An Assessment of Texas State Government

Implementation of Enterprise Risk Management Principles

By

Lynn Altemeyer

An Applied Research Project
(Political Science 5397)
Submitted to the Department of Political Science
Texas State University
In Partial Fulfillment for the Requirements for the Degree of
Masters of Public Administration
Spring 2004

Faculty Approval:

____
Dr. Patricia Shields

____
Dr. Howard Balanoff

____
Bruce Hermes

Table of Contents

Abstract 5
Chapter 1- Introduction and Statement of Research Purpose 8
Research Purpose 11
Chapter Summaries 11
Chapter 2 -The Political and Regulatory Environment 14
Sarbanes-Oxley Act of 2002 14
Government Auditing Standards 15
Texas Legislature 16
Texas State Auditor's Office 16
Evolution of Internal Control Models 17
Other Control Systems – CoCo, Cadbury and Turnbull 19
Control Self-Assessment 20
Table 2.1: Shifting Responsibilities Traditional Audit Approach vs. The Control Self-Assessment Approach 21
Two Problems 23
Need for Business Continuity Planning 24
Governance Failures 24
Solutions to the Two Problems 24
Examples in Texas State Government 26
Texas Commission on Environmental Quality (TCEQ) 26
Texas State Comptroller of Public Accounts 27
Level of Awareness in Texas State Agencies 28
Summary of the Political and Regulatory Environment 28
Chapter 3 – Enterprise Risk Management Framework 30
Enterprise Risk Management 30
Benefits of Enterprise Risk Management Framework 31
The COSO Enterprise Risk Management Framework 31
Chart 3.1 Enterprise Risk Management Framework 32
Internal Environment 33
Table 3.2: Comparison Turnbull Report to the COSO *Enterprise Risk Management Framework* 34
Objective Setting 35
Event Identification 37
Risk Assessment 39
Risk Response 41
Control Activities 43
Information and Communication 45
Monitoring 47
Conceptual Framework 48
Table 3.3: Linking the COSO *Enterprise Risk Management Framework* to the Literature 49
Summary of the Enterprise Risk Management Framework 53
Chapter 4 - Methodology 54

Survey Development and Use of GAIN Survey as a Benchmark 54
Linking the Survey Questions to the Conceptual Framework 55
Table 4.1: Operationalization: Linking the Survey Questions to the Conceptual Framework – Internal Environment: 55
Table 4.2: Operationalization: Linking the Survey Questions to the Conceptual Framework – Objective Setting 56
Table 4.3: Operationalization: Linking the Survey Questions to the Conceptual Framework – Event Identification 57
Table 4.4: Operationalization: Linking the Survey Questions to the Conceptual Framework – Risk Assessment... 58
Table 4.5: Operationalization: Linking the Survey Questions to the Conceptual Framework – Risk Response 59
Table 4.6: Operationalization: Linking the Survey Questions to the Conceptual Framework – Control Activities 60
Table 4.7: Operationalization: Linking the Survey Questions to the Conceptual Framework – Information and Communication 61
Table 4.8: Operationalization: Linking the Survey Questions to the Conceptual Framework – Monitoring... 62
Benchmarking Criteria 62
Survey Administration 63
Table 4.9 Agency Size of Survey Respondents 64
Limitations of the Study 64
Summary of Methodology 65
Chapter 5 – Results 66
Internal Environment 67
Table 5.1: Comparison of Survey Results for Internal Environment 67
Objective Setting 68
Table 5.2: Comparison of Survey Results for Objective Setting 68
Event Identification 69
Table 5.3: Comparison of Survey Results for Event Identification 69
Risk Assessment 70
Table 5.4: Comparison of Survey Results for Risk Assessment 70
Risk Response 71
Table 5.5: Comparison of Survey Results for Risk Response 71
Control Activities 72
Table 5.6: Comparison of Survey Results for Control Activities 72
Information and Communication 73
Table 5.7: Comparison of Survey Results for Information and Communication 73
Monitoring 74
Table 5.8: Comparison of Survey Results for Monitoring 75
Summary of Results 75
Table 5.9: Summary of the Assessment of Status of Texas State Agencies Implementation of Enterprise Risk Management Principles 75
Chapter 6 – Recommendations and Conclusion 77
Table 6.1: Evaluation Criteria 77

