Chapter 2— Auditing IT Governance Controls

TRUE/FALSE

1. To fulfill the segregation of duties control objective, computer processing functions (like authorization of credit and billing) are separated.

   ANS: F PTS: 1

2. To ensure sound internal control, program coding and program processing should be separated.

   ANS: T PTS: 1

3. Some systems professionals have unrestricted access to the organization's programs and data.

   ANS: T PTS: 1

4. IT governance focuses on the management and assessment of strategic IT resources

   ANS: T PTS: 1

5. Distributed data processing places the control IT recourses under end users.

   ANS: T PTS: 1

6. An advantage of distributed data processing is that redundant tasks are greatly eliminated

   ANS: F PTS: 1

7. Certain duties that are deemed incompatible in a manual system may be combined in a computer-based information system environment.

   ANS: T PTS: 1

8. To improve control and efficiency, new systems development and program maintenance should be performed by the same individual or group.

   ANS: F PTS: 1

9. Distributed data processing reduces the risk of operational inefficiencies.

   ANS: F PTS: 1

10. The database administrator should be separated from systems development.

    ANS: T PTS: 1

11. A disaster recovery plan is a comprehensive statement of all actions to be taken after a disaster.

    ANS: T PTS: 1

12. RAID is the use of parallel disks that contain redundant elements of data and applications.

    ANS: T PTS: 1

13. Transaction cost economics (TCE) theory suggests that firms should outsource specific non–core IT assets

    ANS: F PTS: 1

14. Commodity IT assets easily acquired in the marketplace and should be outsourced under the core competency theory.

    ANS: F PTS: 1

15. A database administrator is responsible for the receipt, storage, retrieval, and custody of data files.

    ANS: F PTS: 1

16. Virtualization is the technology that unleased cloud computing.

    ANS: T PTS: 1

17. 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.

    ANS: T PTS: 1

18. An often-cited benefit of IT outsourcing is improved core business performance.

    ANS: T PTS: 1

19. Commodity IT assets include such things are network management.

    ANS: T PTS: 1

20. Specific IT assets support an organization’s strategic objectives.

    ANS: T PTS: 1

21. A generally accepted advantage of IT outsourcing is improved security.

    ANS: F PTS: 1

22. An advantage of distributed data processing is that individual end user groups set specific IT standards without concern for the broader corporate needs.

    ANS: F PTS: 1

23. A mutual aid is the lowest cost disaster recovery option, but has shown to be effective and low risk.

    ANS: F PTS: 1

24. Critical applications should be identified and prioritized by the user departments, accountants, and auditors.

    ANS: T PTS: 1

25. A ROC is generally shared with multiple companies.

    ANS: T PTS: 1

MULTIPLE CHOICE

1. All of the following are issues of computer security except
   a. releasing incorrect data to authorized individuals
   b. permitting computer operators unlimited access to the computer room
   c. permitting access to data by unauthorized individuals
   d. providing correct data to unauthorized individuals

   ANS: B PTS: 1

2. Segregation of duties in the computer-based information system includes
   a. separating the programmer from the computer operator
   b. preventing management override
   c. separating the inventory process from the billing process
   d. performing independent verifications by the computer operator

   ANS: A PTS: 1

3. In a computer-based information system, which of the following duties needs to be separated?
   a. program coding from program operations
   b. program operations from program maintenance
   c. program maintenance from program coding
   d. all of the above duties should be separated

   ANS: D PTS: 1

4. Participation in system development activities include:
   a. system analysts, database designers and programmers
   b. managers and operating personnel who work directly with the system
   c. accountants and auditors
   d. all of the above

   ANS: D PTS: 1

5. Adequate backups will protect against all of the following except
   a. natural disasters such as fires
   b. unauthorized access
   c. data corruption caused by program errors
   d. system crashes

   ANS: B PTS: 1

6. Which is the most critical segregation of duties in the centralized computer services function?
   a. systems development from data processing
   b. data operations from data librarian
   c. data preparation from data control
   d. data control from data librarian

