2017 BEC Book Update

Page numbers refer to 2017 BEC textbook pages. When new/edited text is shown along with old text, the new/edited text is highlighted in gray, unless noted otherwise. For those who prefer to purchase a new textbook due to the significant amount of changes, please visit https://www.rogercpareview.com/cpa-courses/textbooks.

Information Technology

The CPA examiners have been shifting emphasis within the Information Technology (IT) topic from what computers do to how CPAs use computers. For the 2018 edition of our course, we re-organized the IT section accordingly.

In 2017, the examiners released a list of “new” vocabulary that may appear on upcoming Exams. Remember, questions will vary by CPA candidate; some candidates might not see any questions using these terms and others may see more than one. The “new” vocabulary terms include:

- Artificial intelligence and machine learning
- Automation
- Big data, data analytics, and data visualizations
- Blockchain and cryptocurrencies (e.g., bitcoin)
- Cloud operations and data storage
- Cybersecurity
- Digital business models

Each of these terms is discussed in this update as well as our 2018 course materials. Many candidates will find they already are familiar with the concepts behind these terms, if not the terms themselves.

Corporate Governance

Also in our 2018 course materials, we expanded our corporate governance coverage by incorporating a discussion of fraud risk management programs. This does not appear in the AICPA blueprint explicitly; however, it is well within the comprehensive task: Describe the corporate governance structure within an organization (tone at the top, policies, steering committees, oversight, ethics, etc.).

Note: Changes issued in September 2017, are not eligible to be tested until April 2018, not in the January-March 2018 window. Thus, the changes to the COSO Enterprise Risk Management framework will not be tested in Q1 of 2018.
10. What is strategic planning?
   a. It establishes the general direction of the organization.
   b. It establishes the resources that the plan will require.
   c. It establishes the budget for the organization.
   d. It consists of decisions to use parts of the organization's resources in specified ways.
10. (a) A strategic plan begins with the establishment of a mission statement, based on which an entity establishes objectives. Those objectives are then translated into goals, an action plan is developed to enable the achievement of the goals, and performance measures are developed to enable the entity to determine if progress is being made toward achieving them. Strategic planning is a process that an organization uses to identify its long-term goals and determines the best approach to achieve those goals. The strategic planning process is used to establish the general direction of the organization. Strategic planning does not determine the resources that the plan will require directly, but rather allocates existing resources to achieve the long-term goals. Budgeting is more detailed than strategic planning.
Lecture 2.04

FRAUD RISK MANAGEMENT PROGRAM

Overview

Fraud is any illegal act characterized by deceit, concealment or violation of trust. It is generally considered to be intentional, and deals with the integrity of the perpetrator, as opposed to errors, which are considered unintentional and deal with the competency of the perpetrator.

Typically, it can be divided into asset misappropriation (theft) or misstatement of financial statements. Members of upper management generally are more likely than non-management employees to misstate financial statements. Non-management employees generally are more likely than upper management to steal assets and then take steps to conceal the theft.

By its very nature, fraud involves some sort of deceit. An entity is vulnerable to severe long-term impact from fraud without active measures to deter, detect and minimize it. Basically, an ounce of fraud prevention is worth a pound of cure.

When an entity uncovers something that looks like fraud, it typically engages a certified fraud examiner (CFE) to investigate and assist in documenting it for prosecution and recovery, if any. Well-managed entities over a minimal size (often consulting with a CFE or CPA) develop a fraud risk management program (FRMP) long before a probable fraud event occurs.

Purpose Reasons for a fraud risk management program span the spectrum from legal duty to entity survival.

- A FRMP helps the board of directors satisfy
  - Duty of care to stakeholders.
  - Statutory/regulatory requirements (Sarbanes-Oxley, SEC, PCAOB standards, etc.)
- A FRMP helps support stakeholder confidence (impact of fraud on profitability and available funding). Shareholders are unwilling to invest to support a fraudster; they invest to receive financial returns.
- A FRMP helps entity survival
  - Greater profitability
  - Intact or enhanced image
  - Improved efficiency & increased ability to meet commitments and obtain financing
- A FRMP helps to prevent, detect, and deter fraud.
- A FRMP helps enhance employee morale (makes it easier to attract and retain well-qualified talent)
  - Reduced stress
  - Greater job satisfaction and security
- Most fraud is not found by external auditors
  - Internal measures often find fraud while it still is relatively small, increasing the likelihood of recovery or, at least, reducing the size of the loss.
  - Internal measures often are cheaper to implement than paying an external audit firm for essentially the same results.
- The Association of Certified Fraud Examiners (ACFE) report an annual audit and a code of conduct present in about 80 percent of fraud cases. Clearly, these are insufficient alone.

Small entities are particularly vulnerable to fraud, as they tend not to have anti-fraud controls.
Fraud Discovery According to the Association of Certified Fraud Examiners Report to the Nations on Occupational Fraud & Abuse (Using one's occupation for personal gain):

- Tips and whistle-blowers uncover about 40 percent of fraud. Management review and internal auditors each uncover about 15 percent of fraud. Accidents uncover over 5 percent of fraud. External auditors uncover less than 5 percent of fraud.
- Fraud losses are estimated at 5 percent of revenues.
- Typical losses are $140,000 per case and typical cases have an 18-month duration
  - Fraud has the highest impact on small entities.
  - The importance of the position of the perpetrator generally bears a direct relationship to the size of the loss.
- “Red flags” are present in over 80 percent of cases:
  - Living beyond means or personal financial difficulties
  - Unusually close relationships with vendors or customers
  - Excessive control issues

Occupational fraud is the use of one's occupation for personal gain through the deliberate misuse or misapplication of the organization's resources or assets. Types of Occupational Fraud and Abuse include misappropriations of assets, corruption and financial statement Fraud.

COSO outlines five steps in a Fraud Risk Management Program (FRMP).

1. Establish governance policies

2. Conduct a comprehensive risk assessment

3. Plan and execute preventive and detective control processes

4. Perform timely and confidential investigations

5. Monitor and assess the program (periodically, on an ongoing basis, or both periodically and on an ongoing basis) reporting the results and improving the processes

An effective FRMP will deter, but not eliminate, fraud. An effective FRMP:

- Initiates a visible and rigorous fraud governance process
- Promotes a transparent and sound anti-fraud culture
- Entails a thorough periodic fraud risk assessment
- Plans, executes, and maintains preventive and detective fraud control processes
- Responds quickly to fraud allegations, including loss recovery actions and proceedings against perpetrators

Five Fraud Risk Management Principles (CRIME) under COSO

- Control Environment: The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management (Tone at the Top) and their commitment to high integrity and ethical values regarding management fraud risk (CHOPPER).
- Risk Assessment: The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood an significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
- Control Activities: The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
• Information & Communication: The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

• Monitoring Activities: The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communications FRMP deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

Roles of Key Parties in Managing Fraud Risk (outlined by ACRE)

Those Charged with Governance (ideally, the audit committee)
• Consider the risk of management override of controls.
• Monitor fraud risks throughout the entity (using internal auditor or other personnel).
• Meet privately with appropriate individuals (e.g., internal auditor, external auditors).
• Consider reputation risk when reviewing work of management, internal auditors, and external auditors.
• Remain cognizant of the external auditor’s responsibilities pertaining to fraud.
• Seek counsel when responding to allegations of fraud.

Board of Directors (BOD)
• Understand fraud risks (both generally and those affecting the entity).
• Establish and communicate an appropriate level of risk tolerance for the entity.
• Maintain oversight of the fraud risk assessment.
• Monitor management’s reports on fraud risks, policies, and control activities.
• Ensure that management provides effective fraud risk management documentation to encourage ethical behavior.
• Retain outside experts as appropriate.
• Remain cognizant of the external auditor’s responsibilities pertaining to fraud.

Management (CEO, CFO, COO, etc.)
• Design, implement, maintain and document the fraud risk management program.
• Maintain documentation of antifraud controls.
• Evaluate design and operating effectiveness of antifraud controls.
• Report to the BOD on actions that have been taken to manage fraud risks and the effectiveness of the fraud risk management program.
• Educate the entity on areas of potential compliance violations.
• Enforce the entity’s Code of Ethics.

Internal Auditors
• Report to those Charged with Governance
• Provide assurance to the BOD and management regarding existing controls’ appropriateness given the risk tolerance established by the BOD.
• Evaluate the design and operation of antifraud controls for comprehensiveness and adequacy, especially regarding management override risks.
• Support the audit committee in performing detective activities around the risk of management override of controls
• Consider fraud risks when developing audit plans.
• Support management’s education of the entity regarding areas of potential fraud and compliance violations.
Employees (in all functions and at all levels)
- Have a basic awareness of fraud and “red flags.”
- Comprehend policies and procedures (e.g., fraud policy, code of conduct, whistleblower policy, internal controls specific to position, etc.).
- Contribute to a strong control environment.
- Report suspicions or incidences of fraud and corruption.
- Cooperate with audits and investigations.

Typical Shortcomings A fraud risk assessment (part of an entity's broader risk assessment process) considers the ways that fraud and misconduct can occur by and against the entity. The ACRE finds that fraud risk assessment failures typically are due to one or more of the following:
- Assessment consists of an identification of risk factors, but omits an identification of schemes and scenarios.
- Lack of follow up after identification of fraud risks and linkage to mitigating controls.
- Potential perpetrators are not identified (which can lead to insufficient consideration of management override).
- Inadequate consideration of collusive fraud and management override of controls.
- Lack of appropriate involvement in assessment by internal auditors and other appropriate personnel.
- Lack of appropriate monitoring by the audit committee.

While a FRMP cannot guarantee the absence of fraud, it can deter fraud and minimize fraud loss much less expensively than other measures. Entities cannot rely complacently on an annual audit and a code of ethics to prevent fraud.
A company, for instance, may determine that there is a 25% probability that a machine's engine will fail, requiring an overhaul that is expected to cost $10,000. The expected cost of this risk event would be $10,000 x 25%, or $2,500.

**INVESTMENT LIFE CYCLE**

When evaluating an investment's rate of return, all phases of the investment life cycle will be considered as will such factors as acquisition cost, the cost of managing the investment, cash flows, appreciation, depreciation, and costs of disposal.

When an entity makes an investment, the actions it takes over the period during which it is involved with the investment is considered the **investment life cycle**.

**Pre-commitment Evaluation:** An entity plans for the acquisition of an investment, including the evaluation as to whether or not the investment is likely to meet the entity's investing criteria. This includes the investment's cost, volatility, expected return, and whatever other factors the entity considers when comparing investments.

**Acquisition of investment**

**Management:** Manage the investment with an emphasis on growth, earnings, tax benefits, cash flows, or some other factor relevant to the entity. Some investments (such as ownership of a business, product line, or division) require ongoing decisions; others (such as a U.S. Treasury bond) are more passive.

**Monitoring:** Re-evaluate the investment to determine if there are diminishing returns, suggesting the investment either no longer meets the criteria or may no longer be the best alternative.

**Disposal of investment**

**PRODUCT LIFE CYCLE**

A product's life cycle is from the time it is introduced to the time when it is withdrawn. Not all products make it to all phases. For instance, some go from introduction to decline.

**Introduction**

Few and intermittent sales,

- Limited production capacity
- Lack of appropriate retail outlets
- Consumer resistance to change to the established consumption patterns

Highest proportional promotional expenses: Small volume of sales to offset high promotion efforts to create demand,

- Informing potential and present consumers of the new and unknown product
- Inducing a trial of the product
- Screening distribution net-work
Highest product prices possible:
- Low volume to absorb fixed costs
- Technological problems not fully resolved
- Few or no competitors
- Sales to higher income groups/first adopters

**Growth**
Sales rise as consumers accept the product. The prices may remain high to recover some of the development costs. High profits encourage competitors to enter the market.

Sales accelerate.
- Consumer resistance fades
- Distribution network solidifies
- Production is optimized

High promotional expenses.
- Shift from informing consumer to brand identification
- Special offers to consumers or allowances to dealers

Product improvements.
- Competitors do not incur the same extent of research and development or promotional costs as the originator.
- Competitors or originator gain advantage by modifying products.
- Competitors or originator gain advantage by reducing prices.

**Maturity**
Sales accelerate at a declining rate.
- Market reaches saturation.
- Prices soften and become more uniform.
- Competition intensifies as each manufacturer tries to maintain production at a viable level.
  - The more capital-intensive the product is to produce, the more important it is to maintain high output to cover fixed costs at lower prices.
  - The Internet has lengthened the life cycle for many products.

Normal promotional expenses as competition squeezes margins. Manufacturers try to “milk the cash cow” for all it is worth.

Extension strategies: Substantial product modification can have the revised product re-enter the introduction phase to re-start the cycle.
- Development of new markets for existing product
- Development of new uses for existing product
- Development of more frequent use for existing product
- Development of wider range of products (more flavors, colors, etc.)
- Development of style change (slightly different product)

**Decline**
Sales decline rapidly.
- Prices fall
• Over capacity pushes manufacturers to cease production
• Conceivably, this could be a very profitable period for a producer with low fixed costs.

Little or no promotional expenses.
Page 3-27: Lectures 6.06 through 6.08 starting on Page 6-8 are now Lectures 3.21 through 3.24.

**Lecture 3.21**

**RISK MANAGEMENT**

**Expected Returns**

The total return of an investment includes cash distributions (interest, dividends, rents) and the change (growth) in the value of the asset (Total Return = Distribution Rate + Growth Rate). This model, known as the **Gordon Growth Model**, assumes that the reinvested assets will increase distributions by the amount of reinvestment, so that the growth in the assets will be the growth rate of future dividends. Eventually, all earnings are going to be distributed over the life of the company.

***
Page 3-33: The following questions have been moved from Section 6 (#8-14 starting on Page 6-25).

**Lecture 3.22**

26. A company is considering acquiring a derivative to hedge a risk associated with an investment it is currently holding. Which of the following coefficients of variation would indicate that the hedge will be effective?
   a. +0.91
   b. +0.19
   c. -0.19
   d. -0.91

27. Which of the following is a measure of the volatility of an investment?
   a. Expected return.
   b. Standard deviation.
   c. Graphical Evaluation and Review Technique (GERT).
   d. Coefficient of variation.

28. Which of the following is a risk taken by a lender that the value of the loan will decline as a result of a general economic decline?
   a. Market risk.
   b. Credit risk.
   c. Concentration of credit risk.
   d. Economy risk.

29. Which of the following is not a theory that describes the reasons for differences in the yields associated with interest rates?
   a. Expectations.
   b. Market segmentation.
   c. Behavioral finance theory.
   d. Liquidity preference.

**Lecture 3.24**

30. Which of the following is not a characteristic of a derivative?
   a. It can be settled in its net amount for cash or other liquid assets.
   b. It has an original maturity of three months or less.
   c. There is an underlying and a notional amount.
   d. There is either no initial payment or the initial payment is disproportionately lower than the cost of an investment that would react to the market similarly.
31. Rishard Corporation has a cash flow hedge that has increased in value by $60,000 during the year. The hedge is highly effective, and 95% of the change is expected to offset changes in future cash flows on the hedged transaction. How will Rishard report the $60,000 increase?

   a. $57,000 of the gain will be reported in other comprehensive income and the remainder will be disclosed in the footnotes.
   b. The entire amount will be reported in other comprehensive income.
   c. $57,000 of the gain will be reported in other comprehensive income and the remainder will be reported in income.
   d. $57,000 of the gain will be reported in income and the remainder will be reported in other comprehensive income.