Table 6.2: Internal Environment 78
Table 6.3: Objective Setting 78
Table 6.4: Event Identification 79
Table 6.5: Risk Assessment 80
Table 6.6: Risk Response 81
Table 6.7: Control Activities 81
Table 6.8: Information and Communication 82
Table 6.9 Monitoring 83
Summary of Recommendations and Conclusions 83
Bibliography 86
Appendix 1 - Survey Document 89
Appendix 2 - Complete Survey Results 97
Internal Environment 97
Objective Setting 98
Event Identification 99
Risk Assessment 100
Risk Response 101
Control Activities 102
Information and Communication 103
Monitoring 104
Appendix 3 – Graphical Comparison of Survey Results 105
Graph A3.1: Comparison of Survey Results for Internal Environment 105
Graph A3.2: Comparison of Survey Results for Objective Setting 106
Graph A3.3: Comparison of Survey Results for Event Identification 106
Graph A3.4: Comparison of Survey Results for Risk Assessment 107
Graph A3.5: Comparison of Survey Results for Risk Response 108
Graph A3.6: Comparison of Survey Results for Control Activities 108
Graph A3.7: Comparison of Survey Results for Information and Communication 109
Graph A3.8: Comparison of Survey Results for Monitoring 110

Abstract

The field of enterprise risk management is an exciting combination of traditional risk management, strategic planning and management internal control models. The 2003 release of the draft of the COSO *Enterprise Risk Management Framework* is very timely. In the opinion of many in Texas state government internal auditing professionals, the reporting requirements of Sarbanes-Oxley legislation on the private sector is moving to the government sector. The U.S. Congress passed Sarbanes-Oxley legislation in 2002 to enhance accountability in public corporations. One of the most important requirements of Sarbanes-Oxley is the requirement that chief officers of publicly traded corporations document internal control systems and report on internal control systems to the Securities and Exchange Commission.

Professor Urton Anderson[1] reported to the Austin Chapter of the Institute of Internal Auditors in January 2004 that he had heard a presentation about applying Sarbanes-Oxley internal control reporting to government from a representative of the General Accounting Office (GAO). Chapter 1 contains statements from two Texas Internal Audit directors about their thoughts about the impact of Sarbanes-Oxley on government. There has already been one attempt to require Texas state agencies to evaluate and report on risks to their agency. The 78th Texas legislature passed Senate Bill 147, legislation that would have required this reporting, but the governor vetoed the bill. The passage of the bill by the legislature indicates interest in the legislature in proactively managing risk in Texas state agencies. It is reasonable to expect that Texas state agencies

[1] Associate Dean for Undergraduate Programs and Clark W. Thompson, Jr. Professor in Accounting, McCombs School of Business, University of Texas at Austin.

will have heightened reporting requirements on internal controls and risk management in the future.

The COSO *Enterprise Risk Management Framework* is a robust, comprehensive management control system that can be used in conjunction with other management theories like balanced scorecard (Kaplan, Norton, 1996). The COSO *Enterprise Risk Management Framework* builds on the 1992 COSO *Internal Control - Integrated Framework*. The COSO *Enterprise Risk Management Framework* has eight categories and is explained in detail in Chapter 3.

This applied research project assesses the implementation of some of the components of the COSO *Enterprise Risk Management Framework* at Texas state agencies. This assessment was performed by comparing[2] the results of a survey performed by the Institute of Internal Auditors Global Auditing Information Network (GAIN) against the same survey questions given to Texas state agency internal audit directors. The project methodology is located in Chapter 4. The survey results are located in Chapter 5.

The survey results indicate that Texas state agencies are implementing enterprise risk management principles at a rate similar to GAIN survey respondents. Chapter 6 identifies nine areas as high-risk to Texas state agencies based on the evaluation criteria in Table 6.1. The nine high-risk areas are:

- Organization has a formal risk management policy.
- Board level involvement in risk management.
- Senior management committee oversees risk.
- Risks are evaluated to ensure they do not exceed acceptable levels of risk.

[2] The comparison was performed using only the "partly agree" and "agree" responses. These responses indicate that the principle measured was partly or fully in place in the organization surveyed. A major limitation of the study is that there were only 15 responses from Texas state agencies.

- Acceptable tolerance limits on the risk to the achievement of key objectives have been determined.
- The costs and benefits of risk mitigation are taken into account in the evaluation of risk acceptability.
- There is a periodic review process to ensure that the organization's risk assessments remain current.
- The full range of available risk management options is considered when formulating risk responses.
- Alternative responses are evaluated in terms of the resulting costs and benefits.

Texas state agencies should consider these issues when assessing overall risk management and in policymaking decisions for Texas state agencies. The lack of a formal risk management policy is the most important risk for Texas state agencies to address. A formal policy assigns roles and responsibilities and provides criteria to use in assessing implementation of policy. Additional research is needed to determine the applicability and usefulness of COSO *Enterprise Risk Management Framework* principles to Texas state agencies.

