CHAPTER 2
AUDITING IT GOVERNANCE CONTROLS

REVIEW QUESTIONS

1. **What is IT governance?**
   Response: IT governance is a relatively new subset of corporate governance that focuses on the management and assessment of strategic IT resources.

2. **What are the objectives of IT governance?**
   Response: The key objectives of IT governance are to reduce risk and ensure that investments in IT resources add value to the corporation.

3. **What is distributed data processing?**
   Response: Distributed data processing involves reorganizing the central IT function into small IT units that are placed under the control of end users. The IT units may be distributed according to business function, geographic location, or both. All or any of the IT functions may be distributed. The degree to which they are distributed will vary depending upon the philosophy and objectives of the organization's management.

4. **What are the advantages and disadvantages of distributed data processing?**
   Response: The advantages of DDP are:
   a. cost reductions
   b. improved cost control responsibility
   c. improved user satisfaction
   d. back up flexibility

   The disadvantages (risks) are:
   a. inefficient use of resources
   b. destruction of audit trails
   c. inadequate segregation of duties
   d. difficulty acquiring qualified professionals
   e. lack of standards

5. **What types of tasks become redundant in a distributed data processing system?**
   Response: Autonomous systems development initiatives distributed throughout the firm can result in each user area reinventing the wheel rather than benefiting from the work of others. For example, application programs created by one user, which could be used with little or no change by others, will be redesigned from scratch rather than shared. Likewise, data common to many users may be recreated for each, resulting in a high level of data redundancy. This situation
   has implications for data accuracy and consistency.

.

6. **Explain why certain duties that are deemed incompatible in a manual system may be combined in a CBIS computer-based information system environment. Give an example**.
   Response: The IT (CBIS) environment tends to consolidate activities. A single application may authorize, process, and record all aspects of a transaction. Thus, the focus of segregation control shifts from the operational level (transaction processing tasks

that computers now perform) to higher-level organizational relationships within the computer services function.

7. **What are the three primary CBIS functions that must be separated?**
Response: The three primary CBIS functions that must be separated are as follows:
a. separate systems development from computer operations,
b. separate the database administrator from other functions , and
c. separate new systems development from maintenance.

8. **What exposures do data consolidation in a CBIS environment pose?**
Response: In a CBIS environment, data consolidation exposes the data to losses from natural and man-made disasters. Consolidation creates a single point of failure. The only way to back up a central computer site against disasters is to provide a second computer facility.

9. **What problems may occur as a result of combining applications programming and maintenance tasks into one position?**
Response: One problem that may occur is inadequate documentation. Documenting is not considered as interesting a task as designing, testing, and implementing a new system, thus a systems professional may move on to a new project rather than spend time documenting an almost complete project. Job security may be another reason a programmer may not fully document his or her work. Another problem that may occur is the increased potential for program fraud. If the original programmer generates fraudulent code during development, then this programmer, through maintenance procedures, may disable the code prior to audits. Thus, the programmer can continue to cover his or her tracks.

10. **Why is poor-quality systems documentation a prevalent problem?**
Response:
Poor-quality systems documentation is a chronic IT problem and a significant challenge for many organizations seeking SOX compliance. At least two explanations are possible for this phenomenon. First, documenting systems is not as interesting as designing, testing, and implementing them. Systems professionals much prefer to move on to an exciting new project rather than document one just completed. The second possible reason for poor documentation is job security. When a system is poorly documented, it is difficult to interpret, test, and debug. Therefore, the programmer who understands the system (the one who coded it) maintains bargaining power and becomes relatively indispensable. When the programmer leaves the firm, however, a new programmer inherits maintenance responsibility for the undocumented system. Depending on its complexity, the transition period may be long and costly.

11. **What is RAID?**
Response: RAID (redundant arrays of independent disks) use parallel disks that contain redundant elements of data and applications. If one disk fails, the lost data are automatically reconstructed from the redundant components stored on the other disks.

12. **What is the role of a data librarian?**
Response: A data librarian, who is responsible for the receipt, storage, retrieval, and custody of data files, controls access to the data library. The librarian issues data files to computer operators in accordance with program requests and takes custody of files when processing or backup procedures are completed. The trend in recent years toward real-

time processing and the increased use of direct-access files has reduced or even eliminated the role of the data librarian in many organizations.

13. **What is the role of a corporate computer services department? How does this differ from other configurations?**
Response: The role of a corporate computer services department (IT function) differs in that it is not a completely centralized model; rather, the group plays the role of provider of technical advice and expertise to distributed computer services. Thurs, it provides much more support than would be received in a completely distributed model. A corporate computer services department provides a means for central testing of commercial hardware and software in an efficient manner. Further, the corporate group can provide users with services such as installation of new software and troubleshooting hardware and software problems. The corporate group can establish systems development, programming, and documentation standards. The corporate group can aid the user groups in evaluating the technical credentials of prospective systems professionals.

14. **What are the five risks associated with distributed data processing?**
Response: The five risks associated with distributed data processing are as follows:
a. inefficient use of resources,
b. destruction of audit trails,
c. inadequate segregation of duties,
d. potential inability to hire qualified professionals, and
e. lack of standards.

15. **List the control features that directly contribute to the security of the computer center environment**.
Response:
a. physical location controls
b. construction controls
c. access controls
d. air conditioning
e. fire suppression
f. fault tolerance

16. **What is data conversion?**
Response: The data conversion function transcribes transaction data from paper source documents into computer input. For example, data conversion could be keying sales orders into a sales order application in modern systems or transcribing data into magnetic media (tape or disk) suitable for computer processing in legacy-type systems.

