

## CFE-In-Practice - International

---

Licensed Financial Investigator • Certified Fraud Examiners • Forensic CPA • Compliance ITP

### SEATA methodology in Compliance Reviews and Mitigation

Regulatory requirements related to security have changed dramatically over the last 8 years and the changes are likely to continue. Whether it's the EU 2005/60 on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing, FSA on Outsourcing Guidelines, Health Information Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), California Senate Bill 1386 (SB1386), or the myriad of other international, federal, state, and local regulations, regulatory drivers are increasingly and more directly requiring stronger management controls over security functions within companies.

#### SOX 404 as an example:

The best recent example of the regulatory drive for controls is the rush to compliance with SOX section 404. SOX 404 is the first law in this space to really have teeth. The punishment for executives of public companies who fail to meet the requirements of SOX 404 is federal prison.

The language of the law really has no specific requirement for security controls of any sort. However, the requirement for financial controls combined with the use of information technology in accounting and the regulators' interpretation of the law leads to more specific requirements. The most specific requirement identified in the interpretation is the adoption of the recommendations of the Committee Of Sponsoring Organizations (COSO) of the Treadway Commission.

These recommendations identify control requirements that are not specific in any way.

#### **But they do require that top management:**

- Set control objectives
- Identify events that can cause serious negative consequences
- Assess risks associated with those events
- Respond to risks using a risk management strategy
- Deploy control activities appropriate to those responses
- Communicate control requirements effectively throughout the enterprise
- Monitor compliance with those controls

This must be done at the entity, division, business unit, and subsidiary levels as part of strategy, operations, reporting, and compliance.

As enterprises rush to comply, they are required to have their accountants attest to the adequacy of their internal controls.

Their accountants are also rushing to help them comply, but the lack of skilled experts and specific guidance in analysis of control standards like COSO means that there isn't enough expertise to do the job properly. So accounting firms choose more specific control standards, like CoBit, create checklists, and have inexperienced auditors use them to review enterprises.

Enterprises or their employees may misrepresent the situation and are often less than forthcoming, making the process adversarial in nature, and making it impossible to accurately validate the results. The combination often produces results that are expensive to implement, ineffective at managing risk, and don't really meet regulatory or enterprise requirements.

## Service Summary

We are usually brought into the compliance picture before an audit as a pre-audit reviewer, after preliminary audit results as a mediator to reconcile disagreements before the audit is finalized, and after audit completion to help mitigate shortfalls.

### **Pre-audit:**

In the pre-audit role, the most effective process is an Information Protection Posture Assessment (IPPA) with SOX emphasis. This assessment rapidly identifies the issues that have potentially serious negative consequences and are inadequately controlled, identifies general control limitations that should be mitigated, and does a comparison with COSO and more detailed control standards to give a sense of the situation and paths to mitigation. IPPAs take from 30 to 90 man days to complete and are usually scheduled 5 to 10 days in advance.

### **• Mediation:**

In the mediation role, we are usually contacted over specific issues where the accountant and the internal experts disagree. These are usually the result of inconsistencies in the requirements, inadequate understanding of risk issues, checklists that are misapplied, decision makers who don't believe results, and so forth. In these cases we are typically engaged on a retainer basis to negotiate a reasonable solution that the auditors can attest to and the enterprise can implement.

### **• Mitigation:**

In the mitigation role the challenge is often more daunting. We are called on to meet very tight schedules for such things as complete compliance policy rewrites, creation of a full spectrum of activities for a Chief Information Security Officer (CISO), or addressing internal power struggles between Compliance, Internal Audit and Risk Management.

These services are usually provided through pre-defined service offerings such as our policy reconciliation and rewrite service or our CISO service. They involve standard processes at standard pricing with add-ons based on time and materials.

Whether it's EU 2005/60, FSA, SOX 404, HIPAA, GLBA, SB1386, the European Union anti money laundering issues, or any other requirement for regulatory compliance involving security-related issues, including but not limited to certification to compliance for regulatory guidelines for outsourcing, we have the people and the experience to efficiently and effectively resolve the issue in a timely and professional manner.

For information on assistance with regulatory compliance and risk management issues, contact us at [enquiry@cfe-in-practice.com](mailto:enquiry@cfe-in-practice.com) for a scoping call and we will generate a statement of work with a detailed quotation for your consideration.

## Background

In 1992, the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors, the American Accounting Association, the Institute of Management Accountants and the Financial Executives Institute issued a jointly prepared body of work entitled Internal Control – An Integrated Framework.