Chapter 1- Introduction and Statement of Research Purpose

Recent events have brought corporate governance and risk awareness issues to the forefront of management thinking. Regulatory trends, including Sarbanes-Oxley and changes in *Government Auditing Standards,*[3] as well as the heightened awareness level of managers about the risks involved in internal control systems has created a need for a common definition of risk management and how risk management fits into an overall internal control environment. In order to meet this need, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[4] issued the *Enterprise Risk Management Framework*. The COSO *Enterprise Risk Management Framework* was designed to create a consistent "risk and control consciousness" throughout the enterprise and to become a commonly accepted model for discussing and evaluating the organization's risk management processes. The COSO *Enterprise Risk Management Framework* is made up of eight separate components including:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

[3] *Government Auditing Standards* – are generally accepted government auditing standards (GAS) promulgated by the Comptroller General of the United States.

[4] Information about COSO is from the COSO website www.coso.org. COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Reporting. This led to the issuance of the *Internal Control - Integrated Framework* in 1992. For the first time, there was a common language about the components of internal controls. The draft *Enterprise Risk Management Framework* was released for a 90-day public commentary period of July 15, 2003-October 14, 2003, and the final publication is due for release in early 2004.

The eight components work together in a scalable model to allow an organization to manage risk across the entire enterprise. Each of the eight components has several sub-components that were individually identified and assessed during this project.

The COSO *Enterprise Risk Management Framework* enhances the 1992 *Internal Control - Integrated Framework* by expanding the risk management aspects of the model and adding components of strategic planning. Enterprise risk management is a management tool that works with other management theories like balanced scorecard (Kaplan, Norton, 1996) and control self-assessment (CSA)[5].   The COSO *Enterprise Risk Management Framework* can be useful in implanting Sarbanes-Oxley reporting. The U.S. Congress passed Sarbanes-Oxley in 2002 to enhance accountability in public corporations. Sarbanes-Oxley requires that chief officers of publicly traded corporations document internal control systems and report on internal control systems to the Securities and Exchange Commission.

Currently the most popular model for assessing internal controls under Sarbanes-Oxley is the 1992 COSO *Internal Control - Integrated Framework*. The COSO *Enterprise Risk Management Framework* is a more comprehensive model for an organization to assess total risk and controls, the COSO *Enterprise Risk Management Framework* includes all five of the components of the COSO *Internal Control - Integrated Framework* and includes three other components that address risk management. The issuance of the COSO *Enterprise Risk Management Framework* has implications for Texas state agencies because of the potential for Sarbanes-Oxley internal control reporting to be applied to government.

[5] Control self-assessment is also referred to as business self-assessment.

Professor Urton Anderson[6] reported to the Austin Chapter of the Institute of Internal Auditors in January 2004 that he had heard a presentation about applying Sarbanes-Oxley internal control reporting to government from a representative of the General Accounting Office (GAO). Susan Driver the Internal Audit Director at the Texas Comptroller of Public Accounts stated her opinion about Sarbanes-Oxley in an email to the researcher:

> *Although Sarbanes-Oxley currently applies to public companies, many people feel it is just a matter of time before similar legislation applies to government. Sarbanes-Oxley was enacted to protect shareholders, creditors, and other stakeholders. There are vast numbers of stakeholders for government who need to know that their tax dollars are being spent effectively, that their agencies are in compliance with laws and good business practices, and that their leaders are ethically performing their duties. This becomes even more critical as the federal government and states face funding crises for providing government services. Effective corporate governance is beneficial to all organizations, whether they are public companies or government entities.*

Steve Goodson, Internal Audit Director at the Texas Commission on Environmental Quality shares a similar opinion with Ms. Driver. Mr. Goodson made the following assertion to the researcher in an email:

> *There is a movement to require state agencies to review and report on their internal control systems similar to the requirements in Sarbanes-Oxley. We saw this in the last legislative session with SB 147 and I expect we will be seeing an increased emphasis by the GAO for improved fiscal accountability at the state level.*

These statements confirm the current feeling among Texas state agency internal auditors that an internal control reporting requirement is coming to Texas state agencies. The scope and content of the new reporting requirement is not determined yet, but internal

[6] Associate Dean for Undergraduate Programs and Clark W. Thompson, Jr. Professor in Accounting, McCombs School of Business, University of Texas at Austin.

auditors expect that the requirement will resemble Sarbanes-Oxley. Discussion in Chapter 2 indicates that these changes are not only occurring in the United States. Both the United Kingdom and Canada have similar initiatives in progress.

Research Purpose

The purpose of the research is to assess the implementation of the COSO *Enterprise Risk Management Framework's* principles in Texas state agencies using both the principles in the COSO *Enterprise Risk Management Framework* and the results of the Global Auditing Information Network (GAIN) survey performed by *Internal Auditor* magazine as a benchmark. The research purpose was accomplished by surveying Texas state agency internal audit directors using the same questions used in the GAIN survey. Fifteen Texas state agencies responded to the survey. While the volume of responses is statistically insignificant, analysis of the survey results permit an assessment of the status of implementation of enterprise risk management principles for the Texas state agencies that responded to the survey.