   ANS: A PTS: 1

7. Systems development is separated from data processing activities because failure to do so
   a. weakens database access security
   b. allows programmers access to make unauthorized changes to applications during execution
   c. results in inadequate documentation
   d. results in master files being inadvertently erased

   ANS: B PTS: 1

8. Which organizational structure is most likely to result in good documentation procedures?
   a. separate systems development from systems maintenance
   b. separate systems analysis from application programming
   c. separate systems development from data processing
   d. separate database administrator from data processing

   ANS: A PTS: 1

9. All of the following are control risks associated with the distributed data processing structure except
   a. lack of separation of duties
   b. system incompatibilities
   c. system interdependency
   d. lack of documentation standards

   ANS: C PTS: 1

10. Which of the following is not an essential feature of a disaster recovery plan?
    a. off-site storage of backups
    b. computer services function
    c. second site backup
    d. critical applications identified

    ANS: B PTS: 1

11. A cold site backup approach is also known as
    a. internally provided backup
    b. recovery operations center
    c. empty shell
    d. mutual aid pact

    ANS: C PTS: 1

12. The major disadvantage of an empty shell solution as a second site backup is
    a. the host site may be unwilling to disrupt its processing needs to process the critical applications of the disaster stricken company
    b. recovery depends on the availability of necessary computer hardware
    c. maintenance of excess hardware capacity
    d. the control of the shell site is an administrative drain on the company

    ANS: B PTS: 1

13. An advantage of a recovery operations center is that
    a. this is an inexpensive solution
    b. the initial recovery period is very quick
    c. the company has sole control over the administration of the center
    d. none of the above are advantages of the recovery operations center

    ANS: B PTS: 1

14. For most companies, which of the following is the least critical application for disaster recovery purposes?
    a. month-end adjustments
    b. accounts receivable
    c. accounts payable
    d. order entry/billing

    ANS: A PTS: 1

15. The least important item to store off-site in case of an emergency is
    a. backups of systems software
    b. backups of application software
    c. documentation and blank forms
    d. results of the latest test of the disaster recovery program

    ANS: D PTS: 1

16. Some companies separate systems analysis from programming/program maintenance. All of the following are control weaknesses that may occur with this organizational structure except
    a. systems documentation is inadequate because of pressures to begin coding a new program before documenting the current program
    b. illegal lines of code are hidden among legitimate code and a fraud is covered up for a long period of time
    c. a new systems analyst has difficulty in understanding the logic of the program
    d. inadequate systems documentation is prepared because this provides a sense of job security to the programmer

    ANS: C PTS: 1

17. All of the following are recommended features of a fire protection system for a computer center except
    a. clearly marked exits
    b. an elaborate water sprinkler system
    c. manual fire extinguishers in strategic locations
    d. automatic and manual alarms in strategic locations

    ANS: B PTS: 1

18. All of the following tests of controls will provide evidence about the physical security of the computer center except
    a. review of fire marshal records
    b. review of the test of the backup power supply
    c. verification of the second site backup location
    d. observation of procedures surrounding visitor access to the computer center

    ANS: C PTS: 1

19. All of the following tests of controls will provide evidence about the adequacy of the disaster recovery plan except
    a. inspection of the second site backup
    b. analysis of the fire detection system at the primary site
    c. review of the critical applications list
    d. composition of the disaster recovery team

    ANS: B PTS: 1

20. The following are examples of commodity assets except
    a. network management
    b. systems operations
    c. systems development
    d. server maintenance

    ANS: C PTS: 1

21. Which of the following is NOT an example of a specific assets?
    a. application maintenance
    b. data warehousing
    c. highly skilled employees
    d. server maintenance

    ANS: D PTS: 1

22. Which of the following is true?
    a. Core competency theory argues that an organization should outsource specific core assets.
    b. Core competency theory argues that an organization should focus exclusively on its core business competencies
    c. Core competency theory argues that an organization should not outsource specific commodity assets.
    d. Core competency theory argues that an organization should retain certain specific non−core assets in-house.

