superfastCPA

BEC

2021 SuperfastCPA Review Notes

[Updated for the July 2021 changes]

CONTENTS

I: ENTERPRISE RISK MANAGEMENT, INTERNAL CONTROLS, AND BUSINESS PROCESSES

A. ENTERPRISE RISK MANAGEMENT (ERM)

1. PURPOSE AND OBJECTIVES

Enterprise risk management as defined by COSO ERM is "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The purpose of the COSO ERM model is to provide an all-encompassing framework for managing risk throughout all activities of an entity.

Business Strategy in the Context of COSO ERM

The ERM framework is based on the fact that most strategic business decisions don't have a right or wrong answer: there are pros and cons and subsequently levels of risk that go with any strategic decision. By applying the ERM framework as an organization makes and implements business strategies, the organization is able to align its objectives with its risk appetite, evaluate risk responses, and respond to opportunities.

2. COMPONENTS AND PRINCIPLES

The COSO ERM model has 5 components:

The 5 components are:

- Governance and culture
- Strategy and objective-setting
- Performance
- Review and revision
- Information, communication, and reporting

Objectives

The ERM model is geared to achieving 4 main categories of objectives:

- Strategic: high-level goals that align with and support the mission of the entity
- Operations: effective and efficient use of the entity's resources
- Reporting: reliable reporting
- Compliance: compliance with applicable laws and regulations

Limitations of the Model

The limitations are similar to the inherent limitations of an internal control system. These include:

- Human judgment and human error
- Cost vs benefits limitations
- Simple errors can lead to big mistakes
- Circumvention of controls or processes due to collusion
- Management override

Principles of COSO ERM

There are 20 core principles within the 5 components:

Governance and Culture

- Exercises board risk oversight: The board provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives
- Establishes operating procedures: The organization establishes operating structures in the pursuit of strategy and business objectives
- Defines desired culture: The organization defines the desired behaviors that characterize the entity's desired culture
- Demonstrates commitment to core values: The organization at all levels demonstrates a commitment to core values
- Attracts, develops, and retains capable individuals: The organization is committed to building human capital in alignment with the strategy and business objectives

Strategy and Objective-Setting

- Analyzes business context: The organization considers potential effects of business context on risk profile
- Defines risk appetite: The organization defines risk appetite in the context of creating, preserving, and realizing value
- Evaluates alternative strategies: The organization evaluates alternative strategies and potential impact on risk profile
- Formulates business objectives: The organization considers risk while establishing the business objectives at various levels that align and support strategy

Performance

- Identifies risk: The organization identifies risk that impacts the performance of strategy and business objectives
- Assesses severity of risk: The organization assesses the severity of risk
- Prioritizes risks: The organization prioritizes risks as a basis for selecting responses to risk
- Implements risk responses: The organization identifies and selects risk responses
- Develops portfolio view: The organization develops and evaluates a portfolio view of risk

Review and Revision

- Assesses substantial changes: The organization identifies and assesses changes that may substantially affect strategy and business objectives
- Reviews risk and performance: The organization reviews entity performance and considers risk
- The organization pursues improvement in enterprise risk management

Information, Communication, and Reporting

- Leverages information systems: The organization leverages an entity's information and technology of enterprise risk management
- Communicates risk information: The organization uses communication channels to support enterprise risk management
- Reports on risk, culture, and performance: The organization reports on risk, culture, and performance at multiple levels and across the entity

Business Strategy in the Context of COSO ERM

The ERM framework is based on the fact that most strategic business decisions don't have a right or wrong answer: there are pros and cons and subsequently levels of risk that go with any strategic decision. By applying the ERM framework as an organization makes and implements business strategies, the organization is able to align its objectives with its risk appetite, evaluate risk responses, and respond to opportunities.

Other ERM items:

When risk is being prioritized, the most helpful metric is 'expected value', which calculates the likelihood of losses and the amount of losses.

According to COSO, the most effective method of communicating a message of ethical behavior throughout an organization is by demonstrating the behavior by example.

A 'compensating control' is a control that accomplishes the same objective as another control.