Chapter Summaries

Chapter 2 provides background and setting information on the political and regulatory environment and includes discussions of Sarbanes-Oxley Act of 2002, *Government Auditing Standards*, recent activities of the Texas Legislature[7] and Texas State Auditor's Office.

[7] There has already been one attempt to require Texas state agencies to adopt risk management principles during the 78th Legislature Senate Bill 147 passed both houses, but was vetoed by the governor.

Chapter 3 contains a detailed description of COSO *Enterprise Risk Management Framework* and the sub-components that make up each of the eight components of the model.

Chapter 4 contains information about how the project objective was achieved through the use of an existing survey from the Institute of Internal Auditors, Global Auditing Information Network (GAIN). The GAIN survey included all of the components and most of the sub-components of the COSO *Enterprise Risk Management Framework*.

Chapter 5 is the results chapter and includes the findings and results of the research. The "partly agree" and "fully agree" survey responses have been interpreted by this study as implementation of the principle of enterprise risk management. The tables in Chapter 5 indicate the percentage of Texas state agency and GAIN respondents who answered each question that their agency "partly agree" or "fully agree" with the statement. The tables also contain the difference for each category including averages for each component and sub-component of the COSO *Enterprise Risk Management Framework*. The survey results indicate that the 15 Texas state agencies that responded positively to the survey are implementing enterprise risk management principles on a similar level to GAIN survey respondents.

Chapter 6 includes tables that evaluate the survey responses based on the risk to Texas state agencies. The assessment suggests that the responses to nine (18%) of the survey questions are the high-risk[8] to Texas state agencies. For comparison, 26 (50%) of

[8] To rate as **high-risk**, the response rate for "partly agree" and "fully agree" responses must have been below 50% and the response rate for Texas state agencies must have been lower than GAIN survey respondents.

the questions were assessed as low-risk[9].

Appendix 1 contains a copy of the survey instrument. Appendix 2 contains the survey results for the 15 Texas state agencies that responded to the survey. Appendix 3 contains graphical comparisons of the survey responses by question number.

Considering the low response rate, the project results are very favorable to Texas state agencies. Further study is needed to determine the actual implementation level for all Texas state agencies and to evaluate public policy implications.

[9] To rate as **low-risk**, the response rate for "partly agree" and "fully agree" responses must have been above 50% and the response rate for Texas state agencies must have been higher than GAIN survey respondents.

Chapter 2 -The Political and Regulatory Environment

This chapter discusses the impact of federal and state legislation as well as changes in auditing standards that impact the political and regulatory environment of both business and government. As noted in Chapter 1, Texas state agency internal auditors expect political and regulatory changes based on the effects of Sarbanes-Oxley Act of 2003 on government. During the 78th Texas legislative session, Senate Bill 147, legislation requiring mandatory reporting on risks was passed by the legislature but vetoed by the governor. These factors have future implications for Texas state agencies for additional reporting requirements for internal controls and risk management.

Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 addresses a need to improve governance in publicly traded companies in the United States of America. Compliance with Sarbanes-Oxley requires publicly traded companies to evaluate internal controls over financial reporting based on the COSO *Internal Control - Integrated Framework* (1992). As noted below, the United States General Accounting Office GAO statement about establishing the appropriate level of internal controls reporting for federal agencies will probably lead to a similar requirement for government entities. If so, COSO *Enterprise Risk Management Framework* will be a model that could be applied to both public organizations to comply with this requirement.

The Institute of Internal Auditor's publication *The Sarbanes-Oxley Act of 2002: Summary of Key Provisions of Interest to Internal Auditors* identified key provisions of the law (pages 11-12):

- Executive Management must certify the organization's internal controls.
- Management is responsible for ensuring a system of internal controls.
- Management must disclose significant deficiencies in the design or operation of internal controls.
- Management must report fraud.
- Management must disclose significant changes in internal controls.

In commenting on implementing Sarbanes-Oxley Act, Thomas (2003, p. 7), stated "one of the toughest SARBOX 404 issues concerns the proper criteria for evaluating controls. Most feel that the *Internal Control - Integrated Framework* set up by the Committee on Sponsoring Organizations for the Treadway Commission (COSO) in 1992 is most appropriate for now."

In effect, Sarbanes-Oxley requires publicly traded corporations to document internal controls and report on their implementation to the Securities and Exchange Commission. Some corporations are being forced to define, document and evaluate their internal control systems for the first time.

Government Auditing Standards

In June 2003, the General Accounting Office released the revised version of *Government Auditing Standards*. David Walker, Comptroller General of the United States, stated in his cover letter on the new standards,

> "We believe auditor reporting on internal control is appropriate and necessary for publicly traded companies and major public entities. We also believe that such reporting is appropriate in other cases where management assessment and auditor examination and reporting on the effectiveness of internal control add value and mitigate risk in a cost beneficial manner. In this regard, **GAO seeks to lead by example in establishing the appropriate level of auditor reporting on internal control for federal agencies**[10], programs, and entities receiving significant amounts of federal funding." (GAS 2003, p. 1-2)

[10] Bolding added for emphasis.

