Risk Assessment and Risk Response

5122.03 There are two types of risk. Inherent risk is the risk that exists before management takes any steps to control the likelihood or impact of a risk. Residual risk is the risk that remains after management reacts to the risk, such as by implementing internal controls.

An internal control risk assessment has six steps and is performed as follows. (Also see Figure 1.)

5122.04 Identify threats. Companies face the following types of threats:
   a. Strategic (doing the wrong things)
   b. Operating (doing the right things, but in the wrong way)
   c. Financial (financial resources are lost, wasted, or stolen; inappropriate liabilities are incurred)
   d. Information (incorrect input data, faulty or irrelevant stored information, an unreliable system, incorrect or misleading reports)

5122.05 Estimate risk, which is a measure of how likely an error is to occur. Errors are more likely than fraud.

5122.06 Estimate exposure, which is a measure of the magnitude of an error. For example, there is a small risk of an earthquake, but the exposure is enormous if it destroys the information system.

5122.07 Identify controls. One or more controls should be identified to protect the company from each threat. Preventive, detective, and corrective controls complement each other, and a good internal control system employs all three.
   a. A preventive control is superior to a detective one.
   b. If preventive controls fail, detective controls are essential for discovering the problem.
   c. Corrective controls help recover from the problem.

5122.08 Estimate costs and benefits. The following principles should govern this analysis:
   a. An internal control system provides reasonable assurance that control problems do not take place; no system can provide foolproof protection, as the cost would be prohibitive.
   b. Too many controls slow the system down and negatively affect operational efficiency.
   c. The benefits of an internal control procedure must exceed its cost.
   d. The benefit of a control procedure is the difference between the expected loss with the control procedure(s) and the expected loss without it.
   e. Expected loss is the mathematical product of risk and exposure. (Expected loss = Risk × Exposure)

5122.09 Respond to risk.
   a. Reduce the risk. Implementing an effective system of internal controls is the most effective way to reduce the likelihood and impact of risk.
   b. Accept the risk by not acting to prevent the risk or lessen its impact.
   c. Share some of the risk or transfer it to another party by outsourcing an activity, acquiring insurance, or hedging transactions.
   d. Avoid the risk by not engaging in the activity that produces the risk.
Figure 1

1. Identify the events, or threats, that confront the company
2. Estimate the likelihood, or probability, of each threat occurring
3. Estimate the impact, or potential loss, from each threat
4. Identify controls to guard against threat
5. Estimate costs and benefits from instituting controls
6. Is it cost beneficial to protect system from threat? (Yes/No)
   - No: Avoid, share, or accept risk
   - Yes: Reduce risk by implementing controls to guard against threat
5123 Change Control Process

5123.01 Change control is the process of requesting a change, reviewing the effectiveness of the change, approving the change, and implementing the change.

5123.02 Reasons for change:
   a. Business needs have changed.
   b. Business partners have changed.
   c. The organization has changed.

5123.03 Thoughts for a change control process:
   a. Why should changes be approved?
   b. Who is involved?
   c. Who is in charge?
   d. What are the procedures?
   e. What other management procedures are affected?
   f. What tools will be needed?
   g. What is the best means of communication?

5123.04 Procedures:
   a. The change control board approves the change and assigns someone to head the project.
   b. The project leader or project manager makes sure all required signatures and authorities have been received.
   c. The project manager sets up schedules and tasks for individuals involved in the project.
   d. All personnel involved in the project then complete their portion of the project. They all must follow the instructions from the project manager in order to keep things running smoothly.
   e. Once all the work is done, the input must be tested and approved.

Information and Communication

5123.05 The primary purpose of an information system (IS) is to produce information that improves decision making, which helps to better integrate a change control process. This requires an understanding of how:
   a. transactions are initiated, authorized, and handled.
   b. data is captured in electronic form or converted from source documents to an electronic format.
   c. data is processed.
   d. computer files are updated.
   e. data is stored and retrieved.
   f. data is summarized and formatted as output.
   g. information is reported to internal and external users.
These items form what is referred to as an audit trail. An audit trail must go two directions:

a. Individual transactions can be traced from the point where they occur through the system to the financial statements.

b. Financial statement numbers can be traced back through the system to individual transactions.