1. PURPOSES AND OBJECTIVES

COSO

COSO is an integrated framework for internal control and enterprise risk management.

Internal Control & COSO

COSO defines internal control as a process that is affected by all members of an organization that is designed to provide reasonable assurance regarding the achievement of objectives related to operations, reporting, and compliance.

According to COSO there are 5 major components of an internal control system:

- Control environment: “tone at the top”, and management’s philosophy towards internal control and responsibility
- Risk assessment: The process of identifying and managing risks
- Information and communication: The information and communication systems that allow a company’s employees to identify and exchange information regarding controls and operations
- Monitoring: Monitoring the company’s data and its systems
- Control activities: The policies and procedures implemented to ensure actions are taken towards completing the company’s objectives

Purpose of COSO

The purpose of COSO is to provide an integrated framework for internal control and enterprise risk management that businesses and organizations can apply to help achieve their operational, reporting, and compliance objectives.

Objectives of COSO

There are three main objectives of COSO:

- Operations objectives: Objectives pertaining to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss
- Reporting objectives: Objectives pertaining to internal and external financial and non-financial reporting which may encompass reliability, timeliness, transparency, or other terms set by regulators, standards, or entity's policies
- Compliance objectives: Objectives pertaining to adherence to laws and regulations applicable to the entity

Limitations of COSO

There are 6 main limitations of internal control identified by COSO:

- Human judgement can be faulty and subject to bias
- Breakdowns and failures occur as long as humans are involved, even from simple errors
- Management can override internal controls
- Management or other personnel can get around controls through collusion

- There will always be external events that are simply beyond management's control
- Objectives for controls must be suitable as a precondition to internal control (unrealistic or improbable objectives can be set that internal controls can't fully address)

Components of COSO

The components are again:

- Control environment
- Risk assessment
- Information and communication
- Monitoring
- Control activities

Principles of COSO

There are 17 principles of COSO within the 5 components.

Control Environment Principles:

- The organization needs to demonstrate a commitment to integrity and ethical values
- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in pursuit of the objectives
- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives
- The organization holds individuals accountable for their internal control responsibilities in pursuit of objectives

Risk Assessment Principles

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risk relating to objectives
- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed
- The organization considers the potential for fraud in assessing risks to the achievement of objectives
- The organization identifies and assesses changes that could significantly impact the system of internal control

Control Activities Principles

- The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels
- The organization selects and develops general control activities over technology to support the achievement of objectives
- The organization deploys control activities through policies that establish what is expected and procedures that put policies into action

Information and Communication Principles

- The organization obtains or generates and uses relevant, quality information to support the functioning of internal control
- The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

- The organization communicates with external parties regarding matters affecting the functioning of internal control

Monitoring Activities Principles

- The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning
- The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate

3. SARBANES-OXLEY ACT OF 2002

Because of large financial scandals, Sarbanes Oxley was passed which implemented regulations, many regarding the responsibilities of corporate management and external auditors.

Some of the main corporate governance provisions of SOX:

Audit Committees

Public companies are required to have an audit committee, and on the audit committee there must be a 'financial expert', which means that this expert has:

- An understanding of GAAP and financial statements
- Experience in preparing or auditing financial statements
- Experience with internal auditing controls
- An understanding of audit committee functions

If the company doesn't have a "financial expert", it needs to disclose the reason.

The audit committee must have at least 3 members, and each member must be an independent member of the board of directors. Independent meaning they only receive compensation for their service on the board, but no other financial ties to or compensation from the company.

Officer Certifications

On all 10Qs and 10K reports, the CEO and CFO must certify:

- That they have reviewed the report
- That the report doesn't have any material mistakes as far as they know
- That the statements are presented fairly in all material respects
- That they are responsible for and have evaluated internal controls
- That they have disclosed any significant control deficiencies or fraud to the external auditors and to the audit committee

Rules Regarding Auditors

External auditors are not allowed to provide certain kinds of non-audit services to their auditing clients, such as the design and implementation of financial information systems, bookkeeping services, appraisal or valuation services, etc. The auditor can provide tax services if approved by the audit committee.