32. A company is considering entering into an interest rate swap but is concerned that the counterparty may not perform. This is a description of:

   a. Performance risk.
   b. Legal risk.
   c. Market risk.
   d. Credit risk.
26. (d) In order for a hedge to be effective in offsetting a risk associated with an investment, it should respond to market conditions in the opposite way that the hedged investment acts. The closer a coefficient of variation is to 0, the less of a relationship there is between the two items. A coefficient of +1 indicates the two act in pretty much precisely the same manner and a coefficient of -1 indicates that they act in an opposite manner. A coefficient of -0.91 would indicate a strong inverse relationship and a potentially effective hedge.

27. (b) The standard deviation is a measure of the volatility of an investment and is the most common measure of investment risk. Answer (a) is incorrect because the expected return is the estimate of the return the company will receive, taking into account the probabilities of various possible outcomes occurring, each of which may provide a different return. It does not measure volatility. Answer (c) is incorrect because graphical evaluation and review technique (GERT) is a project management approach, not an investment measurement. Answer (d) is incorrect because the coefficient of variation measures the similarity in the way different investments will react to changes in market conditions. It does not measure volatility.

28. (a) Market risk is the risk that the value of a bond or loan will decline due to a decline in the aggregate value of all the assets in the economy. Answer (b) is incorrect because credit risk is the risk that the borrower will default on interest or principal payments. Answer (c) is incorrect because a concentration of credit risk is the risk associated with lending to a relatively small number of borrowers or borrowers with common characteristics. Answer (d) is incorrect because there is no risk assumed by lenders that is referred to as an economy risk.

29. (c) Liquidity preference, market segmentation, and expectations are three theories on the reason for differences in yields. Behavioral finance theory relates to the behavior of stocks, not interest rates.

30. (b) A financial instrument is a derivative if it will be settled in cash or liquid assets for its net amount, there is at least one underlying and notional amount, and there is either no initial cost or the initial cost is disproportionately low compared to other investments that would provide similar reactions to the market. There is no requirement that it have a maturity of 3 months or less.

31. (c) When a derivative is accounted for as a cash flow hedge, any gain or loss due to a change in the value of the hedge will be reported in other comprehensive income to the extent that the hedge is effective. With 95% effectiveness, $57,000 will be reported in OCI. The ineffective portion is recognized in income.

32. (d) Credit risk is the risk that the counterparty to a contract will fail to honor its obligations. Answer (a) is incorrect because there is no risk called performance risk associated with derivatives. Answer (b) is incorrect because legal risk is the risk that legal or regulatory action will invalidate the derivative. Answer (c) is incorrect because market risk, applicable to derivatives acquired for speculation purposes, is the risk that adverse changes will affect the fair value of the derivative.
Written Communication 2

Required:
Grace Fulbright, a research analyst at Dragon Hedge Fund, is concerned that expected changes in interest rates may affect the performance of a portfolio that she is tracking. She has requested that you draft a memorandum explaining the yield curve, the theories that explain its shape, and how its shape may contain relevant information about the future.

REMINDER: Your response will be graded for both technical content and writing skills. Technical content will be evaluated for information that is helpful to the intended reader and clearly relevant to the issue. Writing skills will be evaluated for development, organization, and the appropriate expression of ideas in professional correspondence. Use a standard business memo or letter format with a clear beginning, middle, and end. Do not convey information in the form of a table, bullet point list, or other abbreviated presentation.

To: Miss Grace Fulbright, Research Analyst  
   Dragon Hedge Fund  
From: CPA Candidate
Written Communication Solution 2

To: Grace Fulbright, Research Analyst  
   Dragon Hedge Fund  
From: CPA Candidate

In our earlier conversation, you asked that I explain the yield curve, the theories that explain its shape, and how it may contain relevant information about the future.

The yield curve presents U.S. Treasury interest rates across various maturities. According to the liquidity preference theory, the yield curve should normally be upward sloping (longer-term interest rates being higher than shorter-term interest rates) since investors demand more compensation for long-term investments. According to the expectations theory, long-term interest rates reflect future expected short-term interest rates. According to the market segmentation theory, various participants in bond markets may focus on lending at different terms. Considering all theories jointly, an inverted yield curve (longer-term interest rates being lower than shorter-term interest rates) usually reflects investors’ expectations of upcoming declines in economy-wide interest rates, usually because investors expect falling inflation rates or a recession.

The yield curve provides valuable information both about current interest rates and about investors’ expectations of future economic conditions. If you have any further questions, please feel free to contact me.

Sincerely,

CPA Candidate
### Inventoriable Costs

<table>
<thead>
<tr>
<th></th>
<th>Absorption Costing</th>
<th>Variable Costing</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>DL</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>V O/h</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>F O/h</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>V SGA</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>F SGA</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

Under direct (Variable) costing, whether a cost is included in inventory has nothing to do with whether it is expensed as a variable or fixed cost. Variable selling expenses are not included in inventory, but are included in the computation of contribution margin. Variable manufacturing costs are included in inventory and are included in the computation of contribution margin. Neither fixed manufacturing costs nor fixed selling expenses are included in inventory nor in the computation of contribution margin.
Benchmarking

Benchmarking involves evaluating performance (producing products, delivering services, etc.) on an ongoing basis across subdivisions within an organization and relative to historical and current performance within and outside the organization. Organizations engage in benchmarking in part to identify “best practices” that may then be adopted more widely across the subdivisions of the organization. Common types of benchmarking include:

- **Internal benchmarking**: To track, for instance, how well various subdivisions within one firm carry out one task. Generally, the information is relatively easy to obtain. The disadvantage is that improvement may be limited to the best that one subdivision is doing; external benchmarking may result in more dramatic improvements. For instance, reducing the employee time to process a vendor invoice and issue a check from 29 minutes to 14 minutes is impressive, until compared with 2 minutes to process an electronic funds transfer (EFT).

- **Competitive benchmarking**: To track how well one firm performs relative to its most direct competitors. This may yield dramatic improvements, but the information often is difficult to obtain; while some of this information is directly observable by the public, obtaining this information typically is very difficult as competitors have little incentive to assist and many incentives to protect their competitive advantages.
  - Cross-sectional analysis: exploring data for one time period for multiple firms (i.e., including one’s firm and other firms) in the same industry.
  - Time-series analysis: exploring data for one firm over time.
  - Panel data analysis: exploring data for multiple firms over time (i.e., panel data analysis uses both multiple firms and multiple time periods).

- **Industry benchmarking**: To track one firm against its industry as a whole, instead of against only its direct competitors.

- **Generic benchmarking**: To track one firm against all firms, even if outside its industry. Benchmarking is likely to be more relevant the more alike the firms are that one compares against. Of course, obtaining data is usually easier the broader the category of firms one uses.
QUALITY CONTROL

The International Organization of Standards (ISO) has developed a series of ISO Quality Standards.

- ISO 9000 Series – including five parts (9000 to 9004) focusing on the quality of products and services provided by firms.
- ISO 14000 Series – focusing on environmental goals.

According to the Pareto Principle, 80% of quality problems result from only 20% of the possible causes. Thus, firms should first focus on the most important causes of problems, and only later address less important cases.

**Six-Sigma Quality** is a statistical measure of the percentage of products that are in acceptable form (i.e., achieve the firm’s quality goals), based on standard deviation measures (hence the name sigma). To achieve one sigma, 68% of products must be acceptable. To achieve six sigmas, 99.999997% of products must be acceptable. Six-sigma constitutes the practical hypothetical goal of perfection in manufacturing, with only 3.4 defects per million units.

Total quality management (TQM) is an entity-wide effort to continuously improve the ability to deliver high quality products and services by attending to systematic analysis; thus, it includes insights from suppliers as well as employees. It now is largely supplanted by six sigma and ISO programs; however, concepts from TQM often appear (in more evolved and formal versions) in implementation of these later perspectives.

Businesses may apply the theory of constraints (TOC) to maximize their operating income and overcome bottlenecks in their operations. Under TOC, if demand exceeds capacity for a resource, the resource is defined as a bottleneck resource. If capacity exceeds demand, the resource is defined as a non-bottleneck resource. TOC seeks to simultaneously maximize throughput contribution and minimize investment and operating costs.

- **Throughput contribution** equals revenues minus the direct materials cost of goods sold (COGS).
- **Investment** equals the cost of materials, work in process, inventories; research and development expenses; and (upfront) expenses on equipment and buildings.
- **Operating costs** equals employee compensation, rents paid, utilities (electricity, garbage collection, etc.), and depreciation (e.g., of equipment and buildings).
8. A company has an online order processing system. The company is in the process of determining the dollar amount of loss from user error. The company estimates the probability of occurrence of user error to be 90%, with evenly distributed losses ranging from $1,000 to $30,000. What is the expected annual loss from user error?

   a. $13,050  
   b. $13,500  
   c. $13,950  
   d. $14,400

9. Macaw College allocates support department costs to its individual colleges using the step method. Information for July is as follows:

<table>
<thead>
<tr>
<th></th>
<th>Maintenance</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs incurred</td>
<td>$79,200</td>
<td>$43,200</td>
</tr>
</tbody>
</table>

   Services percentages provided to:
   - Maintenance: -- 10
   - Power: 20 --
   - School of Business: 30 20
   - School of Humanities: 50 70
   - Total: 100 100

   What is the amount of July support department costs allocated to the College of Business?

   a. $32,400  
   b. $36,880  
   c. $38,340  
   d. $39,300

10. Which of the following forecasting methods relies mostly on judgment?

   a. Time series models  
   b. Econometric models  
   c. Delphi  
   d. Regression analysis

11. On a balanced scorecard, which of the following is considered an internal business process perspective?

   a. Number of defects in product that customers report  
   b. Number of hours of employee training  
   c. Percentage of employee advancement  
   d. Percentage of employee retention
12. Apex Athletics, LLC, is manufacturer of premium athletic equipment and apparel. Apex is starting a value based management process. What is an activity for which it most likely will be difficult to trace to the economic value added to Apex?
   a. Cycle time reduction in manufacturing processes
   b. Design of products to reduce packaging and shipping costs
   c. Lead generation
   d. Sponsorship of after-school and summer youth programs in low-income neighborhoods.

13. At 20% of industry sales, Party Hearty, Inc., is one of the top three chains of party stores. These three chains cumulatively have 73% of industry sales. Party Hearty would like to perform benchmarking to determine the best practices for its processes, but is having difficulty obtaining data for benchmarking. For which form of benchmarking will Party Hearty find it easiest to obtain data?
   a. Competitive benchmarking
   b. Generic benchmarking
   c. Industry benchmarking
   d. Internal benchmarking

14. Which of the following quality costs generally are most difficult to quantify?
   a. Detection costs
   b. External failure costs
   c. Internal failure costs
   d. Prevention costs

***

Lecture 6.10

17. General Looms hires a consultant to implement business process management. What best describes the consultant’s goals?
   a. Identify General Looms’ long-term goals and determine how best to reach them.
   b. Ensure that General Looms’ objectives are met while the legitimate needs and concerns of all stakeholders are being addressed.
   c. Establish a code of conduct and encourage appropriate behavior by example.
   d. Align all aspects of General Looms with the wants and needs of its customers.

18. A consultant proposed that Trendy Gizmos, a U.S. manufacturer, have its electronic devices assembled in a factory in India. One member of the team considering the proposal is concerned about the potential loss of control over information about the company’s products and processes. What best describes the team member’s concerns?
   a. Social responsibility risk.
   b. Quality risk.
   c. Intellectual property risk.
   d. Information security risk.
8. (c) Expected value is the sum of possible outcomes multiplied by the probability of occurrence. A 90% likelihood of loss means a 10% likelihood of no loss; the 10% likelihood of zero loss is multiplied by $0. To calculate expected annual loss from user error, find the midpoint of the evenly distributed losses and multiply by the likelihood of losses. The midpoint of 1,000 and 30,000 is 15,500, calculated as (1,000 + 30,000)/2. Multiplying 15,500 by the 90% likelihood equals an expected annual loss from user error of $13,950.

9. (b) Under the step method, costs are allocated from one service department to operating departments and other service departments. Costs are not allocated to a department once costs are allocated from that service department. A percentage of use by a service department with costs already allocated is ignored; new ratios are derived using the relationships between the departments still accepting costs. This scenario (modeled after one from the AICPA) does not establish clearly which service department’s costs are allocated first. The maintenance department (M) costs must be allocated first because if one assumes the power department (P) costs are allocated first, the answer ($39,960) does not appear as one of the options. In the table below, B and H represent the Schools of Business and Humanities, respectively.

<table>
<thead>
<tr>
<th>Allocating P costs first</th>
<th>P $</th>
<th>M ratio</th>
<th>M $</th>
<th>B ratio</th>
<th>B $</th>
<th>H ratio</th>
<th>H $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs (in 1,000s)</td>
<td>$43.2</td>
<td>1/10</td>
<td>$79.20</td>
<td>2/10</td>
<td>8.64</td>
<td>7/10</td>
<td>30.24</td>
</tr>
<tr>
<td>P ratio/allocation [1+2+7=10]</td>
<td>(43.2)</td>
<td>1/10</td>
<td>4.32</td>
<td>2/10</td>
<td>8.64</td>
<td>7/10</td>
<td>30.24</td>
</tr>
<tr>
<td>Subtotal</td>
<td>--0--</td>
<td>83.52</td>
<td>$8.64</td>
<td>$31.32</td>
<td>5/8</td>
<td>52.20</td>
<td></td>
</tr>
<tr>
<td>M ratio/allocation [3+5=8]</td>
<td>(83.52)</td>
<td>3/8</td>
<td>31.32</td>
<td>5/8</td>
<td>52.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals (not an answer option)</td>
<td>--0--</td>
<td>$83.52</td>
<td>$8.64</td>
<td>$39.96</td>
<td>$82.44</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allocating M costs first</th>
<th>M $</th>
<th>P ratio</th>
<th>P $</th>
<th>B ratio</th>
<th>B $</th>
<th>H ratio</th>
<th>H $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs (in 1,000s)</td>
<td>$79.2</td>
<td>2/10</td>
<td>$43.20</td>
<td>3/10</td>
<td>23.76</td>
<td>5/10</td>
<td>39.60</td>
</tr>
<tr>
<td>M ratio/allocation [2+3+5=10]</td>
<td>(79.2)</td>
<td>2/10</td>
<td>15.84</td>
<td>3/10</td>
<td>23.76</td>
<td>5/10</td>
<td>39.60</td>
</tr>
<tr>
<td>Subtotal</td>
<td>--0--</td>
<td>$59.04</td>
<td>$23.76</td>
<td>$45.92</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P ratio/allocation [2+7=9]</td>
<td>(59.04)</td>
<td>2/9</td>
<td>13.12</td>
<td>7/9</td>
<td>45.92</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>--0--</td>
<td>--0--</td>
<td>$36.88</td>
<td>$85.52</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The step method allocates all the first service department costs to production departments and all remaining service departments before allocating the second service department costs.

