
v) Connectivity: Is it Web-enabled so it can easily access the Internet, intranets, and extranets, on its own, or by working with Web browsers or other network software?
vi) Maintenance: Will new features and bug fixes be easily implemented by our own software developers?
vii) Documentation: Is the software well documented? Does it include help screens and helpful software agents?
viii) Hardware: Does existing hardware have the features required to best use this software?
ix) Other Factors: What are its performance, cost, reliability, availability, compatibility, modularity, technology, ergonomics, scalability, and support characteristics?

Answer to the Question# 6 (a):

Three-tier architecture is comprised of the following:

– The presentation tier displays information that users can access directly such as a web page or an operating system's (OS's) graphical user interface.
– The application tier (business logic/applications) controls an application's functionality by performing detailed processing.
– The data tier is usually composed of the database servers, file shares, etc. and the data access layer that encapsulates the persistence mechanisms and exposes the data.

Answer to the Question# 6 (b):

To perform an audit of ATMs, an IS auditor should undertake the following actions:

- Review physical security to prevent introduction of malware.
- Review measures to establish proper customer identification and maintenance of their confidentiality.
- Review file maintenance and retention system to trace transactions.
- Review exception reports to provide an audit trail.
- Review daily reconciliation of ATM transactions including:
  – Review SoD in the opening of the ATM and recount the deposit.
  – Review the procedures made for the retained cards.
- Review encryption key change management procedures.
  – Review physical security measures to ensure security of the ATM and the money contained in the ATM.
  – Review the ATM card slot, keypad and enclosure to prevent skimming of card data and capture of PIN during entry

Answer to the Question# 6 (c):

An IS auditor should review the following:

- Interconnection agreements prepared prior to engaging in an ecommerce agreement. These agreements can be as simple as accepting terms of use to detailed terms and conditions to be in place before the ecommerce interconnections are established.
- Security mechanisms and procedures that, taken together, constitute a security architecture for ecommerce (e.g., Internet firewalls, public key infrastructure [PKI], encryption, certificates, PCI DSS compliance and password management) • Firewall mechanisms that are in place to mediate between the public network (the Internet) and an organization's private network
- A process whereby participants in an ecommerce transaction can be identified uniquely and positively (e.g., a process of using some combination of public and private key encryption and certifying key pairs)
- Procedures in place to control changes to an ecommerce presence
- Ecommerce application logs, which are monitored by responsible personnel. This includes OS logs and console messages, network management messages, firewall logs and alerts, router management messages, intrusion detection alarms, application and server statistics, and system integrity checks.
- Methods and procedures to recognize security breaches when they occur (network and host-based intrusion detection systems [IDSs])
- Features in ecommerce applications to reconstruct the activity performed by the application
- Protections in place to ensure that data collected about individuals are not disclosed without the individuals' consent nor used for purposes other than that for which they are collected
- Means to ensure confidentiality of data communicated between customers and vendors (safeguarding resources such as through encrypted Secure Sockets Layer [SSL])
- Mechanisms to protect the presence of ecommerce and supporting private networks from computer viruses and to prevent them from propagating viruses to customers and vendors
- Features within the ecommerce architecture to keep all components from failing and allow them to repair themselves, if they should fail
- Plans and procedures to continue ecommerce activities in the event of an extended outage of required resources for normal processing
- Commonly understood practices and procedures to define management's intentions for the security of e commerce
- Shared responsibilities within an organization for ecommerce security
- Communications from vendors to customers about the level of security in an ecommerce architecture
- Regular programs of audit and assessment of the security of ecommerce environments and applications to provide assurance that controls are present and effective

Answer to the Question# 6 (d):

Class	Function	Example
Preventive	● 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	● Employing only qualified personnel ● Segregation of duties ● Controlling access to physical facilities ● Well-designed documents to prevent errors ● procedures for authorization of transactions ● Programmed edit checks ● Use of access control software that allows only authorized personnel to access sensitive files ● Use of encryption software to prevent unauthorized disclosure of data
Detective	● Use controls that detect and report the occurrence of an error, omission or malicious act	● Hash totals ● Check points in production jobs • Echo controls in telecommunications ● Error messages over tape labels ● Duplicate checking of calculations

Class	Function	Example
		● Periodic performance reporting with variances ● Past-due account reports ● Internal audit function ● Review of activity logs to detect unauthorized access attempts ● Secure code reviews ● Software quality assurance
Corrective	● Minimize the impact of a threat ● Remedy problems discovered by detective controls ● Identify the cause of a problem ● Correct errors arising from a problem ● Modify the processing system(s) to minimize future occurrences of the problem	● Contingency/continuity of operations planning ● Disaster recovery planning ● Incident response planning ● Backup procedures ● System break/fix service level agreements

---The End---