17. **What may be contained in the data library?**
Response: The data library is a room adjacent to the computer center that provides safe storage for the off-line data files. Those files could be backups or current data files. For instance, the data library could store backups on DVDs, CD-ROMs, tapes, or other storage devices. It could also store live, current data files on magnetic tapes and removable disk packs. In addition, the data library could store the original copies of commercial software and their licenses for safekeeping.

18. **What is an ROC?**
Response: A recovery operations center (ROC) or hot site is a fully equipped backup data center that many companies share. In addition to hardware and backup facilities, ROC service providers offer a range of technical services to their clients, who pay an annual fee for access rights. In the event of a major disaster, a subscriber can occupy the premises and, within a few hours, resume processing critical applications.

19. **What is a cold site?**
Response:
The empty shell or cold site plan is an arrangement wherein the company buys or leases a building that will serve as a data center. In the event of a disaster, the shell is available and ready to receive whatever hardware the temporary user requires to run its essential data processing systems.

20. **What is fault tolerance?**
Response: Fault tolerance is the ability of the system to continue operation when part of the system fails due to hardware failure, application program error, or operator error. Implementing fault tolerance control ensures that no single point of potential system failure exists. Total failure can occur only in the event of the failure of multiple components, or system-wide failure.

21. **What are the often-cited benefits of IT outsourcing?**
Response: Often-cited benefits of IT outsourcing include improved core business performance, improved IT performance (because of the vendor's expertise), and reduced IT costs.

22. **Define commodity IT asset**.
Response: Commodity IT assets are those assets that are not unique to a particular organization and are thus easily acquired in the marketplace. These include such things are network management, systems operations, server maintenance, and help-desk functions.

23. **Define specific asset**.
Response: Specific assets, in contrast to commodity assets, are unique to the organization and support its strategic objectives. Because of their idiosyncratic nature, specific assets have little value outside of their current use.

24. **List five risks associated with IT outsourcing**.
Response:
a. failure to perform
b. vendor exploitation
c. outsourcing costs exceed benefits
d. reduced security
e. loss of strategic advantage

25. **What is virtualization?**
Response:
Virtualization multiplies the effectiveness of the physical system by creating virtual (software) versions of the computer with separate operating systems that reside in the same physical equipment. In other words, virtualization is the concept of running more than one "virtual computer" on a single physical computer.

26. **What is network virtualization?**
Response:
Network virtualization increases effective network bandwidth by dividing it into independent channels, which are then assigned to separate virtual computers. Network virtualization optimizes network speed, flexibility, and reliability; most importantly, it improves network scalability.

27. **What are the three classes of cloud computing services?**
Response:

Cloud computing classes are: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).

28. **What is Software as a Service (SaaS)?**
Response:
Software as a Service (SaaS) is a software distribution model in which service providers host applications for client organizations over a private network or the Internet.

29. **Give two advantages of Infrastructure as a Service (IaaS).**
Response:
One advantage is that the IaaS provider owns, houses, and maintains the equipment, and the client pays for it on a per-use basis.
Another advantage is scalability, which is the ability to rapidly respond to usage changes.

DISCUSSION QUESTIONS

1. **How is pre-SOX IT governance different from post-SOX IT governance?**
Response: Prior to SOX, the common practice regarding IT investments was to defer all decisions to corporate IT professionals. Modern IT governance, however, follows the philosophy that all corporate stakeholders, including boards of directors, top management, and department users (i.e. accounting and finance) be active participants in key IT decisions. Such broad-based involvement reduces risk and increases the likelihood that IT decisions will be in compliance with user needs, corporate policies, strategic initiatives, and internal control requirements under SOX.

2. **Although IT governance is a broad area, only three aspects of IT governance are discussed in the chapter. Name them and explain why these topics were chosen.**
Response: Although all IT governance issues are important to the organization, not all of them are matters of internal control under SOX that may potentially impact the financial reporting process. This chapter examined three IT governance issues that are addressed by SOX and the COSO internal control framework. These are:
    a. Organizational structure of the IT function,
    b. Computer center operations, and
    c. Disaster recovery planning.

3. **What types of incompatible activities are prone to becoming consolidated in a distributed data processing system? How can this be prevented?**
Response: Achieving an adequate segregation of duties may not be possible in some distributed environments. The distribution of the IT services to users may result in the creation of small independent units that do not permit the desired separation of

incompatible functions. For example, within a single unit the same person may write application programs, perform program maintenance, enter transaction data into the computer, and operate the computer equipment. Such a situation would be a fundamental violation of internal control. Often, the control problems previously described can be addressed by implementing a corporate IT function.

4. **Why would an operational manager be willing to take on more work in the form of supervising an information system?**
Response: Managers are responsible for the success of their divisions. If the benefits to be reaped from a DDP are expected to be great enough, the manager may find it is worth her or his while to expend the extra effort. Some of the benefits the manager may hope will materialize within the divisions are more efficiently run operations, better decision making, and reduced processing costs. Increased customer satisfaction may also result if the DDP system is more accommodating.

5. **How can data be centralized in a distributed data processing system?**
Response: The data is stored centrally, but updated or processed at the local (remote) site. Thus, data is retrieved from the centralized data store, processed locally, and then sent back to the centralized data store.

6. **Should standards be centralized in a distributed data processing environment? Explain.**
Response: The relatively poor control environment imposed by the DDP model can be improved by establishing some central guidance. The corporate group can contribute to this goal by establishing and distributing to user areas appropriate standards for systems development, programming, and documentation.