10. (c) Delphi is a structured forecasting method based on the collective judgement of a group of experts. Each expert’s judgment is involved; the forecasts will become more refined after each round—during which experts can revise their previous answers. It is used in novel situations where more objective approaches are unavailable. Answer (a): Time series models objectively analyze a sequence of previously observed data to predict future values, requiring relatively little reliance on judgment. Answer (b): Econometric models are statistical models applying economic theories. Some judgment is involved when selecting theories to apply, but the application of the theories is objective. Answer (d): Forecasting based on regression analysis predicts the dependent variable (y) based on the observed behavior of an independent variable (x). As long as the independent variable and other factors are determined, no subjective judgment is involved.

11. (a) The internal business perspective includes measuring the cost, time, and quality of producing and delivering a product or service. One example of this is the number of defects.
Answers (b), (c), and (d): Employee advancement, training, and retention are considered part of the learning and growth perspective.

12. (d) As a manufacturer of “premium” athletic equipment and apparel, Apex is unlikely to generate much future (and even less immediate) business among those participating in the low-income neighborhood programs; however, the social responsibility demonstrated by Apex’s sponsorship of these programs may resonate with affluent consumers of its products. The extent to which sales are a result of consumers’ appreciation of Apex social responsibility as opposed to those that would have occurred without such sponsorship is difficult to determine. Answer (a): Shorter cycle times equate to less time that inventory is held, reducing the holding costs (such as, property taxes and financing). Answers (b) and (c): Greater revenue, lower costs, and shorter cycles generally are easy to equate to economic value added.

13. (d) Internal benchmarking involves comparing various subdivisions within one company; presumably, the head office merely could instruct each subdivision to collect and report any required information that it does not already receive. Answer (a): Competitive benchmarking involves comparing processes with direct competitors. Competitors are unlikely to assist. Answer (b): Generic benchmarking involves comparing processes at all types of companies; at a minimum, this would involve researching sources of such information. Answer (c): Industry benchmarking involves comparing processes at all companies in the industry; at a minimum, this would involve researching sources of such information.

14. (b) External failure costs include such costs as the loss of reputation, product liability costs, and marketing to maintain or improve the company image. While estimated future sales form an input to determine the loss of reputation costs, it is itself an estimate. These costs are difficult to quantify. Answer (a): Detection costs include inspection costs and customer survey costs. These costs tend to be easy to separate from other costs and objectively calculated, making them relatively easy to quantify. Answer (c): Internal failure costs include the costs of wasted materials, reworking units to correct defects and re-inspecting and retesting after rework. These costs tend to be easy to separate from other costs and objectively calculated, making them relatively easy to quantify. Answer (d): Prevention costs include using materials of known quality, designing production processes to promote quality, monitoring production processes, and employee training. Compared to external failure costs—such as product liability and loss of reputation, prevention costs tend to be calculated objectively; this makes them relatively easy to quantify.

***

17. (d) Business process management involves the alignment of all aspects of a business with the wants and needs of its customers. Answer (a): Strategic planning is the identification of long-term goals and determination of how best to reach them. Answer (b): Corporate governance involves ensuring that an entity’s objectives are met while the legitimate needs and concerns of all stakeholders are being addressed. Answer (c): Implementing internal control involves management establishing a code of conduct and encouraging appropriate behavior by example.

18. (c) Intellectual property risk is the risk that an entity could lose control of information about the entity’s products and processes. Copyright and patent regulation and enforcement is not uniform internationally. Answer (a): Social responsibility risk concerns the ethics of business partners or working practices at the foreign site. Answer (b): Quality risk is due to less control over quality. Answer (d): Information security risk is the risk that an entity could lose control over confidential customer and entity information.
Written Communications 3

Required:

MTDV, Inc. operates retail outlets across many cities, has detailed historical sales data for each individual outlet, and could obtain demographic data about each of the cities where it operates. The company is considering opening a new outlet in a region where it does not have any outlets at this point.

Teresa Highlander, the Chief Executive Officer of the company has asked you to write a memo outlining how they could estimate the sales they could expect in that new outlet, and some of the issues involved in such a calculation.

REMININDER: Your response will be graded for both technical content and writing skills. Technical content will be evaluated for information that is helpful to the intended reader and clearly relevant to the issue. Writing skills will be evaluated for development, organization, and the appropriate expression of ideas in professional correspondence. Use a standard business memo or letter format with a clear beginning, middle, and end. Do not convey information in the form of a table, bullet point list, or other abbreviated presentation.

To: Ms. Teresa Highlander
MTDV Inc.
From: CPA Candidate
Page 6-43: The following solution has been moved from Section 3 (WC 2) on Page 3-56).

Written Communication Solution 3

To: Ms. Teresa Highlander
    MTDV Inc.
From: CPA Candidate

Thank you for your question regarding how to forecast estimates of the new outlet you are considering opening. To estimate sales in an outlet in a new city, MTDV could use forecasting techniques. The reliability of these estimates will be greater the more that the region where the new outlet will be located is similar to the regions where MTDV already operates.

Forecasting techniques first assess the past relationships across variables, e.g., sales at individual outlets and demographic characteristics where the outlets are. Forecasting techniques next use those relationships to make projections. The techniques might take into account, for instance, that the new outlet is located in a city that is fairly small or with income levels that are slightly above average. Sales estimates will be more reliable if the city is similar to other cities where MTDV already operates, e.g., similar size, same proportion of young, vs. elderly residents, etc. Sales estimates will be least reliable if the city differs greatly.

MTDV could use forecasting techniques to project likely sales for its outlet in a new city. Forecasts for new outlets in regions where MTDV has not operated before will be less reliable. Please feel free to contact me if you have any additional questions or concerns.

Sincerely,

CPA Candidate
Starting on Page 7-1, the following replaces all of the text and multiple-choice questions in Section 7.

Lecture 7.01

INFORMATION TECHNOLOGY ROLE IN BUSINESS

The use of computers first focused on relieving humans of the tedious work involved in general recordkeeping and reporting. Now, regulatory requirements include electronic reporting. For instance, the IRS requires electronic submission of many business tax returns.

Transaction processing systems focus on relieving humans of the tedious work involved in general recordkeeping and reporting. Management reporting systems assist in the decision-making process within the organization. The most common business systems include:

- **Management information system** – (MIS) An organized assembly of resources and procedures required to collect, process, and distribute data for use in decision making.
- **Decision support system** – (DSS) An interactive system that provides the user with easy access to decision models and data, to support semi-structured decision-making tasks.
- Enterprise Resource Planning (ERP) is a packaged business software system that allows an organization to automate and integrate the majority of its business processes (sales, inventory management, planning and forecasting), share common data and practices across the entire organization, and produce and access information in a real-time environment. These systems span both transaction processing systems and management reporting systems. Examples of ERP include SAP, Oracle Financials, and J.D. Edwards.
- **Executive support information system** – Systems designed specifically to support executive work (nonroutine decision, helps answer questions regarding competitors and identify new acquisitions).
- **Analytical processing system** – software technology that enables the user to query (ask) the system, retrieve data and conduct analysis.
- **Expert system** – The most prevalent type of computer system that arises from the research of artificial intelligence. An expert system has a built-in hierarchy of rules, which are acquired from human experts in the appropriate field. Once input is provided, the system should be able to define the nature of the problem and provide recommendations to solve the problem.

Connectivity

The Internet and related Web technologies ushered in a paradigm shift from the computer as a number-crunching device to a communication tool. This paradigm shift was aided by significant declines in computing costs coupled with dramatic increases in computing power in the last several decades.

Since the introduction of smart phones in 2007, the Internet has driven another shift—from desktop devices to mobile devices and tablets. Thus, computing is being even more fully integrated into daily life.

For example, in the number-crunching phase, businesses started using computers to record the sales made each day at a store and then made by each cashier, then a
A computer at the store recorded each sale and concurrently updated the inventory files. In the communicating phase, the cashier’s computer automatically contacts the credit card company to confirm that the customer’s available credit limit is sufficient for the purchase. Businesses websites started with contact information and driving directions and evolved to online retail sites.

Obviously, businesses still are using the number-crunching aspect of computers. Indeed, automation of many tasks once performed by humans is ubiquitous. The communications aspect’s applicability to accounting might be less obvious.

For example, decades ago, employees submitted physical copies of receipts and a printed expense report to the accounting department. An A/P clerk reviewed the report, coded expenses by category, confirmed expenses meet per diem and other limits, and requested supervisor approval. After the report was approved, the A/P clerk submitted a paper payment voucher. A check was issued for the employee to take to his or her bank and deposit.

Now, employees use smartphones to take a picture of any paper receipts. They might use the smartphone linked to a credit card to pay for expenses. Employees submit electronic copies of receipts to a website that “reads” the receipts, suggests likely categories, confirms that expenses meet per diem and other limits, and requests supervisor approval. After the report is approved, an A/P clerk reviews the categories (lodging, airfare, local transportation, meals, etc.) to ensure they are correct and submits an electronic payment voucher. An electronic payment is issued to the employee’s bank account.

While these computers are keeping records, they also are communicating with each other: the employee’s smartphone with the credit card company servers, the employee’s tablet that gets an e-mail with a receipt from the taxi driver’s smartphone, the employee’s tablet and smartphone with the server hosting the expense website, the expense website server with the supervisor’s laptop and the employer’s servers, and the A/P clerk’s desktop with the bank’s servers.

A distributor’s computer likewise can communicate with manufacturers’ and retailers’ computers, ordering and shipping product without each shipment being initiated directly by a human.

The ubiquitous nature of computers make it important that their systems are operating as designed.

**Control Objectives for Information and related Technology (COBIT)**

ISACA (formerly Information Systems Audit and Control Association) has developed a framework, referred to as Control Objectives for Information and related Technology (COBIT), for the governance and management of enterprise IT (Information Technology). In 2012, ISACA issued COBIT 5, the most recent iteration of the framework. The COBIT framework is business oriented in that it provides a systemic way of integrating IT with business strategy and business risk.
COBIT 5 helps enterprises of all sizes:
- Maintain high-quality information to support business decisions
- Achieve strategic goals and realize business benefits through the effective and innovative use of IT
- Achieve operational excellence through reliable, efficient application of technology
- Maintain IT related risk at an acceptable level
- Optimize the cost of IT services and technology
- Support compliance with relevant laws, regulations, contractual agreements and policies

COBIT 5 is based on 5 core principles around which an effective governance and management framework can be established, the goal of which is to maximize the benefit provided to stakeholders by their investment in information and technology.

The 5 core principles relate to:
- Meeting stakeholder needs
- End-to-end application
- Development of a single integrated framework
- Enabling a holistic approach
- Separating governance from management

Meeting Stakeholder Needs

The objective of an entity is to bring value to stakeholders, which may be in the form of financial return, as in the case of a “for profit” entity, or public service, as in the case of a not-for-profit entity. Regardless of how stakeholders define value, stakeholder needs are met through balancing the realization of benefits while optimizing risk and resource use. ISACA suggests the use of a “goal cascade” to customize COBIT 5 to create stakeholder value.

The goal cascade consists of 4 steps:
1. Factors influencing stakeholder needs are identified.
2. Stakeholder needs are translated into generic goals of the entity. COBIT 5 suggests 17 generic entity goals that fall into 4 categories. The list is comprehensive, although not intended to be all inclusive:
   - Financial
   - Customer
   - Internal
   - Learning and growth
3. IT-related goals are derived from the generic entity goals. COBIT 5 also suggests 17 IT goals that fall into the same 4 categories.
4. IT-related goals are next translated into what COBIT 5 refers to as enabler goals. Enablers are the processes, structures, and information that enable the entity to achieve its goals.

Financial goals include:
- Value of business investments
- Competitive products and services
- Safeguarding of assets
- Compliance
- Transparency

**Customer** goals include:

- Culture of customer service
- Service continuity and availability
- Ability to respond to change
- Strategic planning based on information model
- Optimization of costs of delivering products or services

**Internal** goals include:

- Optimizing functionality of business functions
- Optimizing process costs
- Management of change
- Productivity
- Compliance with policies

**Learning and growth** goals include:

- Capable, motivated personnel
- Culture of innovation

### End-to-End Application

There are 2 respects in which COBIT 5 addresses the management and governance of IT applying an end-to-end approach to the enterprise.

- The system of governance for IT should “seamlessly” integrate into the system of governance for the enterprise as a whole.
- Systems for the governance and management of IT should apply to all components of the entity in which information is processed, both internally and externally.

### Application of a Single Integrated Framework

COBIT 5 is considered a single integrated framework because it incorporates or aligns with other relevant standards and frameworks, allowing COBIT 5 to be applied to the enterprise as a whole.

### Enabling a Holistic Approach

COBIT 5 describes 7 categories of enablers and indicates that each enabler requires inputs from, and delivers outputs to, other enablers that are necessary for the enablers to be fully effective. The categories are:

- Principles, policies, and frameworks, which apply to all other enablers
- Processes
- Organizational structure
- Culture, ethics, and behavior
- Information, which is also a resource
- Services, infrastructure, and applications, which are also resources
- People, skills, and competencies, which are also resources
Separating Governance from Management

COBIT 5 distinguishes between governance and management.

- Governance determines enterprise objectives, taking into account stakeholder needs, and sets direction for the entity.
- Management oversees the entity’s activities toward achieving enterprise objectives in alignment with governance’s direction.
- Ensures that stakeholders’ needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.
- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

IT Environment

The IT environment is largely dependent on the size of the company and the number of employees and type of computers involved. Historically, a few large computers were operated exclusively by IT personnel. With personal computers, tablets, and phones networked together, it now is not unusual for each employee in a company to use a computer on a daily basis.

- Large companies will have a separate IT department.
- Others will have many IT functions outsourced or partially outsourced and partially performed by end users.
- One characteristic of an IT environment is a reduction in the segregation of duties.

An IT department will normally include systems development and maintenance, operations, and other technical services.

Systems Development and Maintenance

Systems development and maintenance might include the following:

- A systems analyst designs the information system using systems flowcharts and other tools and prepares specifications for applications programmers, as well as acting as an intermediary between the users and programmers. Flowcharts are graphical representations of sequences of activities and decisions, and are useful for both documenting systems and procedures and for isolating control weaknesses.
- An application programmer writes, tests, and debugs programs that will be used in the system. The programmer also develops instructions for operators to follow when running the programs.
- A database administrator is an individual or department responsible for the security and information classification of the shared data stored on a database system. This responsibility includes the design, definition and maintenance of the database.

Note: The systems development life cycle (SDLC) consists of the phases deployed in the development or acquisition of a new software system. SDLC is an approach used to plan, design, develop, test, and implement an application system or a major modification to an application system. Typical phases of the SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation, and post-implementation review.
Operations in an IT Function
Operations might include data control, computer operations, and librarians.

- A **data control clerk** schedules jobs for the computer and manages the distribution of reports and other output. Data control clerks may be involved in coding activities, calculating and checking batch totals, and related clerical tasks.
- The data control department is responsible for collecting data for input into a computer's batch processing operations as well as the dissemination of the finished reports.
- Data entry includes keyboard entry, scanning, and voice recognition. When transactions are entered (batch data entry), they are just stacks of source documents to the keyboard operator. Deciphering poor handwriting from a source document is a judgment call that is often error prone. In online data operations, in which the operator takes information in person or by phone, there is interaction and involvement with the transaction and less chance for error.
- A **computer operator** is a person who operates a computer in a datacenter and performs such activities as commanding the operating system, mounting disks and tapes, and placing paper in the printer. Operators may also write the job control language (JCL), which schedules the daily work for the computer.
- **Librarians** are the individuals responsible for the safeguarding and maintenance of all program and data files.