This authoritative document identifies the fundamental and essential objectives of any business or government entity: economy and efficiency of operations, including safeguarding of assets and achievement of desired outcomes; reliability of financial and management reports; and compliance with laws and regulations. The Internal Control-Integrated Framework, issued by the Committee of Sponsoring Organizations of the Tread way Commission in 1992, (COSO report) has become a widely accepted basis for developing business control systems and assessing their effectiveness. This information tool was developed to help end-users of derivative products establish, assess, and improve internal control systems using the COSO Framework. Many of the control considerations discussed in COSO are also applicable to financial instruments other than derivatives.

To achieve quality, processes must first be in control. To improve quality, controlled processes must be measured and evaluated to identify obstacles to success. Effective internal control opens the door that leads to achievement of success. The approach presented by the Framework goes directly to the one key issue of any business – is there reasonable assurance of achieving our mission, objectives, goals and desired outcome, while adhering to laws and regulations; and can we accurately report our success and outcomes to the public and interested third parties.

The COSO framework describes a unified approach for evaluation of the internal control systems that management has designed to provide reasonable assurance of achieving the fundamental business objectives described above.

The original COSO framework contains five control components needed to help assure sound business objectives. The control components are:

- Control Environment.
- Risk Assessment.
- Control Activities.
- Information and Communication.
- Monitoring.

The new Enterprise Risk Management (ERM) COSO framework emphasizes the importance of identifying and **managing risks across the enterprise**.

The new COSO framework consists of eight components: **Internal control environment, Objective setting, Event identification, Risk assessment, Risk response, Control activities, Information and communication, and Monitoring.**

The three new components of the COSO framework are **Objective setting, Event identification, and Risk response.**

Internal control is a broadly defined process, carried out by people, designed to provide reasonable assurance regarding the achievement of the following three objectives that all businesses should strive towards attaining. They are as follows:

- Economy and efficiency of operations, including achievement of performance goals and safeguarding of assets against loss
- Reliable financial and operational data and reports.
- Compliance with laws and regulations.

Collectively, the three primary business objectives and the new eight components needed to achieve those objectives constitute the internal control framework. When looking at any one of the three primary business objectives, all eight components of the control system must be present and functioning effectively in order to conclude that internal controls over operations are effective.

While internal control is a process, its effectiveness is a state or condition of the process at a fixed point in time. When an internal control system meets the following standard, it can be deemed "effective".

In other words,

## **Control Components**

### **The ORIGINAL COSO Cube**

The original COSO framework contains five control components needed to help assure sound business objectives. The control components are:

- Control Environment.
- Risk Assessment.
- Control Activities.
- Information and Communication.
- Monitoring.

## **2004 COSO Document:**

### **Enterprise Risk Management (ERM) COSO Framework**

### **The New COSO Cube**

The new Enterprise Risk Management (ERM) COSO framework emphasizes the importance of identifying and managing risks across the enterprise. The new COSO framework consists of eight components:

- Internal control environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring.

The three new components of the COSO framework are:

**Objective setting, Event identification, and Risk response.**

This is what CFE-IN-PRACTICE address using its SEATA methodology.

**COSO tells you what it is. SEATA teach you how to do it.**

# CFE-In-Practice

---

Licensed Financial Investigator • Certified Fraud Examiners • Forensic CPA • Compliance ITP

## Introduction to suite of services

CFE-In-Practice is a leader in COSO-based risk management and assessment, and COSO framework-based Internal controls implementation. Utilizing the eight processes noted in the new ERP COSO framework, we will work with your organization to implement a COSO-based framework in compliance with Sarbanes-Oxley and or FEC mandates.

The Security and Exchange Commission (SEC) rule-making for Sarbanes-Oxley Section 404 mandated that a company's internal control over financial reporting should be based upon a recognized internal control framework. The model framework, suggested by the SEC, is the one created by "COSO".

### **The COSO Framework focuses on having a control system in place.**

CFE-In-Practice developed SEATA as the hands-on audit methodology in applying the COSO framework.

By requiring a company to adopt an internal control framework for its control environment, the SEC is a way of requiring a systematic methodology for evaluating internal control over financial reporting.

Compliance with the COSO Framework requires a company to examine itself to see if its business and financial processes contain tangible elements of the COSO recommended methodology for evaluating internal controls over business processes used to protect corporate assets. Therefore, a COSO compliance evaluation is about documenting what a company does to support the eight steps of the COSO internal controls methodology, providing supporting materials broken down by each step.