This statement by the GAO and the prior information reported by Dr. Anderson to the Austin Chapter of Internal Auditors indicate that the GAO plans to establish standards similar to Sarbanes-Oxley provision for federal agencies and entities receiving federal funding.

Texas Legislature

There has already been one attempt to put a risk assessment reporting requirement into law in the 78th Legislative Session in 2003. Senate Bill 147 passed both houses but was vetoed by the governor. The bill would have required agencies to assess risks that would keep them from fulfilling their mission and to describe their risk management strategies and control environment. The bill was associated with traditional risk management rather than governance issues and this may have contributed to its veto. Mike Hay from the State Office of Risk Management stated that S.B. 147 was based on the United Kingdom's Turnbull[11] report in a presentation to the State Agency Internal Audit Forum in June 2003.

Texas State Auditor's Office

In their report on *Major Areas of Risk Facing Texas State Government,* (SAO 03-387, 2003, p. 4) the Texas State Auditor's Office recommended these priorities for the 21st century:

- Legislative reforms that strengthen accountability over state resources and enhance performance management and measurement.
- Increase focus on government systems, programs, and agencies at particular risk of fraud, waste, and abuse.
- Pursue organizational systems that reflect evolving fiscal, technological, and workforce dynamics associated with a transition to a knowledge-based economy.

[11] Institute of Chartered Accountants from England and Wales (ICAEW)

These priorities contain components of basic management principles such as accountability, performance management, risk assessment and organizational structure.

Evolution of Internal Control Models

In 1985, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[12] was formed to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. COSO is made up of the following five professional organizations:

- American Institute of Certified Public Accountants (AICPA)
- The Institute of Internal Auditors (IIA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- American Accounting Association (AAA)

Over the years, COSO has issued several reports, two of these reports are discussed in this paper. The first report was the 1992 *Internal Control – Integrated Framework* that provided a definition of internal controls and what components parts were required. The five components of the internal control framework are: control environment, risk assessment, control activities, information, communication and monitoring. The COSO definition of internal control is:

[12] www.coso.org, retrieved April 24, 2004, home page.

> *Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in these categories:*
>
> - *Effectiveness and efficiency of operations.*
> - *Reliability of financial reporting.*
> - *Compliance with applicable laws and regulations.* (COSO 1992 p. 13)

The 1992 COSO *Internal Control – Integrated Framework* is currently the model used for most Sarbanes-Oxley financial internal control reporting. The definition above encompasses basic management principles and implies accountability, performance management, risk assessment and organization. COSO identifies four key concepts in the definition of internal control.

> "First, internal control is a process, internal control does not stop or start, internal control is ongoing. Second, internal control is effected by people, this means people can make internal control happen, conversely, people can also make internal controls fail. Third, internal controls can only provide reasonable assurance, not complete assurance that things are going well. Last, internal control is geared to the achievement of objectives of the organization." (COSO 1992 p. 13)

A second major COSO report came out in 2003 in draft form and was the COSO *Enterprise Risk Management Framework*. This model incorporates all the components of the 1992 COSO *Internal Control – Integrated Framework* and adds emphasis on event identification, risk assessment, risk responses. The need for the expanded model is further described later in this chapter in the section on the two problems in business and government.

The need for this new model is indicated by McNamee's statement "managers are operating in an increasingly complex and global environment, and risk is a central component of corporate governance. The emergence of risk management as a key organizational process gives the internal auditing profession a unique opportunity to shift its focus to risk" (1998, p. 2). McNamee and Selim point out that "managers need to engage in strategic thinking so they can deal with impending threats or take advantage of upcoming opportunities" (1998 p. 1).

The COSO *Enterprise Risk Management Framework* is analyzed and linked to the literature in Chapter 3. A graphic of the model is presented in **Chart 3.1**. Initial professional research on implementation of enterprise risk management occurred in September 2003 when the Institute of Internal Auditor's, Global Auditing Information Network (GAIN) published the results of an electronic survey on enterprise risk management.

In the *Tone at the Top* article titled "Managing Risk from the Mailroom to the Boardroom," it states that the "COSO *Enterprise Risk Management Framework* allows for governance flexibility and judgment" (2003, p. 2). The article states that the framework is anticipated to be a useful tool for management about "the processes and procedures in place to identify, measure, prioritize, and respond to risk" (p. 3). The article also points out that "the Sarbanes-Oxley Act of 2002 made reporting on internal control a requirement" (p. 1).