Other Technical Services
Other technical services might include telecommunications, systems programming or technical support, and security administration.

- **Telecommunications** is responsible for maintaining and enhancing computer networks and network connections.
- A **systems programmer** or technical support is responsible for updating and maintaining the operating systems.
- **Security administration** is responsible for security of the system including control of access and maintenance of user passwords.

Lecture 7.02
SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)
A traditional SDLC approach is made up of a number of distinct phases, each with a defined set of activities and outcomes. Designing and implementing a new information and control system provides an opportunity to reexamine business processes, making them more efficient and effective. When designing an information and control system, the designers should keep in mind the need for sustainability. The system should meet the entity’s current needs while keeping in mind needs that may evolve in the future as well as environmental, social, economic, and resource considerations, as well as an evolving environment surrounding the governance of an entity. Generally, there are several SDLC steps:

1. **Feasibility Study**
   Determine the strategic benefits of implementing the system either in productivity gains or in future cost avoidance, identify and quantify the cost savings of a new system, and estimate a payback schedule for costs incurred in implementing the system. Further, intangible factors such as readiness of the business users and maturity of the business processes will also be considered and assessed. This business case provides the justification for proceeding to the next phase.
2. **Requirements Definition**
   Define the problem or need that requires resolution and define the functional and qualitative requirements of the solution system. This can be either a customized approach or vendor-supplied software package, which would entail following a defined and documented acquisition process. In either case, the user needs to be actively involved.

3. **Software Selection and Acquisition (purchased systems) or Software Design (systems developed in-house)**
   - **Purchased systems** – Based on the requirements defined, prepare a request for proposal (RFP) from suppliers of purchased systems. In addition to the functionality requirements, there will be operational, support, and technical requirements. These, together with considerations of the suppliers' financial viability and provision for escrow, will be used to select the purchased system that best meets the organization's total requirements (e.g., Salesforce).
   - **Systems developed in-house** – Based on the requirements defined, establish a baseline of system and subsystem specifications that describe the parts of the system, how they interface, and how the system will be implemented using the chosen hardware, software, and network facilities. Generally, the design also includes program and database specifications, and will address any security considerations. Additionally, a formal change control process is established to prevent uncontrolled entry of new requirements into the development process. (Change controls are discussed in more detail in another section.)

4. **Configuration (purchased systems) or Development (systems developed in-house)**
   - **Purchased systems** – Configure the system, if it is a packaged system, to tailor it to the organization's requirements. This is best done through the configuration of system control parameters, rather than changing program code. Modern software packages are extremely flexible, making it possible for one package to suit many organizations simply by switching functionality on or off and setting the parameters in tables. There may be a need to build interface programs that will connect the acquired system with existing programs and databases.
   - **Systems developed in-house** – Use the design specifications to begin programming and formalizing supporting operational processes of the system. Various levels of testing also occur in this phase to verify and validate what has been developed. This would generally include all unit and system testing, as well as several iterations of user acceptance testing. **Scope creep** refers to uncontrolled changes or continuous growth in a project's scope; this can occur when the scope of a project is not properly defined, documented, or controlled.

5. **Final Testing and Implementation**
   Establish the actual operation of the new information system, with the final iteration of user acceptance testing and user sign-off conducted in this phase. The system may also go through a certification and accreditation process to assess the effectiveness of the business application in mitigating risks to an appropriate level and providing management accountability over the effectiveness of the system in meeting its intended objectives and in establishing an appropriate level of internal control. User acceptance testing is considered more important in an object-oriented development process than in a traditional environment because of the implications of the inheritance of properties in hierarchies.

6. **Post-implementation**
   Following successful implementation of a new or highly modified system, implement a formal process that assesses the adequacy of the system and projected cost-benefit or ROI
measurements vis-à-vis the feasibility stage findings and deviations. In so doing, Information Systems (IS) project and end-user management can provide lessons learned and/or plans for addressing system deficiencies as well as recommendations for future projects regarding system development and project management processes followed.

7. The **Maintenance Phase** (some interpretations do not include this phase)

   Monitoring and support of the new system, including ongoing training, help desk resources, and a system for making authorized and tested changes to the system.

**Agile Project Management**

Traditional project management (sequential IT development or waterfall methodology) generally completes each phase of the SDLC before the next is started. This can result in months of effort invested in a system that is a poor match to users' needs.

An agile methodology seeks a more efficient process than waterfall methodology. Scrum is probably the simplest form of agile implementation. Scrum emphasizes empirical feedback, team self-management, and the goal of developing properly tested product increments within short iterations. Whereas traditionally, programmers presented a complete application to users for acceptance testing, agile development is broken into sprints (typically 3-5 weeks, rather than 6-18 months). User stories are developed outlining probable scenarios. These stories form a backlog. The backlog is groomed (stories are refined and ordered based on how essential their function and estimated time to complete). Sprint goals are set at finishing a handful of user stories. As each sprint is finished, results are presented and feedback from users is sought. This feedback is used to further groom the backlog. The Scrum team (typically programmers, developers, and quality assurance specialists) evaluates its performance in the sprint and brainstorms on improvements in process as well as product to improve the results of the next sprint.

**Big Data**

Big data is information in such high volumes that is difficult for traditional information processing to collect and analyze. It is generated by the large volume of IT processing (social media use, cloud storage, website-tracking data, and ecommerce transactions). Instead of merely storing information for contractual, operational, reporting, and compliance purposes, big data is viewed as an asset that can mined to identify trends, enhance insight, and support decision making.

Data analysis (also called data analytics) is a process of examining, cleaning, organizing, and modeling data with the goal of support decision making.

**Data mining** is an analysis of data using tools which look for trends or anomalies without advance knowledge of the meaning of the data. It may involve the sorting through data to identify patterns and establish relationships, to bring to light previously unidentified relationships. Some of the parameters include association, sequence or path analysis, classification, clustering and forecasting (predictive analytics).

For example, Big Box, a large-scale retail store, analyzed receipt information to determine a few recurring shopping cart collections. One recurring companion purchase turns out to be beer and disposable baby diapers purchased between 3:30 and 6:30 p.m. Apparently, customers are stopping to purchase these staples on the way home from work. Big Box can use this insight to place products likely to appeal to customers purchasing these items in its stores near or between these staples.
As data mining can be used to address open-ended questions, it is very useful for auditing.

Data integration is the process of combining data from different sources (for example, from industry publications, customer surveys, invoices, etc.) in one collection for analysis.

Data visualization is the process of presenting data in a visual format, typically a diagram, chart, or word cloud. These presentations are limited only by the preparers' imaginations. A word cloud is a visual summary of text data, typically a circle or square of words or short phrases with frequency and importance indicated by size and color.

**Product Life Cycle Impact**

The Internet removes the physical constraints inherent in former economic models, giving rise to new paradigms. The sales cycle of a successful consumer item will grow to a peak. As its popularity declines, its physical shelf space will be assigned to a more popular item. Availability (and, hence, sales) will decrease to zero quickly. On the other hand, if the item is available online, demand will peter into a small, but sustainable, niche market. Conceivably, a small but ongoing demand will result in more cumulative sales over time than that of the initial peak.

In other words, a physical retail environment has limited space; it is logical to replace less popular items with more popular ones. In the physical world, sales would likely end abruptly, as demand for the item moves to the declining, almost-horizontal portion of the life-cycle curve—the tail end. In contrast, an electronic retail environment can hold less popular items indefinitely because warehouse storage space constraints are not a major concern. Also, the global reach of the Internet increases the likelihood that an extended sustainable niche market continues for less popular items. Search engines enable a large audience to find items in the “niche market” portion of the graph. The digital business model allows the tail end of the product life cycle to be long, giving rise to the phenomena of a long tail for product lives. For some products, the units sold in the long tail can be larger in total than in the mainstream period, especially for electronic products like movies or games.

The "Weighty Whale Superhero" Figurines Life Cycle graph illustrates to how a graph of demand for consumer items (clothing, books, music, videos, memorabilia, etc.) over time shows an upward curve in the introduction period, a large peak for the period when an item is popular, and a period when demand peters out.
For example, Aquatic Adventurers, an animated superhero series, is cancelled after its fifth season. In Fenland—a town of 100,000 people—chances are not good that sufficient customers will purchase the remaining 80 Weighty Whale Superhero figurines that Fenland Toys has in stock at the time the cancellation is announced. A year after the show is cancelled, the chances are even less likely that Fenland Toys will be able to sell these products locally. Without the Internet, a sustainable niche market does not exist for long after the mainstream market subsides; Fenland Toys would dispose of the figurines at a loss to make room for products in high demand. With the Internet, the series’ owners (or a movie webcasting network licensed by the owners) can show subscribers the existing episodes indefinitely. Also, Fenland Toys can offer the remaining figurines to billions of people. Even without the webcasting, Fenland Toys will be able to sell figurines to people nostalgic for the original broadcasts. With the webcasting, Fenland Toys will gain customers from people seeing the series online for the first time—conceivably years after the original broadcasts.

Lecture 7.03

CLASS QUESTIONS

Please see the Class Questions and Class Solutions for this Lecture at the end of this Section.

Lecture 7.04

ELECTRONIC COMMERCE

Whenever a network allows one computer to initiate an action that will have an effect on the other, it is known as a **Value-Added Network (VAN)**.
Electronic Data Interchange (EDI)

Extranets have been established as VANs to enable a process of communication between suppliers and customers (trading partners) known as **Electronic Data Interchange (EDI)**. This allows a company, for example, to have its inventory program automatically send an order to a supplier when quantities in stock of an item drop below a certain level. It is also possible to use the Internet rather than a traditional VAN for EDI (the advantage is that this would permit suppliers and customers to use the system without having previously established an extranet with each other). E-Commerce often involves electronic funds transfers (**EFT**), which can significantly reduce transaction costs. There are several **special considerations related to EDI**:

- **Strict standards** are needed for the form of data, so that it will be understood by the computers at both ends and to ensure completeness and accuracy. The critical nature of many EDI transactions, such as orders and payments, requires that there be positive assurances that the transmissions were complete. An example is the use of the ASCII format for text data.

- **Translation software** is needed by each computer so that it can convert data between the standard used for EDI and the form needed for processing internally. The process of identifying which field on the transmitted form corresponds to each field on the internal form is known as **mapping**.

- **Unauthorized access** to company computers and interception of transmissions are great dangers, requiring the use of **encryption** (application control) programs that make stolen data unreadable to someone without knowledge of the coding method and **firewall** programs that prevent access to the network without the explicit permission originating from the company computer. This is a particular concern with respect to EFT.

In an EDI environment **cryptography**, a public key certificate (also known as a **digital certificate or identity certificate**) is an electronic document which uses a digital signature to bind together a public key with an identity. Such information may include the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

There are numerous **advantages** associated with the use of EDI. It eliminates the need for human intervention and can be more efficient than other systems. When inventory is ordered automatically at the point that the reorder point is reached, it eliminates gaps and shortens the business cycle. In addition, payments are made and received automatically, which will tend to reduce accounts receivable balances.

Electronic commerce using **electronic data interchange** or **EDI** adds to the complexity of auditing. EDI enables:

- Communication without the use of paper
- Electronic funds transfers and sales over the Internet
- Simplification of the recording process using scanning devices
- Sending information to trading partners as transactions occur

**E-Commerce Risks**

Electronic commerce, as is true of any other form of commerce, depends on a level of trust between two parties. The challenges are proving to the buyer that the seller is who they say they are, proving to the buyer that their personal information remains confidential and that the seller cannot later refute the occurrence of a valid transaction. Some of the most important **elements at risk** are:
• **Confidentiality** – potential consumers are concerned about providing unknown vendors with personal information.

• **Integrity** – data, both in transit and in storage, could be susceptible to unauthorized alteration or deletion (i.e., hacking or the e-business system itself could have design or configuration problems).

• **Availability** – business may be conducted 24/7. Hence high availability is important with any system’s failure becoming immediately apparent to customers or business partners.

• **Authentication and nonrepudiation** – the parties to an electronic transaction should be in a known and trusted business relationship, which requires that they prove their respective identities before executing the transaction in preventing man-in-the-middle attacks (i.e., preventing the seller from being an imposter). Then, after the fact, there must be some manner of ensuring that the transacting parties cannot deny that the transaction was entered into and the terms on which it was completed.

• **Power shift to customers** – the Internet gives consumers unparalleled access to market information and generally makes it easier to shift between suppliers.

E-commerce increases the risk of *improper use of information*. Controls might include:

• Security mechanisms and procedures that, taken together, constitute a security architecture for e-commerce

• 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 e-commerce transaction can be identified uniquely and positively

There is also the risk of *improper distribution* of transactions with information being electronically transmitted to an inappropriate company. Controls might include:

• Routing verification procedures

• Message acknowledgement procedures

Finally, there is a danger that orders and confirmations might be sent by an imposter (this is known as **spoofing**), or transmitted files may be intercepted and altered maliciously by third parties before being sent to their destination. The controls might include:

• Echoing of transmitted documents back to the claimed sender so they know what the recipient has received in their name.

• **Digital signatures** on files and emails to prove the identity of the sender and to assure us that the information was unaltered in transmission (the Electronic Signatures in Global and National Commerce Act of 2000 permits the use of these in private contracts).

The reduction in the paper audit trail associated with EDI creates special challenges to the auditor.

• Detection risk may not be sufficiently reduced through substantive testing.

• Control risk must be reduced adequately to achieve an acceptable level of audit risk.

• Controls must be built into the system to insure the validity of information captured.

**Cryptocurrency** (or crypto currency) is a digital asset exchanged over the Internet outside of traditional banking and government institutions (Bitcoin for ex). Cryptocurrency is designed to work as a medium of exchange using blockchains to secure the transactions and to control the creation of additional units of the currency.

• Rather than governments controlling the supply of currency by printing more money or changing banking reserve requirements—resulting in inflation (or rarely, deflation), cryptocurrency is decentralized and has built-in restraints on how much may be created.

• Cryptocurrency networks use blockchains to maintain integrity. Blockchains are expanding chains of blocks (or records) that are linked and secured using cryptography. Each block
typically contains a timestamp, a link to a previous block, and the transaction data. Inherently, blockchains resist data modification.

- The safety, integrity and balance of ledgers within cryptocurrency systems is maintained by a community of mutually distrustful parties, referred to as miners. Miners are members of the general public using their computers to help validate and timestamp transactions. Miners add transactions to the ledger in accordance with an algorithm. Collectively, miners provide security to the system, each having financial incentive to maintain accurate ledgers.

- Compared with traditional currencies held by financial institutions or kept as cash on hand, cryptocurrencies are less susceptible to seizure by law enforcement and somewhat more anonymous (different currencies have different degrees of anonymity). Due to this anonymity, there is a risk that cryptocurrencies may become tools for cyber criminals. Along with facilitating money laundering and tax evasion, cryptocurrencies also may grease the wheels of black markets (illegal drug trade or other illegal activity).

Lecture 7.05

CLASS QUESTIONS

Please see the Class Questions and Class Solutions for this Lecture at the end of this Section.

Lecture 7.06

CONTROL OVERVIEW

One characteristic of an IT environment is a reduction in the segregation of duties. Although this might appear to create a potential problem:

- A computer has no incentive to conceal its errors.
- Functions often can be combined in an IT environment without weakening internal control.