A company may have solid support for most of its processes; however, if a company lacks written Policy for selected processes, the unsupported processes highlight a weakness in the financial system and the control and monitoring of the system.

These are some of our more specific Sarbanes-Oxley Consulting Services areas:

- Sarbanes-Oxley Section 302 and 404 Compliance. Here, we will work with you to implement a financial reporting plan that will assist your organization in assessing and documenting your company's internal controls. This will include Planning, Assessing your Design Effectiveness, Assessing Operating Effectiveness, Reporting, and provide ongoing monitoring.
- Internal Audit Services. Here, in applying SEATA, we work with Internal Audit departments to implement COSO-based audit framework, and establish the methodologies for auditing internal controls in compliance with Sarbanes-Oxley.
- Information Systems Planning and Selection. Here, we' will help you select systems that meet not only your current but also your future needs as well as facilitate your overall business plan. We can help you select systems ranging from enterprise business applications, risk management, voice and data, access control and security management, and communication to financial accounting.

- Section 404 Implementation Services. We will perform a gap analysis and vulnerability review of your current environment. Specifically, we will perform a System and organization inventory, Risk Assessment, Control Framework selection, Control analysis and documentation, Testing of internal controls and an action plan for ongoing testing of internal control. This is what your external auditors will perform most of the attestation. Also, we will perform General Controls Audit of Infrastructure used by the applications impacted by Sarbanes-Oxley, and finally establish Post-Implementation monitoring processes.
- Vulnerability Review of Sarbanes-Oxley Impacted Systems. Here, we'll provide management with an independent assessment (ITP Compliance certification) of whether existing or new systems will resolve Sarbanes-Oxley control issues identified in the replacement systems and whether new Sarbanes-Oxley issues will arise from the implementation of the new system or by using existing systems. This is the Phase I requirements of Sarbanes-Oxley compliance project.
- Financial Data Mapping, development and review of Policy, procedures and compliance manuals.

**Technology is a major player in the FEC and Sarbanes-Oxley compliance.**

CFE-In-Practice is the leading independent third party assessor or integrator of software solutions for implementing COSO-based Audits, FEC Policy and Internal controls for complying with Sarbanes-Oxley Section 404.

Using SEATA, CFE-In-Practice is able to establish a lasting relationship with you to implement a FEC management solution for your organizations. Talk to us so that we can demonstrate to you that we are your resource of choice when it comes to implementing COSO framework-based Audits, FEC Policy and Internal controls for complying with Sarbanes-Oxley Section 404. But please take note that each of these services is separately chargeable.

**Please do not sign on any our service proposals if you have not sought and obtain clearance from your legal advisor.**

# **CFE-In-Practice**

## **Appendix A:**

### **(aka TERMS of Engagement)**

**This is an integral part of any service(s) we offer.**

## **Standard Terms of Engagement**

These terms are to be read in conjunction with our attached Engagement Letter, together form the contract ("this Contract").

### **1. Interpretation**

- 1.1. In this Contract, CFE-In Practice is referred to as "we", "our", and "us".
- 1.2. In this Contract, our client that the Engagement Letter is addressed to is collectively referred to as "you" and "your".
- 1.3. We will perform the Engagement as an independent contractor. Nothing shall be construed to create a partnership, joint venture or other relationship. No party has the right, power or authority to oblige or bind the other in any manner.
- 1.4. In the event of any inconsistency between these Terms of Engagement and the Engagement Letter, the Engagement Letter will take precedence.
- 1.5. This Contract supersedes and extinguishes all prior agreements, statements, representations and understandings whether verbal or written between us relating the matters dealt with in this Contract.

### **2. Services**

- 2.1. We shall perform the Engagement based on the scope as mutually agreed and stated in the Engagement Letter, with due care, competence and diligence.
- 2.2. You agree to provide to us, on a timely basis, the information and resources, which are complete and accurate, that are reasonably necessary. Unless otherwise advised or agreed, we shall rely on that information provided without further verification.
- 2.3. We must use all reasonable commercial efforts to complete the Engagement within the time frame as set in the Engagement Letter or otherwise mutually agreed.

### **3. Deliverables**

- 3.1. We shall report to you in the manner set out in the Engagement Letter.
- 3.2. We give you a royalty-free perpetual licence to utilise the reports, written advice and other deliverables for your own internal use only, which shall include use by your parent and associated companies. If you wish to use these materials outside your own organisation, you must get our prior written permission.
- 3.3. Unless we have agreed in writing, no advice or other information provided to you is to be passed on or made available to be used or relied upon by any third party. We assume no responsibility in any circumstances to any party other than you. For the avoidance of doubt, your, parent and associated companies shall not be considered a "third party" for the purposes of this paragraph 3.3.
- 3.4. We retain all copyright (and other intellectual property rights) in everything we develop (or are involved in developing) either before or during the course of an engagement - including systems, methodologies, software and know-how, except for everything we are obliged to deliver to you under the Engagement.