Public companies have to disclose how much they spend on audit and audit-related services.

The power to hire and fire an external auditor is completely up to the audit committee, instead of management or the board of directors.

PCAOB

The PCAOB was created as a result of SOX. The PCAOB sets audit standards for public companies, and enforces compliance with its rules, SOX, and applicable securities laws and regulations.

Accounting and Financial Reporting Systems

Accounting systems and financial reporting systems vary based on the type of business, the industry the business operates in, as well as the specific objectives of an organization.

The most basic function of an accounting system is to 1) track the income and expenses of an organization, 2) to provide managerial reports, financial statements, reports prepared for external users, and provide adequate information in order to file tax returns. The accounting system should also address the specific needs of the business: some businesses need robust manufacturing or inventory tracking while service-based businesses would prioritize an entirely different set of core functions for their accounting system.

The job of the financial reporting system is to capture data about the relevant transactions and events that occurred during the period, to summarize and present this data in a format that's understandable and useful for its users, usually for external users.

Information flow of the financial reporting system:

- Data is received about a transaction or event.
- The transaction is recorded in a book of prime entry.
- Summary totals from the books of prime entry are posted to the general ledger accounts.
- Ledger accounts are summarized in a trial balance.

- Trial balances are used to generate the financial statements.

Business Process Controls

Categories of Controls

- Preventive controls: These are controls that prevent an error before it occurs
- Detective controls: These are controls designed to detect an error after it has occurred
- Corrective controls: Controls meant to reverse the effects of an error
- Feedback controls: These are procedures where the results of a process are evaluated and if the results are undesirable, the process is adjusted to modify the results
- General controls: These are controls that apply to all parts of information processing, and are "general" in nature such as restricting access to data storage, and physical security of assets and records
- Application controls: These are controls over specific parts of data input and processing meant to ensure the accuracy, completeness, and validity of transaction processing
- Automated vs manual controls: Automated controls are controls built into a system, such as a field in a form only accepting a

phone number instead of text in order to prevent input errors. Manual controls rely on human actions.

Business Process Controls

Segregation of duties: The 3 main types of tasks that should be separated are:

- Authorization (execution) such as granting credit.
- Access (custody) such as custody of the pre-numbered sales invoices or the goods being handled by the shipping department.
- Accounting (record keeping) such as entering customer's order form and dealing with receivables and collections.

Internal Control Objectives for Receipt of Cash

- When cash (checks) are received, they are posted to a remittance log which is a listing of all cash receipts.
- The transaction is also posted in the cash receipts journal, and all cash receipts will be posted to that month's receipts in the general ledger.
- Different employees should open the mail, do the accounting activities, prepare the deposit of checks, and reconcile the bank accounts.

- Each cash receipt should be listed immediately when the mail is open.

    - The best control over cash receipts is a bank lockbox system- then employees never touch cash receipts.

- Employers will "bond" employees that handle cash receipts. Bonding insures the company against loss from illegal acts by employees, and this reduces the risk of dishonesty by employees because the bonding company must approve the employees in the first place, and if employee theft happens, the bonding company does an investigation before paying the company back. So, bonded employees know they will be highly scrutinized if theft occurs.

- Lapping is when cash received from a customer is stolen and the shortage is hidden by crediting the first customer's account with cash received from a second customer. To prevent this, two different people should be receiving cash, and posting payments received to the accounts receivable ledger.

Internal Control Procedures for Expenses/Disbursements

- The purchasing department should make the purchases using pre-numbered purchase orders.

- The receiving department takes possession of deliveries.

- The accounts payable department should handle the accounting function and approve payments.

- Only designated employees should be able to make purchases for the company.

- Checks should require dual signatures.

- For both receipts and disbursements bank reconciliations should be prepared on a timely basis.

- Again, all key documents should be pre-numbered and the sequence should be accounted for as well.

- Supporting documents such as invoices should be canceled as "paid" as soon as they are paid.