In the operation of computer systems, management must focus on two broad types of controls:

- General controls – These relate to the overall integrity of the system. Controls include policies, procedures, and practices (tasks and activities) established by management to provide reasonable assurance that specific objectives will be achieved.
- Application controls – These are specific to individual programs and uses of the system.
## General Controls – Overall Environment

<table>
<thead>
<tr>
<th>Overall Computer Environment</th>
<th>Application (Program Controls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) <strong>Personnel Policies</strong></td>
<td>1) <strong>Input</strong></td>
</tr>
<tr>
<td>• <em>Systems</em> = Development &amp;</td>
<td>• Check Digit → Inputted correctly</td>
</tr>
<tr>
<td>Maintenance* (analysts,</td>
<td>• Validity Check (Valid SS#)</td>
</tr>
<tr>
<td>application programmer,</td>
<td>• Edit Test → #s in SS not letters</td>
</tr>
<tr>
<td>database administrator)</td>
<td>• Limit Test → SS#’s not greater than 9 characters</td>
</tr>
<tr>
<td>• <em>Operations</em> = Input*</td>
<td>• Financial total</td>
</tr>
<tr>
<td>(data entry → make</td>
<td>• Record counts</td>
</tr>
<tr>
<td>sure computer operator</td>
<td>• Hash = A meaningless total</td>
</tr>
<tr>
<td>is computer illiterate);</td>
<td>• Nonfinancial totals</td>
</tr>
<tr>
<td>=Output* (control clerk</td>
<td></td>
</tr>
<tr>
<td>or librarian)</td>
<td></td>
</tr>
<tr>
<td>2) <strong>File Security</strong></td>
<td>2) <strong>Processing</strong></td>
</tr>
<tr>
<td>• Back Up - Grandfather/father/son retention system</td>
<td>• System &amp; software documentation</td>
</tr>
<tr>
<td>• Lock Out</td>
<td>• Error-checking compiler</td>
</tr>
<tr>
<td>• Read-Only</td>
<td>• Test data</td>
</tr>
<tr>
<td>3) <strong>Contingency Planning</strong> – Business Continuity/Disaster Recovery (hot/cold site)</td>
<td>3) <strong>Output</strong> – Accurate</td>
</tr>
<tr>
<td>• Hot Site (Computer’s ready to go)</td>
<td>• Distribution lists</td>
</tr>
<tr>
<td>• Cold Site (No computer waiting)</td>
<td>• Shredders</td>
</tr>
<tr>
<td>• Mirrored web server – off site</td>
<td>• System testing</td>
</tr>
<tr>
<td>4) <strong>Computer Facilities</strong> – Fire/Insurance/smoke detectors/l.D. badges (Physical Controls)</td>
<td>5) <strong>Access Controls</strong> (biometrics)</td>
</tr>
<tr>
<td>5) <strong>Access Controls</strong> (biometrics)</td>
<td></td>
</tr>
</tbody>
</table>

Contingency planning refers to general controls that are designed to protect the information from accidental or intentional destruction or unauthorized alteration. This includes:

- **Backup & planned downtime controls** - Copies of files and programs should be maintained to allow reconstruction of destroyed or altered files. This may include copies on the same computer, backups to removable storage media, such as disks, and off-premises backups to computers and locations outside the company. Copies may be identical or the client may use the grandparent/father/son retention system, in which periodic saving of data versions allows the reconstruction of records by starting with an older file and reentering lost data since that time (the name comes from the general idea of saving at least two generations of older data so that, if the immediate version before the lost file is also lost, reconstruction can start two versions back with reentry of all data processed since that point). Since some downtime is inevitable, planned downtime allows maintenance so that unplanned downtime doesn't interrupt system operations.
**Checkpoint** – Similar to grandfather/father/son, but at certain points, “checkpoints,” the system makes a copy of the database and this “checkpoint” file is stored on a separate disk or tape. If a problem occurs, the system is restarted at the last checkpoint.

**Business continuity and disaster recovery** - The company should have plans in place that will allow operations to be restored and continued in the event of physical destruction or disabling of the site of computer operations. This can be done by maintaining an alternate **hot site**, which has available computers and data ready to begin operations immediately in the event of the disaster, or a **cold site**, which has available space for operations but will require setup of computers and loading of data before operations can begin at that site. All critical applications need to be identified so a plan can be established. Establishment of an off-site **mirrored web server** is an effective way, particularly for an e-commerce company, to assure continuity of operations in the event of a natural disaster.

- The configuration that represents the most complete disaster recovery plan should provide for an alternative processing site, backup and off-site storage procedures, identification of critical applications, and a testing of the plan.

---

**Lecture 7.07**

**CLASS QUESTIONS**

Please see the Class Questions and Class Solutions for this Lecture at the end of this Section.

---

**Lecture 7.08**

**GENERAL CONTROLS**

There are other general controls, in addition to contingency planning. Just as in a manual system, one of the **general controls** in an IT environment involves segregation of the incompatible duties of authorization, recording, and custody:

- **Authorization** - The development of new programs and changes to existing programs should be performed by **systems analysts** and **programmers**. These personnel should not be involved in the supervision of computer operations or the control and review of output. Systems analysts work with operating systems and compilers.

- **Recording** - **Data input clerks** and **computer operators** have the role of entering information into the computer and running the programs. These personnel should not have access to program code that would enable them to modify programs nor should they control the output.

- **Custody** - **Control clerks** and **librarians** obtain and review the output from computers to review exception reports indicating inappropriate functioning of the computer, send printouts and other output to the appropriate destinations, and maintain disks, tapes, or other storage units of data. These personnel should not have the ability to create or alter programs or to operate the computers that generate the information.

Clearly, general controls over **access** to computers and files are of great significance in evaluating internal control in an IT environment. This is particularly important in networks, since the data is distributed widely in such cases. Access to programs and data should require the entry of **passwords** or identification numbers (biometrics), and different levels of password authority should apply so that individuals only gain access to the programs and files that are compatible with their assigned responsibilities. It is also considered good practice to require that individual users change assigned passwords when new accounts are created.
Failure to remove user accounts when an employee leaves a client is a major security risk. An auditor can test these procedures by entering invalid passwords to see that they are rejected and verifying that valid passwords only provide compatible access. The systems access log should also periodically be reviewed to detect computer-related fraud. A **concurrent update control** (concurrency control) helps to address conflicts in a multi-user system, when two people, for example, are trying to purchase tickets at the same time. It will lock the other out, so as not to oversell the tickets.

Limiting access to an entity's computers and the data they hold is becoming an increasingly challenging problem. Measures, referred to as **cybersecurity**, are designed to protect computers against unauthorized access or attack. The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, released a framework for improving critical infrastructure cybersecurity.

**Documentation** of new programs and alterations to existing programs ensures that IT personnel are aware of the availability and proper use of programs and that changes in programming personnel during projects does not interfere with the ability of other employees to understand what has been done previously.

**Hardware controls** are built into the processing equipment by the manufacturer and provide reasonable assurance that data are not altered or modified as they are transmitted within the system. Binary computers can only think in terms of **bits** (binary digits) of information that are on or off ("1" or "0"). A series of 8 consecutive bits will produce a **byte** of information that represents a unit of human thought, such as a letter, number, or other character. Hardware controls may include:

- **Parity check** - In the storage of bytes, one bit will be a "dummy" bit that doesn't represent any actual information, but is turned on automatically when necessary so that the total number of bits in the on position is an odd number (in an odd-parity computer). When the computer is reading bytes of data from a chip or disk drive, a byte with an even number of bits turned on will be known to be functioning improperly.

- **Echo check (Echo control)** - When data is being transmitted from one computer to another, especially over telephone lines, distortions caused by static or other causes can cause information to be transmitted improperly. An echo check involves the data sent from one computer to another being transmitted back to the original one, which will verify that it has received what it sent. If the echoed data doesn't agree with the transmission, the packet of data is then resent.

**Personal computers** (also called microcomputers) present additional control risks since they are small and portable, making them easier to steal or damage. In a microcomputer environment, data and software are also more accessible, and individuals can more readily access unauthorized records and modify, copy, or destroy data and software. Also, individually installed applications make integration difficult in such an environment. A variety of controls can be employed in a microcomputer environment.

- Maintain an inventory listing of all microcomputer equipment and the purposes for which it is used.
- Keyboard locks can be built into the CPUs of microcomputers so that unauthorized users will not have access.
- Microcomputers and monitors can be secured to desks or fixtures to discourage theft.
- Passwords that are changed periodically limit the access of unauthorized users to sensitive data.
• Periodic backup of data on microcomputers enables recovery in the case of alteration or destruction of data.
• Sensitive information can be maintained in offline storage and kept in locked cabinets to prevent unauthorized access.

APPLICATION CONTROLS

Application controls are those applied to specific business activities within a computerized processing system to achieve financial reporting objectives. Application controls are specific to each cycle and refer to a client's activities. Application controls relate to data input, data processing, and data output. They are designed to ensure the proper recording of transactions and to prevent or detect errors and fraud for transactions within these cycles. Because application controls are related to specific transactions, audit teams rely extensively on the effectiveness of these controls to mitigate the risk of material misstatement for account balances or classes of transactions. Application controls include:

- **Preventive controls** are designed to prevent errors and fraud.
- **Detective controls** are designed to detect errors and fraud (e.g., reviewing the audit log).
- **Corrective controls** allow individual users to follow up on detected errors and fraud.

Input Controls

Input controls are designed to provide reasonable assurance that data received for processing by the computer department have been properly authorized and accurately entered or converted for processing. These controls also provide the opportunity for entity personnel to correct and resubmit data initially rejected as erroneous. Errors can be avoided through:

- Observational controls
- Use of point-of-sale devices, such as scanners, to gather and record data automatically
- The use of preprinted recording forms can minimize errors.
- Data transcription controls, such as preformatted screens, can minimize errors when converting data to machine-readable form.
- Automated log-off of inactive users is an effective way to prevent unauthorized access to sensitive data. Many banking institutions use these measures.

As data is being entered, it should be subject to various forms of verification (Logic Tests). These might include:

- **Field checks** - Data is validated as to the correct length, character types, and format accepted. For example, an entry of a license plate might be verified for type (alphanumeric, so that only letters and numbers are acceptable) and length (not longer than 7).
- **Validity checks** - Data is compared with a list of acceptable entries to be sure it matches one of them. For example, a field to accept the two-letter state abbreviation will be checked against a file that lists all the acceptable choices, so that an entry of OG for the state will be rejected as invalid.
- **Limit tests** - Numbers are compared to limits that have been set for acceptability. For example, the entry of a pay rate may be compared to the current minimum wage on the lower side and $50 per hour on the upper side to be sure the number entered makes sense. This is sometimes called a reasonableness test, and is the closest computer equivalent to human judgment in reviewing information.
- **Check digits** - Numbers with no obvious meaning, such as identification numbers, are often designed so that one of the digits is determined by a formula applied to the rest of the number. The computer applies the formula when a number is entered to determine if
it is an acceptable one. This control makes it difficult for someone to invent a fake number if they do not know the formula, since the program will recognize a number that isn’t designed so that the check digit is correct. The check digit can actually be either a number or letter, and can be placed in any consistent position in the overall identification. For example, many states have driver licenses that start with a letter which is derived from a formula applied to the numbers which follow it, and a person trying to create a fictional license will only have a 1 in 26 chance of correctly guessing the letter that should be in the first position based on the numbers.

When using batch processing of data, the data input clerk will often prepare manual control totals to be compared with computer-generated totals of entered information in order to ensure accuracy of inputs. These totals include:

- **Record count** - The total number of records entered into the program during a period.
- **Financial total** - The total dollar amount of entries that are financial in nature.
- **Hash total** - The total of values (such as Social Security numbers) which cannot be meaningfully added together, but which serve as a way to verify the correct entry of these values.

For example, assume that the checks written during a particular day are being entered into a checkbook program, and that the data input clerk is working from the following sheet to make the entries:

<table>
<thead>
<tr>
<th>Check Number</th>
<th>Payee</th>
<th>Amount</th>
<th>Account Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Philipp Corporation</td>
<td>$ 500.00</td>
<td>307</td>
</tr>
<tr>
<td>1002</td>
<td>Rog Enterprises</td>
<td>$3,000.00</td>
<td>602</td>
</tr>
<tr>
<td>1003</td>
<td>Ruiz Company</td>
<td>$ 600.00</td>
<td>302</td>
</tr>
<tr>
<td>3006</td>
<td></td>
<td>$4,100.00</td>
<td>1211</td>
</tr>
</tbody>
</table>

After the data input clerk enters each of the checks, the computer will then indicate:

- Checks Entered = 3 (record count)
- Check Number total = 3006 (hash total)
- Amount total = $4,100.00 (financial total)
- Account Code total = 1211 (hash total)

The data input clerk would have also determined these numbers by computing them from the input sheet, and the agreement of the clerk’s totals with those of the program will indicate all lines most likely have been entered correctly.

A program may also perform edit checks on batch-processed data to verify that each individual entry is appropriate, and generate a list of rejected transactions for review by the control clerk.

**Processing Controls**

Once data is input, processing controls are designed to provide reasonable assurance that data processing has been performed accurately without any omission or duplicate processing of transactions. Many processing controls are similar in nature to input controls, but they are used in the processing phases, rather than at the time input is verified. The most fundamental processing
control a client can implement is periodically testing and evaluating the processing accuracy of its programs.

- Systems and software documentation allows system analysts to verify that processing programs are complete and thorough.
- Computer programs can be tested using error testing compilers to ensure that they do not contain programming language errors.
- Test data exposes the program to one sample of each type of exception condition likely to occur during its use.
- System testing can be used to make certain that programs within the system are interacting properly.

Output Controls

Output controls represent the final check on the results of computerized processing. Output controls are concerned with detecting errors rather than preventing errors. These controls should be designed to provide reasonable assurance that only authorized persons receive output or have access to files produced by the system.

AUDITING ISSUES

Although the existence of an electronic system does not change the basic objectives of an audit engagement, it has a major impact on the approach used to achieve those objectives.

Computer software cannot replace the judgment of the auditor. The responsibility for determining the acceptable level of audit risk and assessing the component risks remains with the auditor.

Differences

AU-C 315 summarizes the differences as follows:

- **Benefits of IT**
  - Consistency – Computers process data the same way every time.
  - Timeliness – Electronic processing and updating is normally more efficient.
  - Analysis – Data can be accessed for analytical procedures more conveniently (with proper software).
  - Monitoring – Electronic controls can be monitored by the computer system itself.
  - Circumvention – Controls are difficult to circumvent when programmed properly, and exceptions are unlikely to be permitted.
  - Segregation of duties – Security controls can prevent the performance of incompatible functions by the same individual or group through security controls in applications, databases, and operating systems.

- **Risks of IT**
  - Overreliance – Without clear output, IT systems are often assumed to be working when they are not.
  - Access – Disclosure, destruction and alteration of large amounts of data are possible if unauthorized access occurs.
  - Changes in programs – Severe consequences without detection are possible if unauthorized program changes occur.
  - Failure to change – Programs or systems are sometimes not updated for new laws, rules, or activities.
Manual intervention – Knowledgeable individuals can sometimes alter files by bypassing the appropriate programs.
Loss of data – Catastrophic data loss is possible if appropriate controls aren’t in place.

