As discussed in chapter 6, “Internal Control,” entity-level controls are very broadly focused and often deal with the organizational environment or atmosphere. They are designed to mitigate risks that exist at the organizationwide level, including those that arise internally as well as externally. Entity-level controls also serve to support, complement, and reinforce process-level and transaction-level controls. Additionally, these controls have a pervasive effect on the achievement of many business objectives. Adequately designed and effectively operating entity-level and process-level controls work in unison and serve as an organization's defense against the risks that threaten the achievement of business objectives.

Chapter 13, “Conducting the Assurance Engagement,” goes on to say that while it is important to understand the process-level tasks and controls, it is also important to understand how the entity-level controls may influence the performance of a process. Weaknesses in entity-level controls can allow the circumvention of well-designed controls within a process. For example, if organizationwide policies tend to be informal and inconsistently enforced, then policies specific to the process subject to audit might be undermined and may not be as relevant or as important to understanding the process as they otherwise would be. Similarly, if there is little entity-level commitment to attracting, training, and developing competent employees in key areas requiring decision-making abilities and complex judgments, the testing approach may need to
be altered as less reliance can be placed on controls performed at the process level by individuals unable to perform complex or highly judgmental tasks.

Management typically completes its own assessment or a series of assessments of the organization’s entity-level controls at periodic intervals (for example, annually or quarterly). Such assessments are based on tests conducted around the time of the assessment, as well as other tests that may have been completed in connection with separate assessments (such as assessments of an ERM program, a compliance program, or certain IT general controls). Management considers the results of its entity-level control assessments when evaluating and opining on the organization’s overall system of internal controls.

Likewise, the internal audit function must consider management’s results as well as their own independent assessment of entity-level controls when developing an internal audit plan and designing tests of process-level and transaction-level controls. Since an assessment of an organization’s entity-level controls is made at periodic intervals, it typically will not be necessary to perform an assessment of the effectiveness of entity-level controls on each engagement. However, the internal auditor should consider the results of the entity-level controls assessment when planning individual engagements to ensure the approach to testing process-level and transaction-level controls is effective and efficient.

**IMPORTANCE OF ENTITY-LEVEL CONTROLS**

It should be intuitive that not all controls are created equal. For example, as discussed in chapter 13, a variety of actions make up a process. All may have a role in achieving the final result, but only a few are truly critical to the outcome; that is, their absence would make it difficult to achieve the desired result. These critical actions are referred to as key controls. Similarly, controls at the organizational level may impact the system of internal controls differently than the more tactical controls at the process level or transaction level. Therefore, it is important to understand how such controls, particularly those that operate across the entire organization (that is, entity-level controls), may impact the system of internal controls.

One of the most widely publicized and well known examples of entity-level controls breaking down is Enron Corporation. While Enron was known to have sophisticated controls and risk management capabilities supporting many of its detailed processes, breakdowns in controls at the board and senior management levels contributed to one of the most significant company failures in history. A closer look at what went wrong at Enron, as well as with some other highly publicized financial failures, can provide a glimpse into the importance of strong entity-level controls.

**Exercise 1:** Research Enron Corporation (U.S.A.), WorldCom (U.S.A.), Wells Fargo (U.S.A.), Volkswagen (Germany), and Barings Bank (England). Be prepared to answer the following questions:

- What were the primary causes for each of these failures?
- Which of those causes appear to represent entity-level control breakdowns?
- What actions by the board or management may have prevented these breakdowns from occurring?

After answering the questions in the exercise above, it should be clear why it is so important for organizations to establish a strong entity-level control environment.
HISTORICAL AND CURRENT PERSPECTIVES 
ON ENTITY-LEVEL CONTROLS

Most types of entity-level controls have been in existence for many years. Many such controls are intuitive and would be implemented by organizations whether required by regulations or not (for example, establishing governance bodies and implementing a code of ethics). Others have become commonplace in reaction to frauds or other scandals (for example, whistleblower hotlines). Regardless of the reasons behind establishing and implementing such controls, until the creation of control models there was not a recognition that certain types of controls have a profound influence on the effectiveness of all other controls and, as such, the effectiveness of the overall system of internal controls.

As discussed in chapter 6, all controls are designed to mitigate risk either at the enterprise level or at the operational level within an organization. The original COSO Internal Control – Integrated Framework, issued in 1992, used the terms “entity level” and “activity level” (“business process” in the 2013 revised Framework) respectively to describe these controls. While this framework established definitions and context for controls at the entity level, there was little practical guidance developed to assist organizations in conducting a comprehensive evaluation of the design adequacy or operating effectiveness of such controls. Generally, there was little guidance developed from other sources over the next 10 to 12 years.