7. **How can human behavior be considered one of the biggest potential threats to operating system integrity?**
Response: The purpose of segregation of duties is to deal with the potential negative aspects of human behavior including errors and fraud. The relationship between systems development (both new systems development and maintenance) and computer operations activities poses a potential risk that can circumvent operating system integrity. These functions are inherently incompatible. With detailed knowledge of application logic and control parameters and access to the computer's operating system and utilities, an individual could make unauthorized changes to the application during its execution.

8. **A bank in California has thirteen branches spread throughout northern California, each with its own minicomputer where its data are stored. Another bank has 10 branches spread throughout California, with its data stored on a mainframe in San Francisco. Which system do you think is more vulnerable to unauthorized access? Excessive losses from disaster?**
Response: The bank that has the data for all of its branches stored on one mainframe computer is at greater risk of access control. All of the firm's records are centrally housed. Once a perpetrator gains unauthorized access to the system, the data for all 10 branches are at risk. For the other bank the perpetrator would have to breach security for each of the thirteen branch computers. Thus, the bank with all of its data centrally stored on a mainframe is more vulnerable to access control. The primary disasters of concern in California are earthquakes and fires. The bank with a central mainframe in San Francisco is probably at the greatest risk of damage from both earthquakes and fires. If that system is destroyed, all of the branches lose their processing capability and, possibly, stored data.

9. **End-user computing has become extremely popular in distributed data processing organizations. The end users like it because they feel they can more readily design and implement their own applications. Does this type of environment always foster more efficient development of applications? Explain your answer**.
Response: Distributed data processing, if not properly managed, may result in duplication of efforts. Two or more individual end users may develop similar applications while completely unaware of each other's efforts. Such duplication is an inefficient use of human resources.

10. **Compare and contrast the following disaster recovery options: mutual aid pact, empty shell, recovery operations center, and internally provided backup. Rank them from most risky to least risky, as well as from most costly to least costly**.
Response: A mutual aid pact requires two or more organizations to agree to and trust each other to aid the other with data processing needs in the event of a disaster. This method is the lowest cost, but also somewhat risky. First, the host company must be trusted to scale back its own processing in order to process the transactions of the disaster-stricken company. Second, the firms must not be affected by the same disaster, or the plan fails. The next lowest cost method is internally provided backup. With this method, organizations with multiple data processing centers may invest in internal excess capacity and support themselves in the case of disaster in one data processing center. This method is not as risky as the mutual aid pact because reliance on another organization is not a factor. In terms of cost, the next highest method is the empty shell where two or more organizations buy or lease space for a data processing center. The space is made ready for computer installation; however, no computer equipment is installed. This method requires lease or mortgage payments as well as payment for air conditioning and raised floors. The risk in this method is that the hardware, software, and technicians may be difficult, if not impossible, to have available in the case of a natural disaster. Further, if multiple members' systems crash simultaneously, an allocation problem exists. The method with lowest risk and also the highest cost is the recovery operations center. This method takes the empty shell concept one step further—the computer equipment is actually purchased and software may even be installed. Assuming that this site is far enough away from the disaster-stricken area not to be affected by the disaster, this method can be a very good safeguard.

11. **Who should determine and prioritize the critical applications? How is this done? How frequently is it done?**
Response: The critical applications should be identified and prioritized by the user departments, accountants, and auditors. The applications should be prioritized based upon the impact on the short-run survival of the firm. The frequency with which the priorities need to be assessed depends upon the amount and kinds of changes that are made to systems over time. Firms that make changes frequently should reassess priorities frequently.

12. **Why is it easier for programmers to perpetrate a fraud than operators?**
Response: It is much easier for programmers to perpetrate a fraud because they know the code. They know how to get around some, or most, of the embedded controls. Better yet, some programmers deliberately program code that gets them around controls and allows them to commit fraud.

13. **Why should an organization centralize the acquisition, testing, and implementation of software and hardware within the corporate IT function?**

Response: The corporate IT group is better able to evaluate the merits of competing vendor software and hardware. A central, technically astute group such as this can evaluate systems features, controls, and compatibility with industry and organizational standards most efficiently. Test results can then be distributed to user areas as standards for guiding acquisition decisions.

14. **Organizations sometimes locate their computer centers in the basement of their buildings to avoid normal traffic flows. Comment on this practice.**
Response: Locating the computer center in the basement of a building can create an exposure to disaster risk such as floods. The Chicago Board of Trade computer center's systems were located in the basement of a multi-storied office building in Chicago. When the century-old water pipelines burst, part of the first floor and the entire basement flooded. Trade was suspended for several days until system functionality could be restored, causing the loss of millions of dollars. This disaster would have been prevented if the computer center had simply been located on the top floor—still away from normal traffic flows, but also away from the risk of flood.

15. **The 2003 blackout that affected the U.S. northeast caused numerous computer failures. What can an organization do to protect itself from such uncontrollable power failures?**
Response: The decision regarding power controls can be an expensive one and usually requires the advice and analysis of experts. The following, however, are options that can be employed. Voltage regulators and surge protectors provide regulated electricity, related to the level of electricity (frequency), and "clean" electricity, related to spikes and other potential hazards. Power outages and brownouts can generally be controlled with a battery backup (known as an uninterruptible power supply).