    ANS: B PTS: 1

23. Which of the following is not true?
    a. Large-scale IT outsourcing involves transferring specific assets to a vendor
    b. Specific assets, while valuable to the client, are of little value to the vendor
    c. Once an organization outsources its specific assets, it may not be able to return to its pre-outsource state.
    d. Specific assets are of value to vendors because, once acquired, vendors can achieve economies of scale by employing them with other clients

    ANS: D PTS: 1

24. Which of the following is not true?
    a. When management outsources their organization's IT functions, they also outsource responsibility for internal control.
    b. Once a client firm has outsourced specific IT assets, its performance becomes linked to the vendor's performance.
    c. IT outsourcing may affect incongruence between a firm's IT strategic planning and its business planning functions.
    d. The financial justification for IT outsourcing depends upon the vendor achieving economies of scale.

    ANS: A PTS: 1

25. Which of the following is not true?
    a. Management may outsource their organizations' IT functions, but they cannot outsource their management responsibilities for internal control.
    b. Section 404 requires the explicit testing of outsourced controls.
    c. The SSAE 16 report, which is prepared by the outsourcer's auditor, attests to the adequacy of the vendor's internal controls.
    d. Auditors issue two types of SSAE 16 reports: Type I report and Type II report.

    ANS: C PTS: 1

26. Segregation of duties in the computer-based information system includes
    a. separating the programmer from the computer operator
    b. preventing management override
    c. separating the inventory process from the billing process
    d. performing independent verifications by the computer operator

    ANS: A PTS: 1

27. A disadvantage of distributed data processing is
    a. the increased time between job request and job completion.
    b. the potential for hardware and software incompatibility among users.
    c. the disruption caused when the mainframe goes down.
    d. that users are not likely to be involved.

    ANS: B PTS: 1

28. Which of the following is NOT a control implication of distributed data processing?
    a. redundancy
    b. user satisfaction
    c. incompatibility
    d. lack of standards

    ANS: B PTS: 1

29. Which of the following disaster recovery techniques may be least optimal in the case of a disaster?
    a. empty shell
    b. mutual aid pact
    c. recovery operation center
    d. they are all equally beneficial

    ANS: B PTS: 1

30. Which of the following is a feature of fault tolerance control?
    a. interruptible power supplies
    b. RAID
    c. DDP
    d. MDP

    ANS: B PTS: 1

31. Which of the following disaster recovery techniques is has the least risk associated with it?
    a. empty shell
    b. ROC
    c. internally provided backup
    d. they are all equally risky

    ANS: C PTS: 1

32. Cloud computing
    a. pools resources to meet the needs of multiple client firms
    b. allows clients to expand and contract services almost instantly
    c. both a. and b.
    d. neither a. not b.

    ANS: C PTS: 1

SHORT ANSWER

1. What is the purpose of a data library?

   ANS:

   A data libray is a room adjacent to the computer center that provides safe storage for the off-line data files. The files could be backups or current data files.

   PTS: 1

2. What are the three primary IT functions that must be separated?

   ANS:

   The three primary IT functions that must be separated are as follows:

   a. separate systems development from computer operations,
   b. separate the database administrator from other functions and systems development, and
   c. separate new systems development from maintenance.

   PTS: 1

3. What are the advantages of separting new systems development from systems maintenance?

   ANS:

   Documentation standards are improved because the maintenance group requires documentation to perform its maintenance duties. Denying the original programmer future access to the program deters program fraud.

   PTS: 1

4. What problems may occur as a result of combining applications programming and maintenance tasks into one position?

   ANS:

   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 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.

   PTS: 1

5. Why is poor-quality systems documentation a prevalent problem?

   ANS:

   Systems professionals do not find this documenting systems as interesting as the design, testing, and implementation steps. Further, the systems professionals are typically eager or pressured to move on to another project before documentation is complete. Job security is another reason for poor systems documentation. When a system is poorly documented it is difficult to interpret, test and debug. Therefore, the programmer who understands the system becomes relatively indispensable. When the programmer leaves, a new programmer inherits maintenance responsibility for the undocumented system. Depending on the complexity, the transition period may be long and costly.

