1. **Chapter 9. Review Question 2 (Page 298)**

   Explain the difference in typical usage between reporting and data-mining tools.

   Reporting tools are used to pull data from data sources, organize that data, and format and display the results. Data mining is used to search for patterns and relationships among data and use the results to make predictions.

2. **Chapter 9. Review Question 8 (Page 298)**

   Summarize five potential problems that can occur when using operational data for data mining.

   - Dirty data: Data collected by an operational system may be correct enough for the purposes of the transaction, but has errors that are consequential in data mining. For example, a gender code that is something other than M or F is impossible to interpret in data mining.
   - Missing values: Data may be missing and as a result, the analysis may be biased.
   - Inconsistent data: Data collected over time may include values for an attribute that has changed (such as area code), making it difficult to use such data meaningfully in a trend analysis.
   - Nonintegrated data: Data may exist in separate, nonintegrated places within the organization and must be integrated before it can be used.
   - Wrong granularity: Data may be too detailed (granularity too fine) or too summarized (granularity too coarse) for the analysis. Detailed data can usually be summarized, but summarized data generally cannot be broken down.
   - Excessive data: There may be too many attributes available resulting in models that fit but are poor predictors. There may be too many data points resulting in the need to employ statistical sampling.

3. **Chapter 9. Applying Your Knowledge 20 (Page 298)**

   Suppose you are a member of the Audubon Society, and the board of the local chapter asks you to help them analyze its member data. The group wants to analyze the demographics of its membership against members' activity, including events attended, classes attended, volunteer activities, and donations. Describe two different reporting applications and one data-mining application that they might develop. Be sure to include a specific description of the goals of each system.

   A variation of the RFM analysis could be performed that could provide rankings of the members based on how recently donations were made, how frequently donations were made, and donation amount. This analysis might suggest the best candidates to target for fund raising activities. An OLAP system would enable members to be easily viewed based on a number of measures and dimensions. This system would enable the board to understand their members by forming groups based on a number of characteristics. The data mining

technique of cluster analysis might be useful in finding groups of similar members based on demographic data and activity and donation records

4. **Chapter 10. Review Question 1 (Page 328)**

List the major functions of the IS department.

Major functions of the ID department include:

- Plan the use of IT to accomplish organization goals and strategy.
- Develop, operate, and maintain the organization's computing infrastructure.
- Develop, operate, and maintain enterprise applications.
- Protect information assets.
- Manage outsourcing relationships.

5. **Chapter 10. Review Question 17 (Page 328)**

Why do companies choose to outsource?

There are three fundamental reasons companies outsource: to save costs, to gain expertise, and to free up management time.

6. **Chapter 10. Review Question 19 (Page 329)**

Compare outsourcing computing infrastructure to outsourcing the cafeteria. How are they the same? How do they differ?

Outsourcing these two areas are similar in that an outside firm takes over the responsibility for providing the entire function using its own employees and managers. A contract carefully specifies the terms of the outsourcing agreement so that both parties know exactly what they are to receive/provide. A major difference between these two areas is the amount of dependency the organization has on the function being outsourced. If the cafeteria arrangement is unsatisfactory, there will be grumbling and complaints but no serious disruption to the business' ability to operate. If there are problems with outsourcing the computing infrastructure, however, the consequences could be extremely serious, possibly inhibiting the firm's ability to operate.

7. **Chapter 10 Applying Your Knowledge 26 (Page 329)**

Suppose you represent an investor group that is acquiring hospitals across the nation and integrating them into a unified system. List five potential problems and risks concerning information systems. How do you think IS-related risks compare to other risks in such an acquisition program?

- Inconsistent use of information systems
- Incompatible hardware infrastructure

- Incompatible enterprise applications
- Use of different standard data definitions
- Uneven data quality

Since one of the drivers of the acquisition program is to link the hospitals' information systems, gain economies of scale, and impose standard operating and reporting procedures on the hospitals, then this goal will be inhibited by incompatibilities between the information systems and technology that is currently in place in the hospitals. The IS-related risks will be high.

8. **Chapter 11. Review Question 4 (Page 363)**

Describe the three major components of a security program.

The first component is senior management, who must establish a security policy and manage the costs and benefits of a security program. The second component is safeguards of various types that provide protection against security threats. The third component is the organization's planned response to the security incidents.

9. **Chapter 11. Review Question 11 (Page 363)**

List the symptoms of spyware and adware.

- The system startup process is slow and/or system performance is sluggish.
- Numerous pop-up ads occur.
- Suspicious changes are made to the browser homepage, system taskbar, or other elements of the interface.
- The hard drive appears to be operating abnormally.

10. **Chapter 11. Review Question 20 (Page 363)**

What constitutes an incident-response plan?

An incident-response plan defines how employees are to respond to security problems, whom they should contact, the reports that should be made, and the steps to take to mitigate loss. Like all plans, incident-response plans should be tested and practice to ensure that they actually work.