16. **Discuss a potential problem with ROCs**.
Response: Because of the heavy investment involved, ROCs are typically shared among many companies. The firms either buy shares in or become subscribers to the ROC, paying monthly fees for rights to its use. That situation does provide some risk because a widespread natural disaster may affect numerous entities in the same general geographic area. If multiple entities share the same ROC, some firm or firms will end up queued in a waiting line.

17. **Discuss two potential problems associated with a cold site.**
Response:
a. Recovery depends on the timely availability of the necessary computer hardware to restore the data processing function. Management must obtain assurances from hardware vendors that the vendor will give priority to meeting the organization's needs in the event of a disaster. An unanticipated hardware supply problem at this critical juncture could be a fatal blow.
b. With this approach there is the potential for competition among users for the shell resources, the same as for a hot site. For example, a widespread natural disaster, such as a flood or earthquake, may destroy the data processing capabilities of several shell members located in the same geographic area. Those affected by the disaster would be faced with a second major problem: how to allocate the limited facilities of the shell among them. The situation is analogous to a sinking ship that has an inadequate number of lifeboats.

18. **Discuss three techniques used to achieve fault tolerance**.
Response:
a. Redundant arrays of inexpensive (or independent) disks (RAID). There are several types of RAID configurations. Essentially, each method involves the use of parallel disks that contain redundant elements of data and applications. If one disk fails, the lost data are automatically reconstructed from the redundant components stored on the other disks.
b. Uninterruptible power supplies. In the event of a power outage, short-term backup power (i.e., battery power) is provided to allow the system to shut down in a controlled manner. This process will prevent the data loss and corruption that would otherwise result from an uncontrolled system crash.

19. **Explain the outsourcing risk of failure to perform.**
Response: Once a client firm has outsourced specific IT assets, its performance becomes linked to the vendor's performance. The negative implications of such dependency are illustrated in the financial problems that have plagued the huge outsourcing vendor Electronic Data Systems Cop. (EDS). In a cost-cutting effort, EDS terminated seven thousand employees, which impacted its ability to serve other clients. Following an eleven-year low in share prices, EDS stockholders filed a class-action lawsuit against the company. Clearly, vendors experiencing such serious financial and legal problems threaten the viability of their clients also.

20. **Explain vendor exploitation**.
Response: Once the client firm has divested itself of specific assets it becomes dependent on the vendor. The vendor may exploit this dependency by raising service rates to an exorbitant level. As the client's IT needs develop over time beyond the original contract terms, it runs the risk that new or incremental services will be negotiated at a premium. This dependency may threaten the client's long-term flexibility, agility, and competitiveness and result in even greater vendor dependency.

21. **Explain why reduced security is an outsourcing risk**.
Response: Information outsourced to off-shore IT vendors raises unique and serious questions regarding internal control and the protection of sensitive personal data. When corporate financial systems are developed and hosted overseas, and program code is developed through interfaces with the host company's network, US corporations are at risk of losing control of their information. To a large degree, US firms are reliant on the outsourcing vendor's security measures, data-access policies, and the privacy laws of the host country.

22. **Explain how IT outsourcing can lead to loss of strategic advantage.**
Response: Alignment between IT strategy and business strategy requires a close working relationship between corporate management and IT management in the concurrent development of business and IT strategies. This, however, is difficult to accomplish when IT planning is geographically redeployed off-shore or even domestically. Further, since the financial justification for IT outsourcing depends upon the vendor achieving economies of scale, the vendor is naturally driven toward seeking common solutions that may be used by many clients rather than creating unique solutions for each of them. This fundamental underpinning of IT outsourcing is inconsistent with the client's pursuit of strategic advantage in the marketplace.

23. **Explain the role of Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report in the review of internal controls**

Response: SSAE 16 is an internationally recognized third party attestation report designed for service organizations such as IT outsourcing vendors. SSAE 16, was promulgated by the Auditing Standards Board (ASB) of the AICPA and replaced Statement on Auditing Standards No. 70 (SAS 70). The SSAE 16 report, which is prepared by the service provider's auditor, attests to the fucntionallity of the vendor's system and the adequacy of its internal controls. This is the means by which an outsourcing vendor can obtain a single attest report that may be used by its clients' auditors and thus preclude the need for each client firm auditor to conduct its own audit of the vendor organization's facilities and internal controls.

24. **How do SSAE 16 Type 1 and Type 2 differ?**
Response:
The Type I report is the less rigorous of the two and comments only on the suitability of the controls' design. The Type II report goes further and assesses whether the controls are operating effectively based on tests conducted by the vendor organization's auditor.

25. **How are the Carve-out and Inclusive methods of reporting on subservice organizations different**?
Response:
Carve-out Method: When using the carve-out method, service provider management would exclude the subservice organization's relevant control objectives and related controls from the description of its system. The service provider must have controls in place to monitor the effectiveness of the controls at the subservice organization.
Inclusive Method: When using the inclusive method of subservice organization reporting the service provider's description of its system will include the services performed by the subservice organization. In addition the report will include the relevant control objectives and related controls of the subservice organization.

26. **Give two differences between ASP and SaaS**.
Response:
1) ASPs typically host the software of third-party software vendors, which is configured to the unique needs of the client organization. SaaS vendors typically develop and manage their own web-based software, which is general purpose and designed to serve multiple businesses.
2) ASP contracts are typically fixed-period or one-time licensing agreements. SaaS vendors often employ a subscription model in which clients pay as they go based on usage.