Risks
There are two risks of major concern to the auditor:

- Unauthorized access to a computer system can cause more damage to the accounting system as a whole than in a manual system where it is difficult for one person to access all the different records of the system.
- The audit trail is an electronically visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source.

An audit trail is also important to the client for the proper functioning of the system during the year, since such a trail allows monitoring of activities, providing a deterrent to fraud and making it possible to answer queries by examining the source data. The auditor should establish the reliability and extent of the audit trail.

Audit Efficiency
When examining a company in an IT environment, the auditor may decide to use a generalized audit software package. This refers to a series of programs that can be used for general processes, such as record selection, matching, recalculating and reporting and might include:

- Programs to access client files for purposes of testing. For example, the auditor’s program may access computerized inventory files to determine the location of inventory, perform analytical procedures (such as calculating inventory turnover), or review dates of last purchase and sale in order to identify obsolete or slow-moving inventory.
- Source code comparison programs that can detect unauthorized changes made by the client in programs that the auditor is testing. For example, after the auditor has verified the proper functioning of a copy of the payroll program provided to them by the client for testing, this program would compare the tested program with the one being used by the client to process an actual payroll period to be sure the files are identical.
- Programs that duplicate common functions of client software that can be used to perform parallel simulation, in which the auditor inputs client data to the auditor’s program (created by the auditor) to see if it produces the same results as the client’s program. For example, the auditor might obtain the raw data for an actual payroll period and run it through a payroll program included in the generalized audit software package to see if the checks and payroll records produced are identical to the checks and records generated by the client’s program.
- Programs to produce spreadsheets for working trial balances and similar audit needs.

When the client has a program that the auditor wishes to verify and for which there is no appropriate equivalent program available to the auditor, techniques involving the direct use of the client program are necessary. One approach is known as the test data approach, in which the auditor will develop simulated transactions to enter into the client’s program. Characteristics of this approach include:

- The auditor can include both valid and invalid transactions to verify that the program processes appropriate data correctly and rejects inappropriate transactions.
- The auditor only needs to design simulated transactions for those valid and invalid conditions that interest the auditor.
• Only **one example** of each valid and invalid condition needs to be included (since computer programs are consistent in the way they handle items), making this an efficient method of testing.

The auditor should obtain audit evidence about the accuracy and completeness of information produced by the entity's information system when that information is used in performing audit procedures. The primary **advantage** of IT as it relates to an audit is that a computer is not subject to **random errors** as is a human. Thus, an auditor who has **verified** that a computer program is working properly will **not** have to **test individual transactions** to be sure the computer is following directions consistently: it will always follow its program. An audit of a computerized system can, therefore, rely more heavily on internal control structure and reduce the need for substantive testing, making the audit potentially more efficient.

It is possible to create **embedded audit modules** in the DBMS so that information wanted by an auditor during annual engagements can be easily accessed. One difficulty in this idea is that these modules should be included in the design of the system itself, forcing the outside auditor to be involved in consulting on the design, and may impair the auditor's independence.

One danger is that the client may provide the auditor with a program to verify which isn't the actual program used by the client. To avoid this, the auditor will often include the **test data** in an **integrated test facility**, including the simulated data (fictitious transactions) along with actual data during a program run. For example, the auditor may add simulated payroll data to the actual data for a pay period, so that the testing occurs at the same time the actual employee information is being processed (of course, the simulated data is specially coded so as not to be permanently mixed with the real data).

If it isn't practical to use an integrated test facility, the auditor may use an approach known as **controlled reprocessing**, in which the auditor supervises the entry of actual client data into the client program to reproduce the results of a previous run of the program by the client. After verifying that the results are identical to the previous run, the auditor knows that the program is the actual one used, and can enter the test data into it at a separate time.

To summarize the techniques available:

<table>
<thead>
<tr>
<th>Data</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Data</strong> (Phony Data) – theoretically only have to check one above and one below credit limit.</td>
<td>Auditor</td>
</tr>
<tr>
<td><strong>Controlled reprocessing</strong></td>
<td>Client's</td>
</tr>
<tr>
<td><strong>Integrated Test Facility (ITF)</strong> (Dummy division or file &amp; fictitious transactions)</td>
<td>Auditor &amp; Client's</td>
</tr>
<tr>
<td><strong>Transaction Tagging</strong></td>
<td>Client's information with a tag</td>
</tr>
<tr>
<td><strong>Parallel Simulation</strong></td>
<td>Client's</td>
</tr>
<tr>
<td>Actual Client Data</td>
<td>Simulated Data</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Actual Client Program</td>
<td>Controlled Reprocessing</td>
</tr>
<tr>
<td>Program Purchased Separately by Auditor</td>
<td>Parallel Simulation</td>
</tr>
</tbody>
</table>

**Trust Services**

Trust Services are governed by SSAE (Statements on Standards for Attestation engagements) and represent attest engagements in which a CPA assesses a client’s commercial internet site and reports on whether the system meets one or more of the following **principles**: Security; Availability for operation; Processing integrity; Online privacy; and Confidentiality. For each Principle reported, the auditor considers each of the following **4 criteria**: Policies; Communications; Procedures; and Monitoring.

Both WebTrust and SysTrust are designed to incorporate a seal management process by which a seal (logo) may be included on a client’s website as an electronic representation of the practitioner’s unqualified WebTrust report. If the client wishes to use the seal (logo), the engagement must be updated at least annually. Also, the initial reporting period must include at least two months. Any of the 5 types of opinions may be issued as discussed in the audit report section.

- **Websites (WebTrust)** – An assurance function designed to reduce the concerns of Internet users regarding the existence of a company and the reliability of key business information placed on its website.
- **Information systems (SysTrust service)** – An assurance function that reviews an entity’s computer system to provide confidence to business partners and customers concerning the security, privacy, and confidentiality of information in addition to system availability and processing integrity.

---

**Lecture 7.09**

**CLASS QUESTIONS**

Please see the Class Questions and Class Solutions for this Lecture at the end of this Section.

---

**Lecture 7.10**

**GLOSSARY**

Acquaintance with these terms is necessary to understand exam IT questions sufficiently well to answer them correctly, although most of this information is tested directly on the AICPA exam only infrequently.

**Artificial Intelligence**

Artificial intelligence is computer learning, planning, and solving problems, when the computer perceives its environment and executes actions designed to reach a goal. It generally includes competing at strategic games (such as chess), understanding human speech, and complex tasks.
(such as driving a car). Machine learning involves algorithms that can learn from data and make predictions on data in a reiterative fashion.

**Transaction Processing**

The processing of transactions can take place in one of two general ways:

- **Online Transaction Processing (OLTP), online real-time (OLRT) processing**
- **Batch processing**

**OLTP** means that the database is updated as soon as a transaction is received (immediately). Online transaction processing keeps business records up-to-date the moment transactions are keyed or transmitted into a system. This produces records that are as up-to-date as possible, but poses a problem of requiring that computers be continually running and accessible at all points-of-transaction. This is a good method to be used by retail businesses. With the common presence of computers, this has become the default processing method for most business activity.

**Batch processing** involves gathering information and then entering transactions in a group (usually dollar fields) to the computer periodically. This allows for greater control over the input process, including more possibility for verifying data entry with control totals and authorization before input. The major difficulty is associated with the delay between the transactions and the input, which can result in accounting records not accurately reflecting the current situation.

As an example of the choice between the two approaches, a bank is going to use OLTP for the processing of cash withdrawals, since it is critical that these be immediately reflected in the depositor’s balance and errors can be easily reversed later with little harm to the bank. On the other hand, a bank would prefer to use batch processing for deposits to be sure that increases in depositors’ balances are authorized and checked carefully for accuracy before accounts are updated. Unauthorized postings of deposits could allow a depositor to withdraw large sums of money and delays in posting would be of little negative consequence to the bank itself. As a practical matter, batch processing tends to be used for large (such as bank deposits over $5,000) or sporadic (such as payroll preparation) transactions.

**Networks**

In the early days of computers, each device was so expensive that a company rarely had more than one and all activity had to take place on that single computer. Although different people could connect to that single computer using remote terminals, these were simply input and output devices (essentially equivalent to just the keyboard and monitor on a current desktop). All activity had to take place on the one computer, known as centralized processing. Today, computers are so reasonably priced that, in many businesses, employees each are assigned their own computers (whether a laptop, tablet, or smartphone). This allows the allocation of a large volume of computer tasks to different employees and computers at different locations, known as distributed processing. Since the data utilized by the company is no longer on a single computer, it is necessary for them to be able to connect to each other in some way to form a network.

In a computer network, computers are connected to one another to enable sharing of peripheral devices, sharing data, and programs stored on a file server. A file server is a high capacity disk storage device or a computer that stores data centrally for network users and manages access to that data. File servers can be dedicated so that no process other than network management can be executed on that server while the network is available. Non-dedicated file servers allow the standard user applications to run while the network is available.
Networks allow various user departments to share information files maintained in databases. Databases should:

- Provide departments with information that is appropriate
- Prevent access to inappropriate information

Network configurations allow the linking of computers in different ways:

- **Local area networks (LANs)**: Communications networks that serve several users within a specified geographical area. A personal computer LAN functions as distributed processing in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network. Good management controls, such as access codes and passwords, are essential.

- **Wide area networks (WANs)**: Computer networks connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries.

- **Value-added network (VAN)**: Links computer files of different companies together. As a result, it is necessary to have increased security for data transmissions to make certain that others will not have access to inappropriate entity information.

- **Virtual Private Network (VPN)**: Allows users to access network resources from remote locations; may or may not be incorporated as part of a larger cloud computing strategy.

The need for solid physical transmission media in LANs has been overcome through the development of wireless local area networks (WLANs). Short-range radio transmission allows different computers to communicate with each other and share printers, Internet connections, and other devices. The two prominent standards for WLANs are **Wi-Fi** (also known as 802.11) and **Bluetooth**. Any devices that are in the vicinity of each other and which follow the same standard can communicate. In addition to computers, cell phones and personal digital assistants (PDAs) are often equipped to use one or both standards.

Clearly, unauthorized access is a major danger with WLANs and both encryption of data and passwords (a technical security control) to connect to the system are critical security needs to prevent others with wireless devices from accessing the system. On the other side, businesses such as hotels and restaurants have sometimes installed Wi-Fi connections for the benefit of guests and patrons to allow them high-speed Internet access (sometimes requiring logging into a network at a fee and sometimes at no charge to encourage visitors).

Networking would get very complicated if every computer in a network had to be able to directly connect to every other computer in the network (in order for 10 different computers in an office to be connected this way in a LAN, there would have to be 45 different cables!). Even in the case of a wireless network, a computer would have to be able to distinguish all the different signals coming from different computers.

**Topology** refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate are determined by the network's topology. To simplify the process, the communication is normally organized (and can be visualized) in one of the following ways:

- **Bus**: A common path or channel between hardware devices, which can be located between components internal to a computer or between external computers in a communications network.

- **Star**: There is one computer (central hub) to which all other computers connect, so that all data is first received and then sent from that one computer (in email systems, this will
allow copies of all messages to be stored on a single computer while still allowing communication among all of the others).

- **Ring** – Each computer is connected to its two closest neighbors in a closed loop, and information is transferred through each intermediate computer to get to the intended destination (notice there will be two directions that can be used, so an interruption of a single connection won't bring down the network).

- **Tree** – Groups of star-configured networks are organized in branches with one computer at the base, so that computers that are on the same branch can connect to each other without going through the root computer, but computers on different branches may have to go through the root computer.

- **Mesh** - Devices are connected with many redundant interconnections between network nodes. In a pure mesh topology, every node has a connection to every other node in the network.

Networks may involve any size group from two (as in the case of many home networks) to the entire world (in the case of the Internet).

An **Intranet** is a network that is limited to the computers of a single company.

An **Extranet** is similar to an Intranet, since it is primarily for users within a single company, but select customers and vendors are able to participate as well.

The **Internet** is a worldwide network that allows virtually any computer system to link to it by way of an electronic gateway. The Internet facilitates data communication services including:

- Remote login
- File transfer
- Electronic mail (Email)
- Newsgroups

The networking of different computers allows more than just the transfer of information from one to another. It also allows one computer to be used to operate the other. In **client/server computing**, the users of client computers will be able to access a server computer and can be given the ability to add, edit, or delete data on the server, or even to operate programs running on the server as well as transfer files between their client and the server. The physical device used by an employee to access these resources, usually a computer, also is called a workstation. The server doesn't, in effect, have any particular user since it is being operated by the users on the client computers, and a server computer doesn't even need a display monitor or keyboard, except for initial set up. **Virtualization** is a method used to create multiple virtual machines for clients to access on a single physical server.

The development of the Internet has also created many opportunities and challenges when it comes to the use and protection of information. One example is the emergence of **mobile computing**. This allows individuals to use various devices to obtain access to data and information from whatever location they are at. Another is the rapidly spreading influence of **social media**. Social media enables individuals to create, share, and exchange information and ideas in virtual communities and networks. Social media has proven an effective tool for:

- Market research
- Communication
- Sales promotions
- Relationship development (match.com)
- E-commerce
Cloud computing is a model that allows organizations to use the Internet to access and use services and applications that run on remote third-party technology infrastructure, rather than rely on in-house platform solutions (e.g., Spotify, Youtube, our online course). Cloud computing is the integration of virtual machines, remote services for hardware and software, and Web access. Working in the cloud can mean simply using remote server for data storage or using a browser to access Web-based applications. Because cloud computing utilizes third-party hardware and software, it usually has lower upfront costs for equipment and maintenance. Cloud computing is generally not the best way to secure sensitive corporate information, as there are security risks to transmitting information over the Internet. Common implementations of cloud computing involve off-the-shelf software that is not developed or modified in-house, with generally limited configuration and program modification options.

Collaborative computing allows users to connect, communicate and work on projects and documents together in real time. Examples include instant messaging (google chat), video conferencing, multicasting, email applications, groupware systems, just to name a few.

Gamification refers to applying game elements and digital game design techniques to solving problems and making decisions that are not generally associated with games. This may include business problems or challenges related to social impact.

Geolocation is information about your physical, real-world location that can be associated with an IP or MAC address. This information can be used by applications to show how nearby your friends or employees are, get directions to a restaurant or customer, or to geotag your photos.

World Wide Web To make use of the Internet more user-friendly, a framework for accessing documents was developed known as the World Wide Web.

- Hypertext Transfer Protocol (HTTP) – The language commonly understood by different computers to communicate via the Internet.
  - Transmission Control Protocol and Internet Protocol (TCP/IP) – an IP is a unique computer address and a TCP/IP is a communications protocol designed to network dissimilar systems, such as viewing a webpage.
- Document – A single file on any computer that is accessible through the Internet.
- Page – The display that results from connection to a particular Internet document.
- Uniform Resource Locator (URL) – The “address” of a particular page on the Internet.
- Web Browser – A program that allows a computer with a particular form of operating software to access the Internet and which translates documents for proper display.
- Server – The computer that is “sending” the pages for display on another computer.
- Client – The computer that is “receiving” the pages and seeing the display.
- Upload – Sending information from a client to a server computer.
- Download – Sending information from a server to a client computer.
- HTML (HyperText Markup Language) and XML (Extensible Markup Language) are specialized programming languages used to create websites.