In 2006, COSO published the guide Internal Control over Financial Reporting – Guidance for Smaller Public Companies, in which the terminology for these concepts was changed to “entitywide” and “process level” respectively. This publication defined entitywide controls as controls that occur at the entity level of a company and have a pervasive influence across the organization.1 Entitywide controls may exist in any of the five components of internal control. Other important points this COSO guidance included were:

- Management considers entitywide controls that are pervasive across the company when evaluating whether controls are sufficient to address identified risks. Management then makes informed decisions as to which processes need additional controls.
- There are 20 basic principles representing the fundamental concepts that are important in achieving effective internal control. It should be noted that, while this former COSO guidance tended to focus on internal control over financial reporting, these principles apply to the other control categories (operational efficiency and effectiveness and compliance with applicable laws and regulations) as well.

In 2011, COSO began a revision of the 1992 Framework, which, after several exposures and revisions, was issued in 2013. One of the major changes in the revised Framework was the inclusion of 17 basic principles representing concepts considered critical to implement the control elements. These 17 principles were derived from the 20 principles found in the 2006 Internal Control over Financial Reporting – Guidance for Smaller Public Companies.

Exercise 2: Go to COSO’s website (www.coso.org) and review the Executive Summary of the 2013 revised COSO’s Internal Control – Integrated Framework, which is available at no cost.

- Review the 17 principles.
- Consider, and be prepared to discuss, why each of these 17 principles is important when evaluating the effectiveness of entitywide—that is, entity-level—controls.
The increase in large-scale financial failures, scandals, and bankruptcies since 2002 was the catalyst for several countries to pass or expand regulations to help restore investor confidence. These regulations focused in part on improving the reliability of internal control over financial reporting. Many required affected organizations to adopt an internal control framework, and, as such, provided heightened focus on the importance of entity-level controls. For example, in the United States, both the U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) specifically mentioned the importance of conducting control evaluations at the entity level. The PCAOB’s Auditing Standard No. 5 (AS5) refers to such controls as entity-level controls. AS5 stated that “Some entity-level controls:

- …such as certain control environment controls, have an important, but indirect, effect on the likelihood that a misstatement will be detected or prevented...might affect the other controls...and the nature, timing, and extent of [testing].”
- …monitor the effectiveness of other controls...identify possible breakdowns in lower-level controls, but not at a level of precision...address the risk of misstatement...might allow the auditor to reduce testing of other controls.”
- …might be designed to operate at a level of precision that would adequately prevent or detect...misstatements.... If [it] sufficiently addresses the assessed risk of misstatement...need not test additional controls relating to that risk.”

AS5 goes on to state that “Entity-level controls include:

- Controls related to the control environment;
- Controls over management override;
- The company’s risk assessment process;
- Centralized processing and controls, including shared service environments;
- Controls to monitor results of operations;
- Controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs;
- Controls over the period-end financial reporting process; and
- Policies that address significant business control and risk management practices.”

However, application-oriented guidance continued to be sparse and, therefore, these evaluations tended to follow a checklist approach and were not linked directly with lower-level control evaluations. As a result, the benefits of effective entity-level controls were not fully realized in the first few years after issuance of these regulations.

Exercise 3: Research internal control regulations from your home country and two other countries. Determine which of these regulations:

- Specifically mention entity-level controls and their role in the system of internal control.
- Provide a definition of entity-level controls.
- Provide guidance regarding how to evaluate such controls.
DEFINITIONS OF DIFFERENT LEVELS OF CONTROLS

It should be clear that controls operate at different levels in the organization. Since there are no widely recognized definitions related to these control levels, the authors developed definitions that capture concepts that are applicable to any system of internal controls and are consistent with what has been taught throughout the textbook. The definitions are:

- **Entity-Level Controls:** Controls that operate pervasively across and throughout the organization to mitigate risks threatening the organization as a whole and to provide assurance that organizational objectives are achieved. Examples of entity-level controls include, but are not limited to:
  - Code of ethics.
  - Risk management policies and procedures.
  - Fraud prevention and detection program.
  - Human resources policies and procedures.
  - Management’s control deficiency escalation process.
  - Variance analyses.
  - IT general controls.

- **Governance Controls:** Entity-level controls established by the board and senior management (for example, the CEOs) to:
  1. Establish the control culture and expectations of the organization. Examples include:
     - Audit committee oversight of internal controls.
     - Senior management’s attitude toward financial reporting.
     - The board and senior management’s risk appetite.
  2. Prescribe guidance that pervasively supports strategic objectives and affects the overall system of internal controls. Examples include:
     - Code of Ethics and compliance policies.
     - Organization-level risk assessment.
     - IT policies.
     - Monitoring business units’ performance.