27. **Why is cloud computing not the best option for all companies?**
Response:
For smaller businesses, startup companies, and some new applications, the cloud concept is a promising alternative to in-house computing. The information needs of large companies, however, are often in conflict with the cloud solution. For example, large firms 1) have typically incurred massive investments in equipment, proprietary software, and human resources; 2) have mission-critical legacy system that cannot be migrated to the cloud; and 3) have esoteric information needs that are not served well by standardized solutions.

MULTIPLE CHOICE QUESTIONS

1. b
2. c
3. e
4. b
5. e
6. c
7. c
8. c
9. b
10. d

PROBLEMS

1. **Disaster Recovery Planning Controversy**

The relevance of a disaster recovery plan (DRP) to a financial statement audit is a matter of debate. Some argue that the existence of a DPR is irrelevant to the audit. Others argue that it is an important control that needs to be considered in the assessment of internal control.

Required:

Argue both side of this debate.

1) Provide a logical argument why a DRP should not be considered in the audit.

2) Argue why a DRP is an important control and should be reviewed within the conduct of a financial audit.

Response:

1) The DRP plays no role in the day-to-day operations of transaction processing. Financial statement audits focus on past period events. If no disaster occurred in the period under review, then the presence or absence of the DRP is irrelevant.

2) This argument is related to the going concern principle.

Investors invest in the future of an organization based in part on past financial performance.

The absence of a DRP, or a poorly designed DRP, is similar to a contingency.

How would investors respond to an organization that was vulnerable in some way, but had no contingency plan?

How would they respond if a disaster struck, and they had not been informed in the audit report that the organization had no DRP in place?

2. **Internal Control**

During its preliminary review of the financial statements of Barton, Inc., Simon and Associates, CPA discovered a lack of proper segregation of duties between the programming and operating functions in Barton's data center. They discovered that some new systems development programmers also filled in as operators on occasion. Simon and Associates extended the internal control review and test of controls and concluded in its final report that sufficient compensating general controls provided reasonable

assurance that the internal control objectives were being met.
Required:
What compensating controls are most likely in place?

Response: Compensating controls that Barton, Inc found may include:

- mandatory vacations for all employees
- operators are prohibited from running systems that they helped develop
- end users review output reports and note any exceptions
- adequate supervision of all ITOperations
- access log identifies the time and duration of all access to data center
- no system documentation is stored in the data center
- periodic comparison of program code to an archived copy
- use of a computer activity log to identify which operators ran which programs, when they ran, and how long they ran.

3. **Physical Security**

Big Apple Financials, Inc., is a financial services firm located in New York City. The company keeps client investment and account information on a server at its Brooklyn data center. This information includes the total value of the portfolio, type of investments made, the income structure of each client, and associated tax liabilities. The company has recently upgraded its Web site to allow clients to access their investment information. The company's data center is in the basement of a rented building. Company management believes that the location is secure enough to protect their data from physical threats. The servers are housed in a room that has smoke detectors and associated sprinklers. It is enclosed, with no windows, and has temperature-controlled air conditioning. The company's auditors, however, have expressed concern that some of the measures at the current location are inadequate and that newer alternatives should be explored. Management has expressed counter concerns about the high cost of purchasing new equipment and relocating its data center.
Required:

1**.** Why are Big Apple's auditors stressing the need to have a better physical environment for the server?
2. Describe six control features that contribute to the physical security of the computer center.
3**.** Big Apple management is concerned about the cost of relocating the data center. Discuss some options open to them that could reduce their operating costs and provide the security the auditor's seek.

Response:
1. When talking of the physical environment, the auditors are not just talking of the potential threat of physical intruders and sabotage, but also of environmental hazards such as fires, floods, wind, earthquakes, or power outages. Though these occurrences are relatively rare, they still should be accounted for, as they can seriously hamper operations. The company would not only just lose the investment in servers and computer systems but also the data and ability to do business. Software checks cannot prevent such losses. Big Apple needs to have a workable disaster recovery plan in place.

2.

a. Physical Location: The physical location of the computer center affects the risk of disaster directly. The computer center should be away from human-made and natural hazards, such as processing plants, gas and water mains, airports, high-crime areas, flood plains, and geological faults.

b. Construction: Ideally, a computer center should be located in a single-store building of solid concrete with controlled access. Utility and communication lines should be underground. The building windows should not be open. An air filtration system should be in place that is capable of excluding dust, pollen, and dust mites.

c. Access: Access should be limited to operators and other employees who work there. Programmers and analysts who need access to correct program errors should be required to sign in and out. The computer center should maintain accurate records of all such events to verify access control. The main entrance to the computer center should be through a single door, though fire exists with alarms are important. Lose circuit camera with video recording is also highly advisable.

d. Air Conditioning: Mainframes and servers, as in the case with Avatar, have heavy processing volumes. These are designed to work at their optimal levels only within a narrow range of conditions, most importantly the temperature. Computers operate best in a temperature range of 70 to 75 degrees Fahrenheit and a relative humidity of 50 percent. Logic errors and static electricity risks can be mitigated by proper use of air conditioning.

e. Fire Suppression: The major features should include automatic and manual alarms (placed in strategic locations connected to fire stations), an automatic fire extinguishing system (not water sprinklers, rather carbon dioxide or halon extinguishers should be used), a manual fire extinguisher, and clearly marked and illuminated fire exists.

f. Fault Tolerance Controls: Commercially provided electrical power presents several problems that can disrupt the computer centers operations including total power failures, brownouts, and power fluctuation. The company should look into the use of surge protectors, generators, batteries, and voltage regulators in order to protect their computer system from the negative effects associated with these disruptions.