Networks and Control Risk
To minimize control risk, a network should have some form of security that limits access to certain files to authorized individuals.
- Certain individuals may have read only access to files.
- Others will be authorized to alter the data in the files, such as read/write.
A virus is a program with the ability to reproduce by modifying other programs to include a copy of itself. A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network. A Trojan horse is a purposefully hidden malicious or damaging code within an authorized computer program. Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.

- A worm is a program that duplicates itself over a network so as to infect many computers with viruses.
- A hoax virus is a widely distributed email message warning of a virus that doesn’t exist.
- A killer application simply refers to a program that is extremely useful, and is not anything dangerous.
- Phishing (brand spoofing or carding) is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Ransomware is an unauthorized program used by cybercriminals to extort money that restricts access to data until a ransom is paid and a digital key is entered.

Antivirus software is a software application deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.

Unauthorized downloads of “pirated” software from the Internet can also create risks of lawsuits and criminal prosecutions (e.g., movies, programs and music).

A tool for establishing security is a firewall, which prevents unauthorized users from accessing data. A firewall can be in the form of a computer program (software) or a physical device that blocks the transmission media being used (hardware). A network firewall is designed to prevent unauthorized access to the company computers, while application firewalls protect individual programs. Network firewalls are easier and cheaper to implement, but if penetrated, leave the computers at severe risk. Application firewalls need to be installed for each individual program the company wishes to protect, but allow additional user authentication procedures to protect the program and data and make access more difficult.

Lecture 7.11

GLOSSARY (CONTINUED)

Hardware

Hardware is the physical electronic equipment. Common components include:

- Central Processing Unit or CPU – The principal hardware component that processes programs.
- Memory – The internal storage space or online storage, often referred to as random access memory or RAM.
- Primary Storage – Computer memory which is used to store programs that must be accessed immediately by the CPU.
- Offline Storage – Devices used to store data or programs externally, including magnetic tape, flash drives, thumb (usb) drives, digital video disks (DVDs), and compact disks (CDs).
- File Server – A high capacity disk storage device or a computer that stores data centrally for network users and manages access to that data. File servers can be dedicated so that no process other than network management can be executed while the network is
available. File servers can also be non-dedicated so that standard user applications can run while the network is available.

- **Input and Output Devices** – Devices that allow for communication between the computer and users, such as a terminal with a screen and a keyboard, scanners, microphones, wireless hand-held units, barcode readers, point-of-sale registers, optical character readers, mark sense readers, light guns, printers, speakers, floppy disk drives, CD and DVD drives, magnetic tape drives, and magnetic disk drives.

- **Router** – A specialized device that receives data packets from one computer and sends it toward its destination in the most efficient manner possible. The Internet, in fact, primarily consists of a series of routers used to transmit information among all the different computers of the world that are connected to the Internet at any one time. When a computer in California connects to a website in Australia, the two computers aren't actually connected to each other, and there might be 10 computers between them acting as intermediary routers. When parts of the Internet go down, due to a power outage or other difficulty, most people never notice because the routers find another way (route) to get the information to its destination.

- **Gateway** – This is a device (router, firewall) on a network that serves as an entrance to another network. In order for a home or business to connect to the Internet, for example, it must connect to a gateway computer at their Internet Service Provider (ISP), which is the first router in the process of connecting to the rest of the Internet.

### Storage Devices

Magnetic tape – Inexpensive form of storage used primarily for backup, since only **sequential** access to data is possible.

Magnetic disks – Permanent storage devices inside a computer (including hard drives) that allow **random** access to data without the need to move forward or backward through all intervening data. Some systems use **RAID** (redundant array of independent disks), which includes multiple disks in one system so that data can be stored redundantly and the failure of one of the disks won't cause the loss of any data.

Transportable forms of storage - In increasing order of capacity, these include:

- Floppy disks
- Zip disks
- Compact disks (CDs)
- Optical disks (DVDs)
- Thumb drives

### Input (Data-entry) and Output Devices

- Visual display terminal (keyboard and monitor)
- Mouse (including stylus, mousepad, joystick, and light pen)
- Touch-sensitive screen
- Magnetic tape reader
- Magnetic ink character reader
- Scanner
- Automatic teller machine
- Radio frequency data communication
- Point-of-sale recorder
- Voice/retina recognition
• Electronic data interchange
• Barcode readers

Software
Software consists of programs and supporting documentation that enable and facilitate use of the computer. Software controls the operation of the hardware and the processing of data. Software is either system software or application software.

• System software is made up of the programs that run the system and direct its operations, comprised of the operating system and utility programs. An operating system (OS) is a set of system software programs in a computer that regulate the ways application software programs use the computer hardware and the ways that users control the computer. Examples of commonly used operating systems are Windows and UNIX. Such programs may be designed to allow functions such as:
  o Multiprocessing – The simultaneous operation of multiple programs on a single computer.
  o Windowing – The ability to display the output of different programs on the monitor or portions of the monitor at the same time, as well as easily switch the display from one program to another (whichever program is set to accept and process the next click of the mouse or keyboard is known as the active window).

• Application software is designed to perform specific tasks for the company.
• Utility programs are used for sorts, merges, and other routine functions to maintain and improve the efficiency of a computer system. Specialized security software is a type of utility program used to control access to the computer or its files.
• Library programs are limited programs used by other programs, such as a random number generator.
• A query program is an application that counts, sums and retrieves items from a database based on user criteria.
• Algorithms are instruction sets used in programs to define and control processes.
• Communication software handles transmission of data between different computers.
• Protocol – Rules determining the required format and methods for transmission of data.
• Heuristic refers to software that can learn and modify its operations, such as a spell-checking program that can accept new words in its dictionary.
• Almost all commercially marketed software is copyrighted, but not necessarily copy-protected.
• Open source is a software development model with free access to programs created and supported by developers and users. The program source code is freely available to download, modify, and adapt to meet specific needs. The growing use of powerful collaborative and networking tools (social networks, blogs, news feeds and aggregators, podcasts, and collaborative content management) fuels the development of open source software.

Programming Languages
• Source program is in the language written by the programmer (high level languages resemble English while assembly languages are close to direct machine instructions).
• Object program is in a form the machine understands (on-off or 1-0).
• Compiler is a program that converts source programs into machine language.
• Fourth Generation Programming Languages (4GL) are commonly used in the development of business applications, and are distinguished by their use of “natural language” commands, making them self-documenting.
• 2 popular programming languages
  o **C++** (pronounced "see plus plus") is a general-purpose programming language with high-level and low-level capabilities. It is a statically typed, free-form, multi-paradigm, usually compiled language supporting procedural programming, data abstraction, object-oriented programming, and generic programming.
  o **Java** is a programming language originally developed by Sun Microsystems and released in 1995. Java applications are typically compiled to bytecode, although compilation to native machine code is also possible. At runtime, bytecode is usually either interpreted or compiled to native code for execution, although direct hardware execution of bytecode by a Java processor is also possible.
    ▪ Java derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. **JavaScript**, a scripting language, shares a similar name and has similar syntax, but is not directly related to Java.

• **HTML** (HyperText Markup Language) and **XML** (Extensible Markup Language) are specialized programming languages used to create websites.

• **eXtensible Business Reporting Language (XBRL)** is an open, market driven computer language that allows for the free electronic exchange of business and financial data. Instead of treating financial information as a block of text (e.g., standard Internet page or Word document), it provides a computer-readable identifying tag for each individual item of data. For example, “net income” has its own unique tag and a computer could immediately generate a comparison of net income for multiple companies or periods. XBRL eliminates the costly process of manual data comparison as computers can select, analyze, store, and exchange data in XBRL documents. Another benefit to XBRL is that it reduces the chance of errors when generating reports.
  o XBRL can handle data in different languages and accounting standards.
  o XBRL is built upon XML (Extensible Mark-up Language).
  o The SEC mandated that all public companies file financial statements in XBRL.
  o Her Majesty's Revenue and Customs (HMRC), the department of the British Government responsible for the collection of taxes, mandated all corporations' tax submissions use iXBRL ("inline" XBRL).

**Data Structure**
The term **binary** refers to the fact that the switches have only two possible positions. Binary computers can only think in terms of **bits** (binary digits) of information that are on or off ("1" or "0"). A series of 8 consecutive bits will produce a **byte** of information that represents a unit of human thought such as a letter, number, or other character. The manner in which data is described includes the following terms:
• **Bit** – A single switch in a computer that is either in the on (1) or off (0) position
• **Byte** – A group of 8 bits representing a character.
• **Character** – A letter, number, punctuation mark, or special character.
• **Alphanumeric** – A character that is either a letter or number.
• **Field** – A group of related characters representing a unit of information (such as a phone number or a city name).
• **Record** – A collection of related information treated as a unit. Separate fields within the record are used for processing the information (such as the name, address, and telephone number of one employee).
  o Primary key – The field in a record that can be used to uniquely identify that record (such as the social security number field for an employee). It must be a field that has a value for every record, and is never the same in two different records (a name would not be a good idea as a primary key, since two people might have the same name).
  o Secondary key – A key that might be able to uniquely locate a record when the primary key is unknown (the employee name, in this example, typically would to find a unique record, but isn't guaranteed to do so as the social security number would be).
• **File** – A group of logically related records (such as the contact info for all the employees).
  o Master file – A permanent source that is used as an ongoing reference and that is periodically updated.
  o Detail file – A file listing a group of transactions which may be used to update a master file. This is also frequently called a transaction file.
• **Database** – A stored collection of related data needed by organizations and individuals to meet their information processing and retrieval requirements (such as a payroll database that might have a file for contact info, a file with rate and withholding information, a file indicating hours worked, etc.).
• **Table** - A set of data elements (values) that is organized using a model of vertical columns (which are identified by their name) and horizontal rows. A table has a specified number of columns, but can have any number of rows. Users making database queries (a common audit technique) often need to combine several tables to get the desired information.
• **Data definition file** – A file that describes the logical structure of a database, including the titles and descriptions of the fields stored in each file and the relationships that exist between the data in the different files (for instance, indicating that the employee ID field in the file of hours worked is linked to one specific record in the contact info file which will have that same employee ID field). The data definition file should be included along with all the other files in the database to allow programs to read and understand all the files in the database.

A database management system (DBMS) is a software system that controls the organization, storage and retrieval of data in a database. The DBMS consists of a program and accompanying database that is used to keep track of information in an organized and efficient manner.

The program and database should be independent of one another, so that the database could be accessed by another user without needing the same program. One reason for this is that the database may be stored on a single file server (such as a website), while different users can use the database from their own client computer. Another reason is that the company may want to limit the access of some users to specific parts of the database, or allow some users to only read and not change data. This also might be done with a program that sets different access levels based on passwords, connection method, or other means. Yet a third reason is that the program maintenance can be performed more readily.

Data normalization is the process of organizing a database for minimum redundancy. While the details of DBMS design are too complicated to expect exam testing, it should be noted that an important goal of the DBMS should be to minimize the repetition and redundancy in the database, both to enhance efficiency and remove the danger of information being stored inconsistently in different places.
For example, the name and address of each employee is stored only in the contact info file and not included with the rate file or the hours worked file (the last two include the employee ID, but not the name). This way, only one file is updated when an employee changes his or her name or address. It is easy to generate reports (such as paychecks) by taking information from the three different files and grouping them together with the necessary computations.

Lecture 7.12

CLASS QUESTIONS

Please see the Class Questions and Class Solutions for this Lecture at the end of this Section.

Lecture 7.13

CLASS QUESTIONS

Please see the Class Questions and Class Solutions for this Lecture at the end of this Section.
CLASS QUESTIONS

Work through the below Class Questions while following along with the respective lectures. Once this is complete, you can begin independently practicing what you've learned by quizzing yourself on this course section in your Interactive Practice Questions (IPQ), which can be found in your online Student Dashboard. Your IPQ simulates the computer-based testing experience, and will also help you understand how concepts are applied to the exam. Each question includes answer explanations from expert CPAs that will help you determine why you answered a question correctly or incorrectly. This is key to your success on the CPA Exam.

Lecture 7.03

1. Which of the following systems assists with nonroutine decisions, serves strategic levels of the organization, and helps answer questions regarding what a company's competitors are doing, as well as identifies new acquisitions that would protect the company from cyclical business swings?
   a. Executive support system
   b. Decision support system
   c. Transaction processing system
   d. Management information system

2. Optimizing functionality and process costs, management of change, productivity, and compliance with policies and procedures are goals related to which category described by COBIT 5?
   a. Customer.
   b. Internal.
   c. Financial.
   d. Learning and growth.

3. During a post implementation review of an accounting information system (AIS), a CPA learned that an AIS with few customized features had been budgeted and scheduled to be installed over nine months for $3 million (including hardware, software, and consulting fees). An in-house programmer was assigned as the project manager and had difficulty keeping the project on schedule. The implementation took 18 months, and actual costs were 30% over budget. Many features were added to the system on an ad-hoc basis, with the project manager's authorization. The end-users are very satisfied with the new system. The steering committee, however, is dissatisfied about the scope creep and would like a recommendation to consider before approving initiation of another large project. Based on those findings, the CPA should recommend implementing a
   a. Change control system.
   b. Contract management system.
   c. Budgeting system.
   d. Project timekeeping system.
4. According to COBIT 5, covering the enterprise from end-to-end means that COBIT 5:
   a. Applies to all of the different systems within the enterprise by the various components that process information.
   b. Involves a process for developing systems of governance from the time the enterprise is created and continuing throughout its life.
   c. Establishes systems for governance of IT, accounting, and enterprise governance.
   d. Integrates governance of enterprise IT with enterprise governance and management.

Lecture 7.05
5. Which of the following characteristics distinguish electronic data interchange (EDI) from other forms of electronic commerce?
   a. The cost of sending EDI transactions using a value-added network (VAN) is less than the cost of using the Internet.
   b. Software maintenance contracts are unnecessary because translation software for EDI transactions need not be updated.
   c. EDI commerce is ordinarily conducted without establishing legally binding contracts between trading partners.
   d. EDI transactions are formatted using strict standards that have been agreed to worldwide.

6. Which of the following allows customers to pay for goods or services from a website while maintaining financial privacy?
   a. Credit card
   b. Cryptocurrency
   c. Electronic check
   d. Sight draft

Lecture 7.07
7. Which of the following describes the primary purpose of a disaster recovery plan?
   a. To document how data will be backed up to expedite recovery.
   b. To document the location of off-site replacement facilities.
   c. To test how well prepared the company is to recover data.
   d. To specify the steps required to resume operations.

8. Which of the following terms refers to a site that has been identified and maintained by the organization as a data processing disaster recovery site but has not been stocked with equipment.
   a. Hot
   b. Cold
   c. Warm
   d. Flying start
9. When a client's accounts payable computer system was relocated, the administrator provided support through a dial-up connection to a server. Subsequently, the administrator left the company. No changes were made to the account payable system at that time. Which of the following situations represents the greatest security risk?

   a. User passwords are not required to be in alpha-numeric format.
   b. Management procedures for user accounts are not documented.
   c. User accounts are not removed upon termination of employees.
   d. Security logs are not periodically reviewed for violations.

10. General controls in an information system include each of the following, except

   a. Information technology infrastructure.
   b. Security management.
   c. Software acquisition.
   d. Logic tests.