- **Management-Oversight Controls:** Entity-level controls established by management (for example, business unit and line management) to mitigate risks threatening the business unit and to provide assurance that business unit objectives are achieved. These controls are generally consistent in nature among business units but may vary in their execution from one business unit to another. Examples include:
  - Monthly analyses of budget versus actual results.
  - IT physical and environmental controls.
● Business unit-level risk committees and activities.
● Certain period-end controls.

**Process-Level Controls:** *Non-entity-level* controls established by process owners to mitigate the risks threatening the process and to provide assurance that process objectives are achieved. These controls are generally consistent in nature across processes but may vary in their execution from one process to another. Examples include:

- Reconciliations of key accounts.
- Physical verifications of assets (such as inventory counts).
- Process employee supervision and performance evaluations.
- Process-level risk assessments.
- Monitoring/oversight of specific transactions.

**Transaction-Level Controls:** *Non-entity-level* controls implemented to mitigate the risks threatening the execution of individual transactions and to provide assurance that transaction objectives are achieved. These controls are generally consistent in nature among different types of transactions but may vary in their execution from one transaction type to another. Examples include:

- Authorizations.
- Documentation (such as source documents).
- Segregation of duties.
- IT application controls (input, processing, output).

As defined above, entity-level controls consist of two different types of controls—governance controls and management-oversight controls. Some current literature refers to these types of controls as indirect and direct controls, and while those characteristics typically are consistent with the nature of governance and management-oversight controls, those descriptions do not encompass the source of such controls and, as such, the authors prefer the definitions provided above. Process-level and transaction-level controls are not entity-level controls, but rather operate at a lower level within the organization.
Exhibit CS 1-1, which is taken from exhibit 4-3 in chapter 4, “Risk Management,” depicts the top-down approach to evaluating a system of internal controls.

The key points to be understood from this illustration are:

- Every organization faces a variety of risks, depending on its business objectives. Some of these business objectives may describe the desired state of operation brought about by a good system of internal controls. For example, controls-focused business objectives may be stated in the following terms:
To establish and promote a culture of integrity, compliance, competence, and accountability; doing the right thing.

To reduce entity-level risks to acceptable levels.

Risks that impact an organization’s ability to achieve its business objectives are shown in exhibit CS 1-1 as colored balls of varying sizes. This reflects the fact that some risks will have greater impact than others. Additionally, some risks are clustered together, representing the fact that while the risks individually may not be serious, when related risks are aggregated, they can become more serious. Initially, these risks are uncontrolled, or are in their inherent, or gross, risk state. Examples of risks affecting controls-focused business objectives include:

- Inadequate understanding of management’s expectations, including risk appetite.
- Noncompliance with laws and regulations.
- Employees conducting themselves in an unethical manner.
- Incentives that promote the wrong behavior.

The system of internal controls is depicted as a funnel to illustrate the “filtering” of key risks that occurs at varying levels of that system. For example, the largest risks should be mitigated by the entity-level controls at the top of the funnel. Examples of such risks can be seen under the definitions above. Those that pass through the entity-level filters are next subjected to the process-level and transaction-level controls. Recall that controls may be considered key or secondary, depending on whether they reduce the risk associated with critical objectives. Distinguishing between key controls and secondary controls also applies to entity-level controls. Additionally, in some cases, management may deploy additional mitigating and compensating controls to further limit the impact of the risks.

If the system of internal controls is designed adequately and operates effectively, those risks that make it all the way through the funnel should be acceptable to the organization. Stated another way, the residual, or net, risk does not exceed the organization’s risk appetite.

The exhibit shown above should reinforce two important concepts.

1. It is important to apply a top-down approach. That is, the effectiveness of entity-level controls must be evaluated first to understand which risks have passed through the filters down to the process-level and transaction-level controls. Failure to assess entity-level controls first will likely result in over-testing of controls at the process and transaction levels. This is an ineffective and costly way of evaluating the overall system of internal controls.

2. The approach to conducting an assessment of entity-level controls is the same as discussed in chapter 13. That is, one must first understand the organization’s objectives before identifying and assessing its risks. Only after those steps are completed can controls be tested and assessed. This objectives-risks-controls-assessment approach applies to any type of assurance activity, including an assessment of entity-level controls.