3. The company could look into the outsourcing option. This may involve either traditional outsourcing or the more flexible cloud computing approach, depending on the nature of the applications that Big Apple uses in its operations. SaaS and IaaS options are readily available for financial services firms.

Outsourcing vendors that are SSAE 16 certified will have adequate disaster recovery and security features in place. Since outsourcing vendor can earn economies of scale, the cost of service and security can be provided at a lower cost that Big Apple could achieve independently.

4. **Disaster Recovery Plans**

The headquarters of Hill Crest Corporation, a private company with $15.5 million in annual sales, is located in California. Hill Crest provides for its 150 clients an online legal software service that includes data storage and administrative activities for law offices. The company has grown rapidly since its inception 3 years ago, and its data processing department has expanded to accommodate this growth. Because Hill Crest's president and sales personnel spend a great deal of time out of the office developing new clients, the planning of the IT facilities has been left to the data processing professionals.

Hill Crest recently moved its headquarters into a remodeled warehouse on the outskirts of the city. While remodeling the warehouse, the architects retained much of the original structure, including the wooden-shingled exterior and exposed wooden beams throughout

the interior. The distributive processing computers and servers are situated in a large open area with high ceilings and skylights. The openness makes the data center accessible to the rest of the staff and promotes a team approach to problem solving. Before occupying the new facility, city inspectors declared the building safe; that is, it had adequate fire extinguishers, sufficient exits, and so on.

In an effort to provide further protection for its large database of client information, Hill Crest instituted a tape backup procedure that automatically backs up the database every Sunday evening, avoiding interruption in the daily operations and procedures. All tapes are then labeled and carefully stored on shelves reserved for this purpose in the data processing department. The departmental operator's manual has instructions on how to use these tapes to restore the database, should the need arise. A list of home phone numbers of the individuals in the data processing department is available in case of an emergency. Hill Crest has recently increased its liability insurance for data loss from $50,000 to $100,000.

This past Saturday, the Hill Crest headquarters building was completely ruined by fire, and the company must now inform its clients that all of their information has been destroyed.

Required:

a. Describe the computer security weaknesses present at Hill Crest Corporation that made it possible for a disastrous data loss.

b. List the components that should have been included in the disaster recovery plan at Hill Crest Corporation to ensure computer recovery within 72 hours.

c. What factors, other than those included in the plan itself

Response:

a. The computer security weaknesses present at Hill Crest Corporation that made it possible for a disastrous data lost to occur include:

- Not housing the data-processing facility in a building constructed of fire-retardant materials, and instead using one with exposed wooden beams and a wooden-shingled exterior.
- The absence of a sprinkler (halon) system and a fire-suppression system under a raised floor; fire doors.
- An on-line system with infrequent (weekly) tape backups. Backups, with checkpoints and restarts, should be performed at least daily. "Grandfather" and "Father" backup files should be retained at a secure off-site storage location.
- Data and programs should have been kept in a library separate from the data-processing room, with the library area constructed of fire-retardant materials.
- Lack of a written disaster recovery plan with arrangements in place to use an alternate off-site computer center in the event of a disaster or an extended service interruption. There was a phone list of DP personnel, but without assigned responsibilities as to actions to be taken when needed.
- Lack of complete systems documentation kept outside the data-processing area.

b. The components that should have been included in the disaster recovery plan at Hill Crest Corporation to ensure computer recovery within 72 hours include the following:

- A written disaster recovery plan should be developed with review and approval by senior management, data-processing management, end-user management, and internal audit.
- Backup data and programs should be stored at an off-site location that will quickly accessible in the event of an emergency.

- The disaster recovery team should be organized. Select the disaster recovery manager, identify the tasks, segregate into teams, develop an organizational chart for disaster procedures, match personnel to team skills and functions, and assign duties and responsibilities to each member.
- The duties and responsibilities of the recovery team include:
    - Obtaining use of a previously arranged alternate data-processing facility; activating the backup system and network, and
    - Retrieving backup data files and programs, restoring programs and data, processing critical applications, and reconstructing data entered into the system subsequent to latest saved backup/ restart point.

c. Factors, other than those included in the disaster recovery plan itself, that should be considered when formulating the plan include:

- Arranging business interruption insurance in addition to liability insurance.
- Ensuring that all systems' and operations' documentation is kept up to date and is easily accessible for use in case of a disaster.
- Performing a risk/ cost analysis to determine the level of expense that may be justified to obtain reasonable, as opposed to certain, assurance that recovery can be accomplished in 72 hours.

5. Segregation of Duties

Arcadia Plastics follows the philosophy of transferring people from job to job within the organization. Management believes that job rotation deters employees from feeling that they are stagnating in their jobs and promotes a better understanding of the company. A computer services employee typically works for six months as a data librarian, one year as a systems developer, six months as a database administrator, and one year in systems maintenance. At that point, he or she is assigned to a permanent position.

Required:
Discuss the importance of separation of duties within the information systems department.
How can Arcadia Plastics have both job rotation and well-separated duties?

Response: Because the employee will have performed several highly incompatible tasks, this company needs to employ strong password access controls and constantly require its employees to change their passwords. This is especially necessary because these employees have either designed or viewed authorization access tables. Strong controls over program maintenance, such as program modification reports, are also a necessity. The key is that when an employee transfers from one job to another, she or he should have no access to functions in previous positions.

6. **DDP Risks**

Write an essay discussing the primary risks associated with the distributed processing environment.