   PTS: 1

6. What is RAID?

   ANS:

   RAID is 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.

   PTS: 1

7. What are some risks associated with DDP?

   ANS:

   Inefficient use of resources, destruction of audit trails, inadequate segregation of duties, hiring qualified professionals, lack of standards

   PTS: 1

8. For disaster recovery purposes, what criteria are used to identify an application or data as critical?

ANS:

Critical application and files are those that impact the short-run survival of the firm. Critical items impact cash flows, legal obligations, and customer relations.

PTS: 1

9. List three pairs of system functions that should be separated in the centralized computer services organization. Describe a risk exposure if the functions are not separated.

Functions to Separate	Risk Exposure
_____	_____
_____	_____
_____	_____

ANS:

separate systems development from data processing operations (unauthorized changes to application programs during execution),
separate database administrator from systems development (unauthorized access to database files),
separate new systems development from systems maintenance (writing fraudulent code and keeping it concealed during maintenance),
separate data library from computer operations (loss of files or erasing current files)

PTS: 1

10. Describe the components of a disaster recovery plan.

ANS:

Every disaster recovery plan should:
designate a second site backup
identify critical applications
perform backup and off-site storage procedures
create a disaster recovery team
test the disaster recovery plan

PTS: 1

11. What is a mirrored data center?

    ANS:

    A mirrored data center duplicates programs and data onto a computer at a separate location. Mirroring is performed for backup purposes.

    PTS: 1

12. What is a recovery operations center? What is its purpose?

    ANS:

    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.

    PTS: 1

13. The distributed data processing approach carries some control implications of which accountants should be aware. Discuss two.

    ANS:

    Incompatibility of hardware and software, selected by users working independently, can result in system incompatibility that can affect communication.

    When individuals in different parts of the organization "do their own thing," there can be significant redundancy between units.

    When user areas handle their own computer services functions, there may be a tendency to consolidate incompatible activities.

    Small units may lack the ability to evaluate systems professionals and to provide adequate opportunities and may therefore have difficulty acquiring qualified professionals.

    As the number of units handling systems tasks, there is an increasing chance that the systems will lack standards.

    PTS: 1

14. Describe two tests that an auditor would perform to ensure that the disaster recovery plan is adequate.

    ANS:

    Review second site backup plan, critical application list, and off-site backups of critical libraries, applications and data files; ensure that backup supplies, source documents and documentation are located off-site. Review which employees are members of the disaster recovery team.

    PTS: 1

15. What is an auditor looking for when testing computer center controls?

    ANS:

    When testing computer center controls, the auditor is trying to determine that the physical security controls are adequate to protect the organization from physical exposures, that insurance coverage on equipment is adequate, that operator documentation is adequate to deal with operations and failures, and that the disaster recovery plan is adequate and feasible.

    PTS: 1

16. What is IT Governance?

    ANS:

    IT governance is a broad concept relating to the decision rights and accountability for encouraging desirable behavior in the use of IT. Three aspects of IT governance are of particular importance to SOX compliance: organizational structure of the IT function, computer operations, and disaster recovery planning.

    PTS: 1

17. Why should the tasks of systems development and maintenance be segregated from operations?

    ANS:

    The segregation of systems development (both new systems development and maintenance) and operations activities is of the greatest importance. Systems development and maintenance professionals acquire (by in-house development and purchase) and maintain systems for users. Operations staff should run these systems and have no involvement in their design and implementation. Consolidating these functions invites fraud. With detailed knowledge of an application's logic and control parameters along with access to the computer operations, an individual could make unauthorized changes to application logic during execution. Such changes may be temporary (on the fly.) and will disappear with little or no trace when the application terminates.

    PTS: 1

18. Briefly explain the core-competency theory.

ANS:
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.

PTS: 1

19. What are commodity IT assets?

ANS:
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.

PTS: 1

20. Briefly outline transaction cost economics as it relates to IT outsourcing.

ANS:
Transaction cost economics 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.