The relationship between objectives, risks, and controls is illustrated in exhibit CS 1-2.
CASE STUDIES

Case Study 1: Auditing Entity-Level Controls

EXHIBIT CS 1-2
ENTITY-LEVEL CONTROLS FRAMEWORK

Entity-Level Objectives

Entity-Level Risks

Entity-Level Controls

Objective 1

Objective 2

Risk 1

Risk 2

Risk 3

Risk 4

Risk 5

Control 1

Control 2

Control 3

Control 4

Control 5

Control 6

Control 7

Entity-Level Controls Assessment
### EXHIBIT CS 1-3
**IMPACT OF ENTITY-LEVEL CONTROLS ON LEVEL OF TESTING**

<table>
<thead>
<tr>
<th>Governance Controls Assessment</th>
<th>Management-Oversight Controls Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HIGH</strong></td>
<td>Moderate testing of process-level controls and limited testing of transaction-level controls.</td>
</tr>
<tr>
<td>All appropriate governance controls appear to be in place and operating effectively.</td>
<td><strong>HIGH</strong></td>
</tr>
<tr>
<td><strong>MEDIUM</strong></td>
<td>Moderate testing of process-level controls and moderate testing of transaction-level controls.</td>
</tr>
<tr>
<td>Some governance control gaps, but they are not pervasive or significant.</td>
<td><strong>MEDIUM</strong></td>
</tr>
<tr>
<td><strong>LOW</strong></td>
<td>Moderate testing of process-level controls and moderate testing of transaction-level controls.</td>
</tr>
<tr>
<td>Fatal situation; there are likely to be multiple material weaknesses, rendering reliance on any controls risky at best.</td>
<td><strong>LOW</strong></td>
</tr>
</tbody>
</table>

**Governance Controls Assessment**

**HIGH**
- All appropriate governance controls appear to be in place and operating effectively.

**MEDIUM**
- Some governance control gaps, but they are not pervasive or significant.

**LOW**
- Several pervasive and/or significant governance control gaps.

**Management-Oversight Controls Assessment**

**HIGH**
- Several oversight controls exist.

**MEDIUM**
- A few oversight controls exist.

**LOW**
- No oversight controls exist.
CASE STUDIES

Case Study 1: Auditing Entity-Level Controls

CASES

Case 1

Applying the concepts from the top-down approach discussed and illustrated above, the internal auditor can use the framework that is shown in exhibit CS 1-3 for determining the nature and extent of testing of process-level and transaction-level controls.

ENTITY-LEVEL CONTROLS AND COSO’S INTERNAL CONTROL – INTEGRATED FRAMEWORK

Based on the definition of entity-level controls, it might be assumed that such controls primarily occur in the Control Environment component in COSO’s Internal Control – Integrated Framework. However, while entity-level controls are very prevalent in that component of the framework, they also occur to some extent throughout the framework. Exhibit CS 1-4 outlines the extent to which entity-level controls occur within each of the components and shows examples of specific entity-level controls.

<table>
<thead>
<tr>
<th>COSO Component</th>
<th>Extent of Entity-Level Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>Extensive</td>
</tr>
<tr>
<td></td>
<td>• Organizationwide code of conduct</td>
</tr>
<tr>
<td></td>
<td>• Whistleblower program</td>
</tr>
<tr>
<td></td>
<td>• Qualified, independent governing board</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive job descriptions</td>
</tr>
<tr>
<td></td>
<td>• Delegation of authority</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Extensive</td>
</tr>
<tr>
<td></td>
<td>• Organizationwide risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Defined organizational risk appetite</td>
</tr>
<tr>
<td></td>
<td>• Risk assessment embedded in strategic planning process</td>
</tr>
<tr>
<td></td>
<td>• Fraud prevention and detection program</td>
</tr>
<tr>
<td>Control Activities</td>
<td>Limited</td>
</tr>
<tr>
<td></td>
<td>• Organizationwide policy protocol</td>
</tr>
<tr>
<td></td>
<td>• IT general controls</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>Limited</td>
</tr>
<tr>
<td></td>
<td>• External and internal benchmarking</td>
</tr>
<tr>
<td></td>
<td>• Employee communication systems</td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>• Robust internal audit function</td>
</tr>
<tr>
<td></td>
<td>• Performance management system</td>
</tr>
<tr>
<td></td>
<td>• Issues escalation process</td>
</tr>
</tbody>
</table>
Exhibit CS 1-4 illustrates the interrelationships between entity-level controls and all aspects of a sound system of internal controls.

**TESTING ENTITY-LEVEL CONTROLS**

Entity-level controls can be classified as “soft” or “hard,” depending on whether they indirectly or directly affect people’s actions. Soft controls typically influence how people think and act but do not directly result in evidence that a risk has been mitigated. Hard controls typically provide more direct evidence that a risk has been mitigated. As a result, the approach to testing entity-level controls will be dependent on the nature of such controls. The following describes testing characteristics for soft and hard controls.