Other Control Systems – CoCo, Cadbury and Turnbull

The United States is not the only country to develop internal control guidance frameworks. In 1995, the Canadian Institute of Chartered Accountants published the *CoCo*[13] Report. Great Britain issued the Cadbury Report and later issued *Internal Control – Guidance for Directors on the Combined Code* also known as the Turnbull Report. The Turnbull Report (Implementing Turnbull, 1999, p.3) is strikingly similar to

[13] CoCo stands for Criteria of Controls.

the COSO *Enterprise Risk Management Framework* and includes the following guidelines:

- *Obtain management buy-in at all levels of the organization*
- *Identify clear company objectives*
- *Prioritize the risks to the achievement of the objectives*
- *Establish a clear risk to the achievement f the objectives*
- *Establish a clear risk management policy and control strategies*
- *Consult throughout the business*
- *Improve the business culture where appropriate*
- *Monitor continuously*
- *Incorporate Turnbull in your management and governance processes*
- *Aim to obtain business improvement.*

The Turnbull report documents that regulatory and legislative changes are occurring worldwide in the field of reviewing internal controls.

Control Self-Assessment

Control self-assessment (CSA) is a methodology where organizations can assess risk and document control activities that allow organizations to achieve their objectives. The Institute of Internal Auditors defines control self-assessment as "a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met" (Graves *et al* 2003, p. 41). In reviewing the literature, there is a great deal of similarity in the practices and terminology used by the sources.[14]

Control self-assessment has led to a change in the traditional roles of management and audit. Hubbard used the information in Table 2.1 to compare the difference in the

[14] This may be because of its widespread use in the past decade and the sheer volume of literature in the professional journals about the practice. It may also be because of the trends in the profession and the inclusion of these practices in continuing education programs and certification examinations.

assignment of responsibilities under the traditional audit approach and the control self-assessment approach (Graves *et al*, 2003, p. 41 citing Hubbard 2000 p. 5).

Table 2.1: Shifting Responsibilities Traditional Audit Approach vs. The Control Self-Assessment Approach

Responsibilities	Traditional Approach	CSA Approach
Setting business objectives	Management	Management
Assessing risks	Management	Management
Adequacy of internal controls	Management	Management
Evaluating risks and controls	Auditors	Work Teams
Reporting	Auditors	Work Teams
Validate evaluation of risks and controls	Auditors	Auditors
Objectives used	Auditors	Management

Note that the responsibility for setting business objectives, assessing risks and the adequacy of internal controls is a management responsibility under both approaches. Change occurs in responsibility for evaluating risks and controls, reporting and the objectives used. The CSA approach narrows the auditor's responsibility to include only the validation of risks and controls.

The Ottawa Chapter of the Institute of Internal Auditors (Ottawa IIA) sponsored a research study on control self-assessment in 1996. They found that internal controls are a shared responsibility between management and internal audit (1996, p. 1-2). The Ottawa IIA recommends, "CSA's examination of the internal control environment should be conducted within a structured, documented, and repetitive process. This concept of a repetitive process highlights the continuous improvement aspect of CSA. As employees within the process participate in a number of CSA sessions, they will develop ways to improve their business process" (IIA Ottawa, 1996, p. 1-2).

In *Control Self-Assessment: Making the Choice*, Jordan identifies five strategic objectives for control self-assessment (1995, p. 23):

- Self-assessment helps line employees at all levels to assume responsibility and accountability for effective control and risk management.
- Corrective action is more effective because participants "own" results.
- Self-assessment provides broader coverage on important issues.
- Self-assessment improves communication at all levels.
- Self-assessment teaches participants how to analyze and report on internal control.

As noted by Jordan (1995), control self-assessment can be used to assist an organization in evaluating important issues that may not have been previously considered. This can include evaluating internal controls or a specific business processes such as communication between departments. Control self-assessment can be scaled to the level needed to address the issue being addressed from strategic planning to evaluate a specific departmental process. The work team for a control self-assessment evaluation is developed based on getting staff members who actually work with or supervise the process in question. Control self-assessment provides a uniform method for an organization to use in assessing and evaluating a situation or process.

For example, an organization may need to revise its strategic plan on a biennial basis. It can bring executive management together and use a control self-assessment workshop to identify the strategic goals and objectives of the organization. As a second step the group identifies the problems, events or barriers to achieving those objectives. This event identification process is then used to assist management with breaking down each goal and planning to prevent problems from keeping the organization from achieving its goals.

An example of a problem is organizational planning for meeting an objective to ensure that the telephones are answered 24 hours a day, seven days a week. In this case, telephone and computer systems going down or not being accessible is a risk that is not acceptable to management. To manage this risk, the organization needs to have more than one call center, preferably geographically separated by a distance of 50 miles or more[15] so that a regional power outage or severe weather will not impact customer service. Resources, budget and staff are then assigned to implement and test the internal control.