PTS: 1

21. What is contained in the SSAE 16 attest report?

ANS:

The SSAE attest report provides a description of the service provider's system including details of how transactions are processed and results are communicated to their client organizations. The report also describes relevant internal control issues consistent with the COSO control model, specific control objectives and the controls designed to achieve those objectives.

PTS: 1

22. What are the often cited benefits of IT outsourcing?

ANS:

Oft-cited benefits of IT outsourcing include improved core business performance, improved IT performance (due to the vendor's expertise), and reduced IT costs.

PTS: 1

23. Define specific asset.

    ANS:

    Specific IT 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.

    PTS: 1

24. List five risks associated with IT outsourcing.

    ANS:

    Failure to Perform
    Vendor Exploitation
    Outsourcing Costs Exceed Benefits
    Reduced Security
    Loss of strategic advantage.

    PTS: 1

25. What are the objectives of IT Governance?

    ANS:
    Key objectives of IT governance are to reduce risk and ensure that investments in IT resources add value to the corporation.

    PTS: 1

ESSAY

1. Describe how a Corporate Computer Services Function can overcome some of the problems associated with distributed data processing.

   ANS:
   The Corporate Computer Services Function may provide the following technical advice and expertise to distributed data processing units:
   central testing of commercial software and hardware;
   installation of new software;
   trouble-shooting hardware and software problems;
   technical training;
   firm-wide standard setting for the systems area; and
   performance evaluation of systems professionals.

   PTS: 1

2. Discuss the advantages and disadvantages of the second site backup options.

   ANS:
   Second site backups include mutual aid pacts, empty shell, recovery operations center, and internally provided backups.

   Mutual Aid Pacts

Advantages	Inexpensive
Disadvantages	May encounter reluctance to share facilities during an emergency

   Empty Shell

Advantages	Inexpensive
Disadvantages	Extended time lag between disaster and initial recovery
	May encounter competition among users for shell resources

   Recovery Operations Center

Advantages	Rapid initial recovery
Disadvantages	Expensive

   Internally Provided Backups

Advantages	Controlled by the firm
	Compatibility of hardware and software
	Rapid initial recovery
Disadvantages	Expense of maintaining excess capacity year round

   PTS: 1

3. Auditors examine the physical environment of the computer center as part of their audit. Many characteristics of computer centers are of interest to auditors. What are they? Discuss.

   ANS:
   The characteristics of computer centers that are of interest of auditors include: *physical location* because it affects the risk of disaster–it should be away from man-made and natural hazards; *construction* of the computer center should be sound; *access* to the computer center should be controlled; *air-conditioning* should be adequate given the heat generated by electronic equipment and the failure that can result from over-heating; *fire suppression* systems are critical; and adequate *power supply* is needed to ensure service.

   PTS: 1

4. Compare and contrast the following disaster recovery options: empty shell, recovery operations center, and internally provided backup. Rank them from most risky to least risky, as well as most costly to least costly.

   ANS:

   The 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 of 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.

   PTS: 1

5. What is a disaster recovery plan? What are the key features?

   ANS:

   A disaster recovery plan is a comprehensive statement of all actions to be taken before, during, and after a disaster, along with documented, tested procedures that will ensure the continuity of operations. The essential features are: providing second site backup, identifying critical applications, backup and off-site storage procedures, creating a disaster recovery team, and testing the disaster recovery plan.

   PTS: 1

6. Explain the outsourcing risk of failure to perform.

   ANS:

   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 Corp. (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.

   PTS: 1

7. Explain vendor exploitation.

ANS:
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.

PTS: 1

8. Explain why reduced security is an outsourcing risk.

ANS:
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.

PTS: 1

9. Explain how IT outsourcing can lead to loss of strategic advantage.

ANS:
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 to 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.

PTS: 1

10. Although IT governance is a broad area, only three of them are discussed in the chapter. Name them and explain why these topics were chosen.

    ANS:

    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:

    1) organizational structure of the IT function, 2) computer center operations, and
    3) disaster recovery planning.

    PTS: 1