- **Soft Controls** – Tend to be indicative of the culture (more a state of mind and perceptions):
  - Inquiries and surveys are not sufficient by themselves.
  - Need to corroborate the results.
  - Build a body of evidence to support conclusions.

- **Hard Controls** – Traditional audit approaches can be employed, for example:
  - Re-perform a monthly budget to actual analysis.
  - Inspect minutes from board committee meetings.

As discussed in chapter 13, determining a testing approach requires a significant amount of judgment and experience. Developing a testing approach for entity-level controls requires even more judgment due to the different approaches that must be taken for soft and hard controls. The following offers some tips regarding the skills, timing, and documentation necessary to assess entity-level controls.

- **Skills Needed:**
  - Top-down perspective (need to see the forest from the trees).
  - Experience (capacity to sense when things are not right).
  - Credibility (audit evidence supporting the assessment may be less tangible).

- **Timing of Evaluations:**
  - Should drive annual audit planning.
  - Therefore, probably should be done in the fourth quarter.
  - Updated/rolled forward as needed (at least annually).

- **Documentation:**
  - Similar to other risk-based audit documentation.
  - Be sure to cover all five COSO components.
SUMMARY

Entity-level controls exist, to some extent, within every organization. These controls have a pervasive effect on the organization, including how effectively controls at the process and transaction levels will operate. Because entity-level controls are so important, internal auditors must conduct periodic assessments to determine the design adequacy and operating effectiveness of such controls. The following summarizes the key points:

- Entity-level controls are one of two types; governance or management oversight.
- The objectives, risk, control, and assessment approach works when evaluating entity-level controls.
- Robust and effective entity-level controls and a top-down, risk-based internal control assessment approach will result in the need to rely on quantifiably fewer:
  - Process and transaction-level controls.
  - Mitigating and compensating controls.
  - Resources devoted to testing such controls.
- As a result, there is an increase in efficiency and potential reduction in cost to the organization.
- Greater experience and different skillsets are needed to assess entity-level controls.

The following case study provides students with an opportunity to apply the concepts covered in this chapter. The case study activities focus primarily on 1) studying and evaluating entity-level controls and 2) illustrating how control assessment outcomes at the governance and management-oversight levels affect the nature, timing, and extent of testing internal controls at the process and transactions levels.

CASE STUDY

Background Information

SHR Corporation (SHR) is a midsize, publicly traded direct marketer and retailer of outdoor sporting goods based in the United States. Its common stock is listed on the New York Stock Exchange under the symbol “SHR.”

The company prides itself on selling high-quality outdoor sporting goods at competitive prices and providing outstanding customer service. SHR directly markets its merchandise through two major channels—its catalogs and its website—to customers in the United States and nearly 100 other countries. It currently has retail stores and distribution centers in the United States, Canada, and Europe.

SHR Corporation recently purchased MVF Company, a manufacturer of high-quality outdoor sportswear. SHR also purchases merchandise from highly reputable vendors in the United States and several other countries.

SHR Corporation has enjoyed several consecutive years of sustained growth as reflected in the selected financial information, expressed in millions of dollars (US), presented below:
Case Study 1: Auditing Entity-Level Controls

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2016</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Assets</td>
<td>$700.5</td>
<td>$546.5</td>
<td>$491.3</td>
</tr>
<tr>
<td>Sales Revenue</td>
<td>763.5</td>
<td>665.7</td>
<td>589.8</td>
</tr>
<tr>
<td>Operating Income</td>
<td>57.5</td>
<td>45.0</td>
<td>38.9</td>
</tr>
<tr>
<td>Net Income</td>
<td>34.3</td>
<td>29.0</td>
<td>26.0</td>
</tr>
</tbody>
</table>

Senior management is continuing its efforts to grow the company, increase its market share, and enhance shareholder value by:

- Further expanding its direct sales globally.
- Systematically increasing the number of retail stores.
- Selectively acquiring other businesses that are aligned with its core competencies.

Increasing competition over the past several years has motivated management to continuously pursue new and innovative ways to differentiate SHR’s products, streamline the company’s business processes, and take full advantage of advances in IT. Operating efficiency is a critical component of SHR’s competitive pricing strategy.