11. A company began issuing handheld devices to key executives. Each of the following factors is a reason for requiring changes to the security policy, except

   a. Storage of sensitive data.
   b. Portability of the device.
   c. Vulnerability of the device.
   d. Convenience of the device.

12. Which of the following classifications of security controls includes smoke detectors, generators, security guards, and ID badge?

   a. Technical.
   b. Physical.
   c. Administrative.
   d. Logical.

13. An entity has the following invoices in a batch:

<table>
<thead>
<tr>
<th>Invoice #</th>
<th>Product</th>
<th>Quantity</th>
<th>Unit price</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>F10</td>
<td>150</td>
<td>$5.00</td>
</tr>
<tr>
<td>202</td>
<td>G15</td>
<td>200</td>
<td>$10.00</td>
</tr>
<tr>
<td>203</td>
<td>H20</td>
<td>250</td>
<td>$25.00</td>
</tr>
<tr>
<td>204</td>
<td>K35</td>
<td>300</td>
<td>$30.00</td>
</tr>
</tbody>
</table>

   Which of the following most likely represents a hash total?

   a. FGHK80
   b. 4
   c. 204
   d. 810
14. A retail store uses batch processing to process sales transactions. The store has batch control total and other control checks embedded in the information processing system of the sales subsystem. While comparing reports, an employee notices that information sent to the subsystem was not fully processed. Which of the following types of controls is being exercised by the employee?
   a. Preventive.
   b. Corrective.
   c. Detective.
   d. Input.

15. Which of the following controls is a processing control/Input control designed to ensure the reliability and accuracy of data processing?

<table>
<thead>
<tr>
<th>Limit test</th>
<th>Validity check test</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>b. No</td>
<td>No</td>
</tr>
<tr>
<td>c. No</td>
<td>Yes</td>
</tr>
<tr>
<td>d. Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

16. Passenger 1 and passenger 2 are booking separately on an airline website for the last available seat on a flight. Passenger 1 presses the enter key a few seconds before passenger 2, thus locking out passenger 2 and obtaining the last seat. This locking is a form of which of the following types of control?
   a. Concurrent update control.
   b. Compensating control.
   c. Data entry control.
   d. Operational data control.

17. A systems engineer is developing the input routines for a payroll system. Which of the following methods validates the proper entry of hours worked for each employee?
   a. Check digit.
   b. Capacity check.
   c. Sequence check.
   d. Reasonableness check.

18. An auditor most likely would test for the presence of unauthorized computer program changes by running a
   a. Program with test data.
   b. Check digit verification program.
   c. Source code comparison program.
   d. Program that computes control totals.
19. Processing data through the use of simulated files provides an auditor with information about the operating effectiveness of control policies and procedures. One of the techniques involved in this approach makes use of
   a. Controlled reprocessing.
   b. An integrated test facility.
   c. Input validation.
   d. Program code checking.

Lecture 7.12
20. An entity doing business on the Internet most likely could use any of the following methods to prevent unauthorized intruders from accessing proprietary information except
   a. Password management
   b. Data encryption
   c. Digital certificates
   d. Batch processing

21. Cloud computing can best be defined as a model that
   a. Streamlines business processes onto a well-secured and highly available in-house e-commerce platform to optimize customers' online experience.
   b. Is designed for rapid application deployment by making several virtual servers run on one physical host.
   c. Allows users to access network resources from remote locations through a virtual private network.
   d. Allows organizations to use the Internet to access and use services and applications that run on remote third-party technology infrastructure.

22. In an effort to recognize improvement opportunities, a company is reviewing its in-house systems. The best reason for the company to consider switching to cloud computing as a solution is that it
   a. Is the best way to secure sensitive corporate information.
   b. Is accessible only from within the company on its Intranet.
   c. Usually has lower upfront costs for equipment and maintenance.
   d. Provides better program modification options.

23. Which of the following is the primary advantage of using a value-added network (VAN)?
   a. It provides confidentiality for data transmitted over the Internet.
   b. It provides increased security for data transmissions.
   c. It is more cost effective for the company than transmitting data over the Internet.
   d. It enables the company to obtain trend information on data transmissions.
CLASS SOLUTIONS

1. (a) An executive support system is designed to support the work of executives, including making nonroutine decisions, answering questions about competitors, and identifying new acquisitions. Answer (b) is incorrect because a decision support system provides users with easy access to decision models and data. Answer (c) is incorrect because a transaction processing system is a set of procedures to be applied to the processing of a particular type of transaction. Answer (d) is incorrect because a management information system is an organized assembly of resources and procedures required to collect, process, and distribute data.

2. (b) Internal goals include optimizing functionality of business functions, optimizing process costs, management of change, productivity, and compliance with policies. Answer (a) is incorrect because customer goals include a culture of customer service, continuity and availability of service, ability to respond to change, information based strategic planning, and optimizing the cost of delivery. Answer (c) is incorrect because financial goals include value of business investments, competitive products and services, safeguarding of assets, compliance, and financial transparency. Answer (d) is incorrect because learning and growth goals include having well-trained and motivated personnel and a culture of innovation.

3. (a) A change control process is designed to minimize adverse effects resulting from changes. Change requests are made and analyzed. Decisions about making a requested change are made. If approved, the requested change is planned and implemented. The change is monitored to be sure it is implemented properly and also that the change is having the intended effects. Scope creep refers to incremental changes or continuous growth in a project's scope; this can occur when the scope of a project is not properly defined, documented, or controlled. (This topic also is discussed in the Corporate Governance section.) Answer (b) is incorrect because a contract management system generally is used to manage the contracts and the contract documents of independent contractors and suppliers; it is unlikely to highlight or prevent scope creep. Answer (c) is incorrect because a budget system generally has a role to play in project management, but is unlikely to highlight or prevent scope creep. Answer (d) is incorrect because a project timekeeping system may have a role to play in project management, but is unlikely to highlight or prevent scope creep.

4. (d) According to COBIT 5, covering the enterprise from end-to-end includes the seamless integration of the system for governing IT with the system for governing the enterprise and applying the systems for the governance and management of IT applying to all components of the enterprise that are involved in the processing of information, internally or externally. Answer (a) is incorrect because as a result, the components of the enterprise that process information would not use different systems. Answer (b) is incorrect because it relates to all aspects of the enterprise, not its duration. Answer (c) is incorrect because accounting is a component involved in the processing of information and would not be subject to a separate system of governance or management.

5. (d) Since electronic data interchange requires computers to communicate with one another, it requires strict standards that have been agreed to worldwide, translation software installed on those computers involved, and encryption to prevent unauthorized access. Answer (a) is incorrect because the cost would not be lower than the Internet, since the cost of using the Internet is largely limited to the cost of access, but the Internet would not provide a reasonable level of security. Answer (b) is incorrect because translation software needs to be updated regularly, which is often facilitated with a software maintenance contract. Answer (c) is incorrect because entities
will use the same types of arrangements, including legally binding contracts, when employing EDI, as used in other systems.

6. (b) The use of cryptocurrency (such as Bitcoin) allows a customer to pay for goods or services from a website while maintaining financial privacy. The cryptocurrency address is tracked, rather than a name. Cryptocurrency is designed to allow payments through an intermediary such that the transmission of sensitive credit or bank account information is not required. (a) The use of a credit card does not allow customers to pay for goods from a website while maintaining financial privacy. Using a credit card to pay for purchases from a website requires the purchaser to enter the credit card number, expiration date and, usually, a security code. (c) An electronic check is a type of electronic funds transfer that is essentially an electronic version of a paper check; it requires the drawer to provide the routing and account numbers. (d) A sight draft is similar to a check. The process of paying with a sight draft is very similar to paying with a check and requires the drawer of the draft to provide routing and account numbers.

7. (d) A disaster recovery plan outlines procedures to follow in the event of a disaster. Answer (a) is incorrect because while documentation of data backup procedures may be included in the plan, it is not the primary purpose. Answer (b) is incorrect because while documentation of the off-site replacement facility locations may be included in the plan, it is not the primary purpose. Answer (c) is incorrect because while testing the plan is prudent, it is not the primary purpose of the plan.

8. (b) A cold site has available space for operations but will require setup of computers and loading of data before operations can begin at that site and can be used as a data processing recovery center in the case of a data processing disaster. Answer (a) is incorrect because a hot site can also be used as a data processing recovery center in the case of a disaster, but it is ready to go with computers set up and software loaded. Answer (c) is incorrect because there is no term such as a warm site to describe a data processing recovery center. Answer (d) is incorrect because there is no term such as a flying start site to describe a data processing recovery center.

9. (c) If user accounts are not removed upon termination of employees, those employees would continue to have access to computer programs and data, creating a security risk. Answer (a) is incorrect because not requiring passwords to be an alpha-numeric format does not create an additional security risk as long as passwords are constructed to make them difficult to figure out. Answer (b) is incorrect because the documentation of security procedures does not make them more or less effective. It is their execution that is significant. Answer (d) is incorrect because although a practice of not reviewing security logs for violations may allow violations to recur, it is not as significant a security risk as allowing terminated employees to have access.

10. (d) Logic tests are application controls. They depend on specifics found at the application level. Information technology infrastructure, security management, and software acquisition procedures are applicable to the entire computer system, not a particular application. Answer (a) is incorrect because information technology infrastructure is applicable to the entire computer system, not a particular application. Answer (b) is incorrect because security management is applicable to the entire computer system, not a particular application. Answer (c) is incorrect because software acquisition procedures are applicable to the entire computer system, not a particular application.

11. (d) Storage of sensitive data, portability of the device, and vulnerability of the device are all security considerations which merit changes to the security policy. Convenience is not. The question asks for the exception. Answer (a) is incorrect because storage of sensitive data merits changes to the security policy. Answer (b) is incorrect because portability of a device merits
changes to the security policy. Answer (c) is incorrect because vulnerability of a device merits changes to the security policy.

12. (b) Smoke detectors, generators, security guards, and ID badges are all forms of physical security, because they protect assets from physical damage or intrusion. Answer (a) is incorrect because technical controls are performed or managed by a computer, such as a firewall. Answer (c) is incorrect because administrative controls involve the exercise of authority by people. Answer (d) is incorrect because logical controls employ instructions on what is logical in a given situation; for instance, a logical access control would not allow even a high-ranking official stationed on the east coast with no travel plans to access a west coast facility.

13. (d) A hash total is a total of values where the total is not a meaningful financial amount but it can be used to verify that all items in that field of a batch have been entered correctly. The total of the invoice numbers, for example, is 810, which indicates that it is likely all of the invoice numbers were entered correctly. Answer (a) is incorrect because FGHK80 is not a total but rather an accumulation of the letters from the product numbers and the total of the product numbers. Answer (b) is incorrect because 4 is the number of invoices being entered, which is a meaningful total, not a hash total. Answer (c) is incorrect because 204 is the number of the last invoice and is not a total.

14. (c) Detective controls detect error and fraud that has occurred already. Answer (a) is incorrect because preventive controls ensure mistakes are not made; a batch control total is determined after sales have been made for a period of time—not soon enough to prevent errors and fraud. Answer (b) is incorrect because corrective controls permit users to resolve detected errors and fraud. Answer (d) is incorrect because Input controls operate at the time of input, not when the information has been incorporated into a batch.

15. (a) A limit check is used to determine that data entered falls within acceptable limits, indicating a potential error when it does not. A validity check test compares certain data to acceptable values, indicating a potential error when there is not a match. Both are designed to ensure the reliability and accuracy of data processing.

16. (a) A concurrent update control, also referred to as a concurrency control, is one that updates data on a real-time basis and is particularly useful when multiple users have access to limited resources. This control allows users to access the resources, such as seats on an airline flight, as long as there are resources available, usually on a first-come, first-served basis, but will lock out all remaining users once capacity has been filled. Answer (b) is incorrect because a compensating control is a data security measure that compensates for some other security measure that is deemed too difficult or impractical to implement. Answer (c) is incorrect because a data-entry control validates data. Answer (d) is incorrect because operational data control is not a commonly used term.

17. (d) A reasonableness check would be the best input validation technique to use in this situation, because based on the entity's policies for using full-time and part-time workers and regarding overtime, the number of hours entered for any given employee should fall within a relatively narrow range. Answer (a) is incorrect because a check digit might be used to determine if all employee I.D. numbers were appropriate, but would not provide meaningful information about hours. Answer (b) is incorrect because a capacity check is a term commonly used in warehouse management and cellular networks and is generally a procedure used for physical storage or network operations, not data storage. Answer (c) is incorrect because a sequence check is used to
validate that a correct expected sequence of numbers in an entry or that all records in a sequence, such as pre-numbered payroll checks, are accounted for.

18. (c) To detect unauthorized program changes, an auditor would need to examine the source code or program documentation to determine whether such changes were made. Answer (a) is incorrect as test data is data developed and entered to test a program's operation. Answer (b) is incorrect as a check digit is a digit added to an identification number to verify that other digits in the number are entered correctly; verifying such a digit does not confirm that no unauthorized program changes were made. Answer (d) is incorrect as a control total is designed to test a batch of data, not to detect unauthorized program changes.

19. (b) Under the integrated test facility approach, fictitious and real transactions are processed, using the client's system. The auditor then reviews the client system's processing of the data to evaluate the effectiveness of its control environment. Controlled reprocessing involves reprocessing client data through the client's programs under the control of the auditor. Input validation and program code checking are application control procedures.

20. (d) Batch processing is simply a system under which transactions are periodically entered into the system in groups, rather than as they occur as in a real-time system. It does not specifically prevent unauthorized intruders from accessing proprietary information. Answer (a) is incorrect because password management provides assurance that only those with a valid password will have access, preventing unauthorized intruders. Answer (b) is incorrect because data encryption prevents unauthorized intruders from being able to understand data that they are not authorized for without obtaining the codes to decrypt the information. Answer (c) is incorrect because digital certificates provide identifying information to determine if a user is authorized to have access.

21. (d) Cloud computing is a model that allows organizations to use the Internet to access and use services and applications that run on remote third-party technology infrastructure, rather than rely on in-house platform solutions. Answer (a) is incorrect because cloud computing is a model that allows organizations to use the Internet to access and use services and applications that run on remote third-party technology infrastructure; it is not inherently secure. Answer (b) is incorrect because virtualization is a model that is designed for rapid application deployment by making several virtual servers run on one physical host. Answer (c) is incorrect because users may access network resources from remote locations through a virtual private network (VPN); a VPN may or may not be incorporated as part of a larger cloud computing strategy.

22. (c) Cloud computing utilizes third-party hardware and software, so it usually has lower upfront costs for equipment and maintenance. Answer (a) is incorrect because cloud computing is generally not the best way to secure sensitive corporate information, as there are security risks to transmitting information over the Internet. Answer (b) is incorrect because cloud computing allows information to be accessed by companies and their clients over the Internet, not via a company intranet. Answer (d) is incorrect because common implementations of cloud computing involve off-the-shelf software that is not developed or modified in-house, with generally limited configuration and program modification options.

23. (b) A value added network links the computer files of different companies, which requires increased security over data transmissions. Answer (a) is incorrect because since it shares files, it does not provide confidentiality. Answer (c) is incorrect because it is probably not as cost effective as transmission of data over the Internet, the cost of which would be generally limited to the cost of Internet access, but it provides a layer of security that transmission over the Internet cannot. Answer (d) is incorrect because it does not necessarily provide trend information.