Response:
Potential risks associated with DDP include the inefficient use of resources, the destruction of audit trails, inadequate segregation of duties, an increased potential for programming errors and systems failures, and the lack of standards.

a. Inefficient use of resources. Several risks are associated with inefficient use of organizational resources in the DDP environment.

- First, is the risk of mismanagement of organization-wide resources, particularly by end users. Some argue that when organization-wide resources exceed a threshold amount, perhaps 5 percent of the total operations budget, they should be controlled and monitored centrally.
- Second, is the risk of hardware and software incompatibility, again primarily by end users. Distributing the responsibility for hardware and software purchases to end-users may result in uncoordinated and poorly conceived decisions. For example, decision makers in different organizational units working independently may settle on dissimilar and incompatible operating systems, technology platforms, database programs and office suites.
- Third, is the risk of redundant tasks associated with end-user activities and responsibilities. Autonomous systems development throughout the firm can result in each user area reinventing the wheel. For example, application programs created by one user, which could be used with little or no change by others, will be designed from scratch rather than shared.

b. Destruction of audit trail. The use of DDP can adversely affect the audit trail. Because audit trails in modern systems tend to be electronic, it is not unusual for the electronic audit trail to exist in part, or in whole, on end-user computers. Should the end user inadvertently delete the audit trail, it could be lost and unrecoverable. Or if an end user inadvertently inserted uncontrolled errors into the audit log, the audit trail could effectively be destroyed. Numerous other risks are associated, including care of the hardware itself.

c. Inadequate segregation of duties. The distribution of IT services to users may result in the creation of many small units that do not permit the necessary separation of incompatible functions. For example, within a single unit, the same person may write application programs, perform program maintenance, enter transaction data into the computer, and operate the computer equipment. This condition would be a fundamental violation of internal control.

d. Hiring qualified professionals. End-user managers may lack the knowledge to evaluate the technical credentials and relevant experience of candidates applying for positions as computer professionals. Also, if the organizational unit into which a new employee is entering is small, the opportunity for personal growth, continuing education, and promotion may be limited. For these reasons, managers may experience difficulty attracting highly qualified personnel. The risk of programming errors and system failures increases directly with the level of employee incompetence.

e. Lack of standards. Because of the distribution of responsibility in the DDP environment, standards for developing and documenting systems, choosing programming languages, acquiring hardware and software, and evaluating performance may be unevenly applied or nonexistent.

7. **Cloud Based Recovery Service Provider**

Visit SunGard's Web site, http://www.sungard.com, and research its Recovery2Cloud services offered. Write a report of your findings.

Response:

SunGard Recover2Cloud[SM] Services are a suite of cloud based customizable solutions for recovery of an organization's critical applications.

SunGard creats the a mix of services to support the recovery objectives of each customers applications.

SunGard takes full responsibility for recovery

SunGard claims to reduce recovery costs by 30-50% compared to recovery on physical systems.

Recovery2Cloud features include:

- Contractual service-level agreements that guarantee specific recovery time and recovery point objectives
- Fully managed recovery services with testing and recovery performed by SunGard experts
- Multiple availability options built to fit customer needs and budget
- Cloud deployment alternatives including public and private clouds

Recover2Cloud Options Include:

Recover2Cloud for Server Replication

- Supports near-zero recovery point objectives (the amount of time data are lost)
- Recovery time objectives of less than four hours.
- Incorporates Continuous Data Protection to enable recovery to any point in time within several days prior to a failure.

Recover2Cloud Storage Replication

- For large virtual environments,
- Supports less than four-hour recovery time objectives and near-zero recovery point objectives by replicating data to networked storage devices at a SunGard facility.

Recover2Cloud for Vaulting

Vaulting is the process of sending data off-site, where it can be protected from hardware failures, theft, and other threats. Backup services compress, encrypt, and periodically transmit customer data to a remote vault. In most cases the vaults will feature auxiliary power supplies, powerful computers, and manned security

- SunGard Recover2Cloud for Vaulting supports recovery time objectives of less than 12 hours,
- Provides de-duplicated backup copies of data stored in a secure vault at a SunGard location, in close proximity to recovery infrastructure.
- Claim reduction in total cost by 35% or more when compared to an in-house solution.

8. **Internal Control Responsibility for Outsourced IT**

Explain why managers who outsource their IT function may or may not also outsource responsibility for IT controls. What options are open to auditors regarding expressing an opinion on the adequacy of internal controls?

Response:
Management may outsource their organizations' IT functions, but they cannot outsource their management responsibilities under SOX for ensuring adequate IT internal controls. The PCAOB specifically states in its Auditing Standard No. 2, "The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Rather, user management should evaluate controls at the service organization, as well as related controls at the user company, when making its assessment about internal control over financial reporting." Therefore, if an audit client firm outsources its IT function to a vendor that processes its transactions, hosts key data, or performs other significant services, the auditor will need to conduct an evaluation of the vendor organization's controls, or alternatively obtain a SSAE 16 report from the service provider organization.

9. **Competing Schools of Thought Regarding Outsourcing**

Explain the *core competency* argument for outsourcing and compare/ contrast it with *TCE theory*. Why does one theory tend to prevail over the other in making outsourcing decisions?