The risks that concern senior management the most heading into fiscal 2018 include:

- The continuing economic uncertainty further decreases discretionary consumer spending, which in turn will adversely affect the company’s sales and profitability.
- Mounting competition in the industry may make it increasingly difficult to differentiate the company’s high-quality merchandise at prices consumers are willing to pay.
- Deterioration of the company’s brand or its positive image in the marketplace may adversely affect sales and profitability.
- Failure to successfully integrate newly acquired businesses may adversely affect the company’s performance.
- The inability to generate operating efficiencies and leverage IT may adversely affect the company’s profits.
- Placing too much emphasis on operating efficiencies may adversely affect product quality and customer service.

During the first six months of 2018, SHR has experienced slower sales growth and higher operating expenses than anticipated. There is growing concern that forecasted performance targets for the year will not be achieved.

Scenario 1: Ethical Behavior is Good Business

The concept that “ethical behavior is good business” is integral to SHR’s strategy. For example, the company’s 2017 annual report includes this statement: “Sound ethical conduct is a key component of how we do business and continues to contribute significantly to the company’s success.”
An illustrative business objective and associated business risk that reflect the company’s philosophy regarding ethical conduct are expressed as follows:

**Business Objective:** To demonstrate sound ethical conduct in everything we do.

**Business Risk:** Disregard for sound ethical principles, either intentional or unintentional, may cause managers and employees to cut corners, embellish performance results, misuse company resources, or otherwise act in a manner that harms the company and its stakeholders.

Use the business objective and business risk stated above as the basis for answering the following questions. As he or she deems necessary, your instructor will facilitate the formulation of collective answers to certain questions that will serve as uniform starting points for answering subsequent questions.

### Scenario 1 Activities

1. Management asserts that entity-level controls are designed adequately and operating effectively to reduce the above stated risk to an acceptably low level. Identify the key entity-level controls you expect to find in place if management’s assertion is true. Keep in mind that entity-level controls may exist in any of the five COSO components of internal control (control environment, risk assessment, controls, information and communication, and monitoring). [Note: Students are encouraged to review exhibit CS 1-4, but answers should be case-specific.]

2. Many elements of the control environment are “soft” in nature. They may, for example, involve senior management behavior that intrinsically leaves little, if any, audit trail. An example of a soft control that you may have included in your answer to question 1 above is expressed as follows:

   Senior management fosters a strong corporate ethical climate by what they say and what they do. They lead by example when faced with tough business decisions involving ethical ramifications.

   a. Identify the audit procedures you would use to determine whether this control exists within SHR Corporation. Be specific.

   b. Assume that this control does in fact exist within SHR Corporation.

      1. Identify the audit procedures you would use to determine whether it is operating effectively. Be specific. Keep in mind that you need to build a sufficient body of appropriate evidence to support a valid conclusion.

      2. Describe the evidence you might find that would indicate operating effectiveness.

3. The PCAOB's Auditing Standards No. 5 indicates that entity-level controls include both 1) controls to monitor other controls and 2) controls to monitor results of operations. Provide an example of each type of monitoring control that would be useful in mitigating the business risk expressed above.
4. Study the scenario presented below about SHR Corporation’s entity-level controls over the company’s ethics program.

SHR Corporation has a reputation of sound ethical conduct. In recent years, however, the company has not had to deal with an economic downturn, the level of new competition it is now facing, or the decreasing profitability it has experienced during the first two quarters of 2018.

Three years ago, the company put in place a comprehensive, written code of conduct (the Code) that is applicable to directors, management, and employees. The Code is posted on the organization’s website and intranet. All new employees receive a copy of the Code when they are hired and participate in orientation training that includes coverage of the Code. Some minor revisions were made to the Code during the first few months after its introduction, but no changes have been made since then.

A whistleblower program that includes an anonymous hotline was put in place last year for employees and third parties to report suspected violations of the Code. The vice president of internal audit and her direct reports monitor the whistleblower hotline and report suspected violations of the Code to appropriate levels of management and/or the audit committee. Calls on the anonymous hotline have been infrequent, with very few suspected Code violations of a significant nature being reported to senior management or the audit committee.

The internal audit function (internal auditing) recently surveyed senior management and the audit committee regarding the company’s ethics program and conducted follow-up interviews with the audit committee chair and selected members of the senior management team. These procedures produced the following information:

- The audit committee’s charter does not include an explicit provision for overseeing senior management’s ethical conduct or monitoring its adherence to prescribed internal control policies and procedures. The audit committee chair is confident, however, that any misconduct on the part of senior management would come to light via the company’s whistleblower program and the committee’s quarterly meetings with the vice president of internal audit.

- The senior management team informally holds each other accountable for complying with the Code.

- Senior management believes that it clearly conveys the importance of ethical conduct and compliance with the Code via emails, webcasts, and town hall meetings.