3.5. You acknowledge that the working papers we produce in the course of the Engagement, which are not or do not form an integral part of the Deliverables of the Engagement, are our property.

3.6. We do not guarantee the security and integrity of any electronic communications or information sent or received in relation to this engagement. Whilst it is our policy to check our e-mail correspondence and other electronic information with anti-virus software, we do not guarantee that transmissions or other electronic information will be free from infection.

3.7. You acknowledge that we may, from time to time, wish or be required to work with its affiliates in other locations around the world regarding the execution of the engagement. You hereby authorize us to forward all information as we consider reasonably necessary for such purposes through mail, fax, electronic or other means.

#### **4. Confidentiality**

4.1. We, and our staff members, shall not disclose to third parties confidential information relating to you or to anything related to this Engagement, unless compelled to do so by law. We acknowledge that your confidential information is your property.

4.2. You will not disclose to third parties confidential information relating to us or our processes, ideas, concepts or techniques unless compelled to do so by law. You acknowledge that our processes, concepts and techniques are our property and are also confidential information.

#### **5. Conflict of interest**

5.1. We are not presently aware of any conflict of interest which would affect our ability to perform the Engagement. We shall advise you if we become aware of any potential conflict of interest, and we will work with you to reach a suitable solution.

#### **6. Fees and expenses**

6.1. Our fees reflect the time costs incurred on the Engagement and we have taken into account the degree of responsibility, the level and the experience of the staff members involved. We shall endeavor to provide a staff mix that will produce the most efficient services.

6.2. Any fee estimate provided by us is prepared based on the understanding specified in the Engagement Letter or otherwise mutually agreed. We reserve the right to revise the fee estimate if it becomes apparent that the understanding we relied on is no longer valid and we shall discuss and agree with you on additional fees prior to commencing the work.

6.3. You agree to pay all out of pocket expenses reasonably incurred by us in providing the services, upon receiving supporting documentation of such expenses actually incurred that are satisfactory to you.

#### **7. Payment**

7.1. You agree to pay fees and expenses as specified in our Engagement Letter.

7.2. We shall invoice you on a monthly basis, or on the completion of the Engagement, or in the manner specified in the Engagement Letter, or otherwise mutually agreed. You have the right to withhold payment of the fee (or any part thereof) if there is any dispute on the amount invoiced and/or if we fail to provide the Services according to the terms of this Contract.

## **8. Liability**

8.1. We shall use reasonable skill and care in the performance of the Engagement and the preparation of any deliverables.

8.2. All of our civil liability (including interest and costs) to you, concerning the subject matter of this Contract, including the liability of any of our directors, partners, employees or agents, in respect of any breach of Contract or breach of duty or fault or negligence or otherwise whatsoever arising out of or in connection with the engagement, shall be limited to zero point five times the fees **paid** to us by you under this Contract. This provision shall have no application to any liability for death or personal injury, or any other liability for which exclusion or restriction is prohibited by law or to any liability arising as a result of fraud on our part.

8.3. In determining proportionality of loss or damage caused, account shall be taken of any loss or damage that is reasonably attributable to any third party.

8.4. You agree that we may, in our absolute discretion, choose either to re-perform the Engagement, or to pay you the cost of having the Engagement re-performed if it is fair and reasonable for us to make that choice.

8.5. In no circumstances we shall be liable to you for accidental, indirect, special, punitive or consequential damages whatsoever (including loss of profits) even if we have been advised of, knew or should have known of the possibility of such loss or damage.

8.6. We are not liable to the extent that you are responsible for an act or omission that contributed to your loss, including inaccuracy and incompleteness of the information provided by you.

8.7. We accept no responsibility to any party other than you, including any company that you are closely connected, affiliated, or forms part of any group of companies to which you belong.

## **9. Termination**

9.1. You may, provided 30 days written notice to us is given, terminate this Contract. Termination will not affect your obligation to pay our fees for all services performed to the date of the notice of termination.

9.2. Any of the terms and conditions of this agreement, which are intended to apply after termination, will continue to apply.

## **10. Governing Law**

10.1. This Contract will be governed by and interpreted in accordance with the laws of Singapore.

\*\*\*\*\*