CSA[16] is a technique that management or audit can use to evaluate internal controls. Often CSA is combined with a control model structure such as the COSO *Enterprise Risk Management Framework* to assess the problem against.

Two Problems

Two problems have recently been identified in both business and government that have led to increased concerns about internal controls and governance in organizations. The first is after September 11th many businesses and governmental organizations recognized that they were not prepared for a disaster or business interruption. The second problem is the failure of governance functions in many organizations. Some high profile examples are Enron, WorldCom and Arthur Andersen. In each of these cases, executive management made decisions that were unethical and illegal with major negative impacts on shareholders, employees and public investment markets.

[15] Many business continuity planners recommend that alternate locations be located on a separate power grid.

[16] The most common forms of control self-assessment are workshops with actual users and managers participating. Surveys and document analysis can be used.

Need for Business Continuity Planning

The September 11th terrorist attacks, anthrax in the mail and the recent SARS epidemic have shown both business and government that their continuity planning is incomplete. Many organizations planned for their technology to fail, but did not plan for their people to be unavailable due to quarantine. Brune recommends that audit departments not currently involved in business continuity planning should consider evaluating their processes, especially in light of recent SARS incidents (August 2003, p. 2).

"Internal Auditing and business continuity planning are two key functions in the successful risk management program of an organization" (Kirchner, Ziegenfuss 2003 p. 56). Assessment and management of risk are key components of the COSO *Enterprise Risk Management Framework* referred to later in this paper.

Governance Failures

Funston discusses the governance failures that led to Sarbanes-Oxley Act. "In the aftermath of last year's corporate debacles and governance meltdowns, stakeholders are demanding greater transparency about the risks an enterprise faces and a commensurate level of assurance about the robustness of the organization's risk-management processes and the achievability of its business, reporting, and compliance objectives. Regulators, markets, boards of directors, analysts, and insurers are realizing the importance of managing risk proactively and have introduced many new and far-reaching measures to assist in the effort" (Funston, 2003, p. 59).

Solutions to the Two Problems

Funston offers a solution to the two problems discussed above, the lack of preparedness for disaster or business interruption and the failure of governance functions. Funston maintains that enterprise risk management can allow organizations to "systematically identify potential exposures, take corrective action early, and learn from those actions to better achieve objectives" (Funston, 2003, p. 59). Funston also points out that the definition of "corporate risk has expanded to include not only financial risks but all business and compliance risks. As a result many organizations are implementing enterprise risk management to address this problem" (Funston, 2003, p. 60). Funston also points out that enterprise risk management must be a component part of an organization's strategic planning and decision-making process (Funston, 2003, p. 63).

McNamee (1998. p. 1), a leader in the field of enterprise risk management states, "Both internal audit and risk management are co-evolving with the ascendance of global business risk as a major corporate governance issue". This "co-evolution" has resulted in the business risk self-assessment process discussed in this paper that combines the principles of enterprise risk management and control self-assessment.

The key point of these two problems is for business leaders to see that they are connected. Both business problems due to external disasters and internal corruption can be viewed by the organization as "risks." This is a broadening of the meaning of risk in management. In addition there is a broadening of the meaning and importance of governance – corruption conceptualized as a failure of governance. This recognition of the need to expand management theory and to incorporate emergency management principles, strategic planning principles and internal auditing principles into a comprehensive framework is one reason the COSO *Enterprise Risk Management Framework* was developed. This new concept recognizes that risk events can emerge at any level of the organization and therefore the model needs to be scalable. Additionally, management needs to take responsibility for risk management that deals with both risk management and governance issues including corruption.

The COSO *Enterprise Risk Management Framework* is an expansion of the existing COSO *Internal Control – Integrated Framework* that addresses risk and management in a new way. The model includes existing and accepted internal control principles as well as the expanded roles of risk event identification, risk assessment and risk responses.

Examples in Texas State Government

The next section of the paper describes the activities of two state agencies in implementing enterprise risk management and control self-assessment principles at their agencies.

Texas Commission on Environmental Quality (TCEQ)

In their annual audit plan for fiscal year 2004, Texas Commission on Environmental Quality (TCEQ) presented a proposal to "assist the agency in implementing enterprise-wide business risk management" (TCEQ, 2003, p. 1). The proposal states that the use of business risk management grew out of a need to enhance effective and efficient business process at TCEQ developed by management at a planning retreat in January 2003. TCEQ's model provides agency managers with the tools to systematically oversee their area of responsibility." TCEQ also states that they will build upon recent efforts in business continuity and strategic planning.