- Senior management’s assessed level of inherent ethical misconduct risk has remained consistently low over the past three years.

Internal audit separately surveyed a sample of managers and employees regarding the company’s ethics programs and received responses from 75 percent of the survey recipients. This survey produced the following information:

- All company personnel are required to certify in writing on an annual basis that they understand and are in compliance with the Code. Follow-up procedures performed by internal audit indicated that 80 percent of managers and 90 percent of employees submitted the fiscal 2017 certification.
■ 50 percent of the respondents said that they referred to the Code one or more times during 2017.

■ Managers commonly discuss business ethics during employee performance evaluations, but written performance evaluation standards do not include ethical conduct criteria. No formal provisions exist for rewarding personnel who demonstrate sound ethical behavior or for disciplining those who demonstrate unethical behavior.

■ Managers and employees are unenthusiastic about using the anonymous whistleblower hotline, largely because they see no evidence that appropriate actions will be taken to address unethical conduct.

■ Periodic ethics training is encouraged but not required. The company offers no ethics training in-house, other than that provided to new employees.

■ Managers and employees in general believe that senior management is ethical. They also believe, however, that senior management does very little to inform them about the company’s ethical policies. Less than 50 percent of the respondents could recall hearing or reading anything about business ethics from senior management during the first six months of 2018. A smaller percentage was aware of senior management’s “ethics is good business” statement in the 2017 annual report.

■ One manager included a written comment in his survey response indicating a perception that senior management appears to be preoccupied with the lackluster performance results the company is achieving.

a. Identify the strengths and weaknesses in SHR Corporation’s entity-level controls over the company’s ethics program. Be sure to consider both governance and management-oversight controls. Propose specific recommendations to rectify the weaknesses noted. Based on the information provided, formulate an overall conclusion about the effectiveness of SHR’s entity-level controls over its ethics program.

b. Discuss how the entity-level controls relating to the company’s ethics program might affect senior management’s decisions given the nature of the risks the company now faces. Provide some examples.

c. Discuss how the entity-level controls relating to the company’s ethics program might affect managers’ and employees’ behavior at the business process level. Provide some examples.

d. Discuss how SHR’s entity-level controls over the company’s ethics program may impact your subsequent audit of controls over the company’s purchases and accounts payable process. More specifically, discuss how your conclusion would affect your:

1. Professional skepticism.

2. Assessment of process-level inherent risks.

3. Approach to evaluating the design adequacy of process-level controls.

4. Inclination to perform direct tests of transactions in search of indirect evidence to support your conclusion about the design adequacy and operating effectiveness of process-level controls.
5. Assume that internal audit concludes that the effectiveness of SHR’s entity-level controls over its ethics program is significantly deficient but not to the level of a material weakness. Prepare a scenario in which the combination of the deficiencies in the entity-level controls over the company’s ethics programs and deficiencies in related entity-level controls could rise to the level of a material weakness. Hint: consider entity-level controls pertaining to the company’s hiring and compensation practices.

Scenario 2: Using IT to Gain a Competitive Edge

Judiciously leveraging advances in IT is a fundamental enabler of SHR’s business strategy. In fact, SHR is recognized within the industry as a leader in the use of IT to gain operational efficiencies. For example, SHR implemented electronic data interchange (EDI) with its primary vendors several years ago to streamline its purchasing process and to maintain an uninterrupted flow of incoming inventory to its distribution centers and retail stores. The company places special emphasis on IT controls.

Illustrative business objectives and associated risks pertinent to SHR’s heavy reliance on IT are expressed as follows:

**Business Objective 1**: Align the company’s IT strategies with its business strategies. Judiciously leverage advances in IT to streamline the company’s business processes and information systems, gain operational efficiencies, and increase shareholder value.

- **Business Risk 1a**: Insufficient, irrelevant, unreliable, inaccurate, and/or untimely information may cause management to make poor IT investment decisions.

- **Business Risk 1b**: Failure to effectively and efficiently integrate acquired IT resources into business processes may adversely affect operational performance and cause unacceptable returns on IT investments.

**Business Objective 2**: Safeguard the company’s resources against misuse and loss.

- **Business Risk 2**: Unauthorized company personnel and/or outside parties may access the company’s information systems and misuse or misappropriate proprietary information and other assets.

**Business Objective 3**: Accurately record all valid, and only valid, purchase transactions on a timely basis.

- **Business Risk 3a**: Failure to record a valid purchase transaction may cause inventory and accounts payable to be understated.

- **Business Risk 3b**: Recording an invalid purchase transaction may cause inventory and accounts payable to be overstated.