Response:
Core competency theory argues that an organization should focus exclusively on its core business competencies while allowing outsourcing vendors to efficiently manage the non-core areas such as the IT functions. This premise, however, ignores an important distinction between commodity and specific IT assets.
Commodity IT assets are not unique to a particular organization and are thus easily acquired in the marketplace. These include such things as network management, systems operations, server maintenance, and help-desk functions. Specific IT assets, in contrast, are unique to the organization and support its strategic objectives. Because of their idiosyncratic nature, specific assets have little value outside of their current use. Such assets may be tangible (computer equipment), intellectual (computer programs), or human. Examples of specific assets include systems development, application maintenance, data warehousing, and highly skilled employees trained to use organization-specific software.
Transaction Cost Economics (TCE) theory is in conflict with the core competency school by suggesting that firms should retain certain specific non-core IT assets in house. Because of their esoteric nature specific assets cannot be easily replaced once they are given up in an outsourcing arrangement. Therefore, if the organization should decide to cancel its outsourcing contract with the vendor, it may not be able to return to its pre-outsource state. On the other hand, TCE theory supports the outsourcing of commodity assets, which are easily replaced or obtained from alternative vendors.

Naturally, a CEO's perception of what constitutes commodity IT assets plays an important role in IT outsourcing decisions. Often this comes down to a matter of definition and interpretation. For example, most CEOs would define their IT function as a non-core commodity, unless they are in the business of developing and selling IT applications. Consequently, a belief that all IT can, and should, be managed by large service organizations tends to prevail. Such misperception reflects, in part, both lack of executive education and dissemination of faulty information regarding the virtues and limitations of IT outsourcing g.

10. **Distributed Processing System**

The internal audit department of a manufacturing company conducted a routine examination of the company's distributed computer facilities. The auditor's report was critical of the lack of coordination in the purchase of PC systems and software that individual departments use. Several different hardware platforms, operating systems, spreadsheet packages, database systems, and networking applications were in use.

In response to the internal audit report, and without consulting with department users regarding their current and future system needs, Marten, the Vice President of Information Services, issued a memorandum to all employees stating the following new policies:

1. The Micromanager Spreadsheet package has been selected to be the standard for the company, and all employees must switch to it within the month.
2. All future PC purchases must be Megasoft compatible.
3. All departments must convert to the Megasoft Entree database package.
4. The office of the Vice President of Information Services must approve all new hardware and software purchases.

Several managers of other operating departments have complained about Marten's memorandum. Apparently, before issuing this memo, Marten had not consulted with any of the users regarding their current and future software needs.

Required

a. When setting systems standards in a distributed processing environment, discuss the pertinent factors about:
1. Computer hardware and software considerations.
2. Controls considerations.

b. Discuss the benefits of having standardized hardware and software across distributed departments in the firm.

c. Discuss the concerns that the memorandum is likely to create for distributed users in the company.

Response

a.

1. Computer hardware factors that need to be considered include:
understanding the primary applications for which the equipment will be used. the operating system for each type of hardware and whether appropriate software is available for the desired applications. file options such as hard disk drives, Zip drive, floppy diskettes, or CDROM, communication considerations such as interface between microcomputer(LANs), mainframe compatibility for downloading and uploadininformation, and technical specifications of communication protocol.
2. Controls considerations include:

clear, well-written, tested documentation for hardware and software; adequate maintenance contracts, and software support; adequate user training
adequate security provisions for file protection, effective password policy, appropriate database access authority, backup procedures for internal record integrity, and off-site storage procedures for disaster recovery

b. The benefits of having standardized hardware and software include:
cost savings from quantity discounts and multiple use of software licensing agreements. technological growth capabilities such as network compatibility.
standardized and centralized system backup procedures for both hardware and software and provisions for facility sharing in the event of breakdowns.
improved standard operating procedures and software implementation through experience by a large user base with distributed knowledge.

c. The memorandum is likely to create the following concerns:
The memorandum suggests a lack of understanding of user needs that may inhibit their cooperation.
The new policy does not provide for an adequate transition period for converting existing department applications to the prescribed ones.

11. Describe the key features of cloud computing.

Response:

The key features of cloud computing are:

- Client firms acquire IT resources from vendors on demand and as needed. This is in contrast to the traditional IT outsourcing model in which resources are provided to client firms in strict accordance with long-term contracts that stipulate services and time frames.
- Resources are provided over a network (private or Internet) and accessed through network terminals at the client location.
- Acquisition of resources is rapid and infinitely scalable. A client can expand and contract the service demanded almost instantly and often automatically.

Computing resources are pooled to meet the needs of multiple client firms. A consequence of this, however, is that an individual client has no control over, or knowledge of, the physical location of the service being provided.

12. **Service Provider Audit**
The Harvey Manufacturing Company is undergoing its annual financial statement audit. Last year the company purchased a SaaS application from Excel Systems (a cloud service provider) to run mission critical financial transactions. The SaaS application runs on an IaaS server, which Excel Systems outsourced to another service provider.
Required:

Explain how the Harvey Manufacturing auditors will assess the relevant internal controls related to these mission critical transactions.
Response:

The auditor would either need to audit the controls at service provider and subservice provider locations, or rely on a SSAE 16 report from the primary service provider. Since a subservice organization is involved, its relevant controls over the mission critical application must also be assessed. Two reporting techniques for subservice providers are:

Carve-out Method. When using the carve-out method, service provider management would exclude the subservice organization's relevant control objectives and related controls from the description of its system. The description would, however, include the nature of the services performed by the subservice organization. Typically the service provider would obtain an SSAE 16 from the subservice organization, and must have controls in place to monitor the effectiveness of the controls at the subservice organization.

Inclusive Method. When using the inclusive method of subservice organization reporting the service provider's description of its system will include the services performed by the subservice organization. In addition the report will include the relevant control objectives and related controls of the subservice organization.