Internal Control Procedures for Payroll

- Process consists of employee timecards, time sheets, or time sheets for salary employees taken and then payroll is prepared and recorded in the payroll journal. Then checks are given to employees, and the month's payroll is posted to the general ledger.

    - The approval of time cards by an employee's direct supervisor is one of the best controls for making sure employees only get paid for work performed.

- HR keeps records that contain pay rates and personnel files. Certain HR employees should be the only ones who have access to these files.

- The treasury issues the checks and signs them and distributes the checks.

- Payroll department calculates payroll and does the record-keeping each period.

System and Organization Controls (SOC)

Many businesses outsource various parts of their information systems needs to "service organizations" that specialize in such areas, such as outsourcing all payroll to an outside service. These service organizations are audited to provide reporting on the service organization's internal controls over these information systems, and the controls being audited are grouped into five categories called "trust service principles".

The 5 Trust Service Principles are:

1. Security
    a. Firewalls
    b. Intrusion detection
    c. Multi-factor authentication
2. Availability
    a. Performance monitoring
    b. Disaster recovery
    c. Incident handling
3. Confidentiality
    a. Encryption
    b. Access controls

    c. Firewalls
4. Processing integrity
    a. Quality assurance
    b. Process monitoring
5. Privacy
    a. Access control
    b. Multi-factor authentication
    c. Encryption

Levels

There are two levels of SOC reports which are also specified by SSAE no. 18:

- Type I, which describes a service organization's systems and whether the design of specified controls meet the relevant trust principles. (Are the design and documentation likely to accomplish the goals defined in the report?)
- Type II, which also addresses the operational effectiveness of the specified controls over a period of time (usually 9 to 12 months). (Is the implementation appropriate?)

Types

There are three types of SOC reports.

- SOC 1 — Internal Control over Financial Reporting (ICFR)
- SOC 2 — Trust Services Criteria
- SOC 3 — Trust Services Criteria for General Use Report

Additionally, there are specialized SOC reports for Cybersecurity and Supply Chain.

SOC 1 and SOC 2 reports are intended for a limited audience - specifically, users with an adequate understanding of the system in question. SOC 3 reports contain less specific information and can be distributed to the general public.

Business Process Controls in Action

A basic "walkthrough" of what appropriate business process controls would look like is:

- The business would have appropriate segregation of duties over key functions, roles, and processes:
    - Authorization
    - Custody of assets
    - Record keeping
- There would be input edit checks, which are preventive controls, to ensure that data and transactions entered are complete and accurate:
    - A completeness check forces all key fields to be entered before moving onto the next step.
    - Closed-loop verification is when data entered is checked against a reference and displayed to ensure accuracy, such as entering an address in a form and the system validates the address or displays an error.

    - Field checks are when a field only accepts a certain format or type of character, such as a phone number field only accepting numbers.
- The business would have a system of authorization and approval:
    - Employees are authorized to perform certain tasks or access specific parts of the system, and the approval or review of events or transactions is performed by another employee or supervisor.
- There would be verification controls and physical controls in place to grant or restrict access to physical locations or systems:
    - Users of the system have usernames and passwords that let them access specific parts of the system, or RFID badges that let them through certain doors, or biometric devices to grant or restrict access.
- There would be controls over master files (standing data):
    - Again there would be access or authorization controls, or change controls where every time a change is made to a key file or system, there is a review and approval process.
    - There would be a backup process in place for standing data.
- There would be spreadsheet controls, as most businesses use some form of spreadsheets as part of their business processes:
    - There would be access and authorization controls.
    - Key cells containing formulas or data that shouldn't change would be locked or restricted to key personnel.
    - There would be data validation controls built into the spreadsheets.
    - There would be a backup process in place.
- There would be controls over reconciliations.

    - Reconciliations are a form of detective control where transactions or events are reviewed.
- There would be supervisory controls which would perform both preventive and detective functions:
    - Preventive supervisory controls would be hiring guidelines, org charts, supervision, and approval procedures.
    - Detective supervisory controls would be performance reviews, reconciliations, reviewing KPIs, audits, job rotation and/or mandatory vacations.