- **Business Risk 3c**: Recording a valid purchase transaction in the wrong accounting period may cause inventory and accounts payable to be understated or overstated.
**Business Objective 4:** Process purchase transactions efficiently, that is, with a minimum of time, effort, expense, and waste.

**Business Risk 4:** Disruption or corruption of electronic transmissions between the company and its EDI vendors may cause delays in processing purchase transaction, which in turn will cause inventory shortages at the distribution centers and retail stores.

Use the business objectives and risks stated above as the basis for answering the following questions. As he or she deems necessary, your instructor will facilitate the formulation of collective answers to certain questions that will serve as uniform starting points for answering subsequent questions. Students may want to refer to chapter 7, “Information Technology Risks and Controls,” as they complete the Scenario 2 Activities.

**Scenario 2 Activities**

1. SHR’s senior management team understands the importance of aligning the company’s IT strategies with its business strategies. Identify two types of IT strategic decisions senior management already has made or is likely to make in the foreseeable future. Clearly explain the linkage between these IT strategic decisions and SHR’s business strategies.

2. Sound decision-making requires high-quality information.

   a. What information does senior management need to make informed IT strategic decisions?

   b. Identify the entity-level controls you would expect to be in place to ensure that senior management has high-quality information upon which to base its IT strategic decisions.

3. Explain what role, if any, internal audit should have in the IT strategic decision-making process.

4. One of SHR’s business strategies is to selectively acquire companies that complement its core competencies.

   a. Explain the effects a business acquisition could have on the inherent risk of failure to effectively and efficiently integrate acquired IT resources into its business processes.

   b. Describe the entity-level controls SHR should have in place to mitigate these effects.

5. SHR uses EDI to purchase inventory from its primary vendors.

   a. Identify the inherent business risks associated with the use of EDI. Include in your answer both entity-level risks and process-level risks.

   b. Identify the governance-level controls associated with the company’s use of EDI you would expect to find in place.
c. Management asserts that controls are designed adequately and operating effectively to mitigate the risk of unauthorized individuals accessing the company’s EDI system and misusing or misappropriating proprietary information or other assets.

1. Identify the management-oversight level IT controls you would expect to find in place if management’s assertion is true.

2. Identify the process-level controls and transaction-level controls, both manual and automated, you would expect to find in place if management’s assertion is true.

3. Assume that internal audit examined the IT management-oversight level controls identified in 1) above and found them to be inadequately designed. Explain how, if at all, this finding will affect the nature, timing, and extent of the audit procedures performed to determine the design adequacy and to test the operating effectiveness of the controls identified in 2) above. Provide specific examples to support your explanation.

6. All of SHR’s purchasing processes, including those in which EDI is not implemented, are highly automated. SHR’s perpetual inventory system also is fully automated.

a. Assume that internal audit examined the IT general controls pertaining to SHR’s purchasing processes and perpetual inventory system and found them to be designed adequately and operating effectively. Explain how, if at all, internal audit’s assessment of IT general controls will affect the nature, timing, and extent of the audit procedures performed to determine the design adequacy and to test the operating effectiveness of the IT application controls built into the automated purchasing processes and perpetual inventory system. Provide specific examples to support your explanation.

b. Assume that internal audit found the IT application controls built into the automated purchasing processes and perpetual inventory system to be designed adequately and operating effectively. Explain how, if at all, this assessment will affect the nature, timing, and extent of the audit procedures performed to determine the design adequacy and to test the operating effectiveness of the manual process-level and transaction-level controls pertaining to purchases, accounts payable, and inventory. Provide specific examples to support your explanations.

7. Management asserts that controls are designed adequately and operating effectively to mitigate the risk of delays in processing purchase transactions and inventory shortages caused by disruption or corruption of electronic transmissions between SHR and its EDI vendors.

a. Identify the management-oversight level IT controls you would expect to find in place if management’s assertion is true.

b. Identify the process-level controls and transaction-level controls, both manual and automated, you would expect to find in place if management’s assertion is true.

c. Assume that internal audit examined the IT management-oversight level controls identified in a. above and found them to be designed adequately and operating effectively. Explain how, if at all, this finding will affect the nature, timing, and extent of the internal audit procedures performed to determine the design adequacy and to test the operating effectiveness of the controls identified in b. above.
8. Assume that internal audit concluded, prior to beginning its testing of IT controls, that deficiencies in entity-level controls over the company’s ethics program and hiring and compensation practices, when considered in combination, constitute a material weakness in internal control. Explain what impact, if any, this conclusion should have on internal audit testing of IT controls at the:

a. Governance level.
b. Management-oversight level.
c. Process and transaction levels.

---

3 Ibid., paragraph 24.