The expected benefits for implementing business risk management are to be able to systematically:

- Identify their most important strategic and operational goals;
- Assess the risks related to those goals; and,

- Develop risk mitigation strategies to assure the accomplishment of the goals. (TCEQ, 2003, p. C-1)

The proposal indicates that TCEQ believes that business risk management is a holistic “process that will transform the way TCEQ will perceive and manage risk, and provide reasonable assurance that strategic objectives are being met” (TCEQ, 2003, p. C-6). Executive sponsorship of the initiative occurred when the TCEQ Deputy Executive Director agree to sponsor the initiative. According to Steve Goodson, Internal Audit Director for TCEQ, the project was first piloted and then implemented in January 2004.

Texas State Comptroller of Public Accounts

Graves, Longenecker, Marsh, and Milstead performed a case study of the Texas Comptroller of Public Accounts concerning the use of control self-assessment to implement enterprise risk management. The case study reports that since 2001 “50 risk assessment workshops have been completed and requests for more continue to come in” (Graves et al 2003, p. 43).

The Texas Comptroller of Public Accounts enterprise risk management process is built around risk self-assessment workshops (another term for CSA). The case study reports that a number of important benefits have been achieved from CSA including:

- Expanded employee understanding of their area’s risks and internal controls
- Increased employee involvement in managing risks
- Improved employee understanding of how their key activities are related to the key activities of other employees or work teams
- Discovery of and preparation for new risks before they happen (Graves et al 2003, p. 43)

The case study is summarized with a statement that the “Comptroller has experienced an enhanced management ability to focus on the internal controls that really matter” (Graves et al 2003, p. 43).

Level of Awareness in Texas State Agencies

Graves reported on a second survey sent to 750 members of the Government Finance Officers Association of Texas (GFOA). Only three organizations responded that they used control self-assessment in their jurisdiction. Graves states, "this suggests that either CSA is underutilized by governments of the state of Texas or that it is being used but is known by another name such as enterprise risk management" (Graves et al 2003, p. 43).

The adoption of enterprise risk management combined with control self-assessment techniques at two large agencies in Texas is an indicator that there is some knowledge and acceptance of enterprise risk management.

These results indicate a need for further study in the levels of acceptance and implementation of enterprise risk management in Texas state agencies. The next section of this summarizes the political and regulatory environment.

Summary of the Political and Regulatory Environment

This chapter contains an overview of the political and regulatory environment. Sarbanes-Oxley is leading to increased focus on the internal controls over financial reporting. The U.S. Government Accounting Office has stated its intent that government auditors should report on internal controls in federal agencies. The State of Texas came close to enacting a bill[17] that would have required Texas state agencies to proactively manage risk and report their efforts to an oversight agency. McNamee asserts that internal audit and risk management are evolving to address business risk management as a corporate governance issue (1998, p. 1). When these factors are considered together with the initiatives at the Texas Comptroller of Public Accounts and the Texas

[17] Senate Bill 147, 78th Texas Legislature.

Commission on Environmental Quality, the potential impact on Texas state agencies becomes apparent. The next chapter describes the *COSO Enterprise Risk Management Framework*.

Chapter 3 – Enterprise Risk Management Framework

This chapter discusses the components of the COSO *Enterprise Risk Management Framework*. This model is used to assess the implementation of enterprise risk management principles in Texas state agencies.

Enterprise Risk Management

The COSO *Enterprise Risk Management Framework* was released in 2003 as an exposure draft and contains the components of the 1992 COSO *Internal Control - Integrated Framework*. Enterprise risk management is defined as follows:

> "Enterprise risk management 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[18]

This definition reflects certain fundamental concepts. Enterprise risk management:

- Is a *process* – it's a means to an end, not an end in itself
- Is *effected by people* – it involves people at every level of an organization
- Is *applied in strategy setting*
- Is *applied across the enterprise,* at every level and unit, and includes taking an entity level portfolio view of risks
- Is designed to identify events potentially affecting the entity and manage risk within its *risk appetite*
- Provides *reasonable assurance* to an entity's management and board
- Is geared to the *achievement of objectives* in one or more separate but overlapping categories."

Mahadeva states "a dynamic enterprise risk management strategy requires there are systems in place to make a company more resilient and adaptable to these changes" (2003, p. 6). Mahadeva also discusses that enterprise risk management can be used to balance the needs of all stakeholders in an organization (p. 6).

[18] (COSO, 2003, p. 3)

Osborne and Gaebler, in their popular book *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*, discuss why change is needed in the way organization's function. Old style bureaucracy moves slowly. Bureaucratic government is "slow, inefficient, impersonal" (1992, p.14). Today we are in a different environment, government and what it does has changed over the years. So, logically, government must change how government does what it does.

Benefits of Enterprise Risk Management Framework

The COSO *Enterprise Risk Management Framework* draft document identifies benefits of using enterprise risk management in an organization (COSO, 2003, pages 2-3):

- Align risk appetite and strategy
- Link growth, risk and return
- Enhance risk response decisions
- Minimize operational surprises and losses
- Identify and manage cross-enterprise risks
- Provide integrated responses to multiple risks
- Seize opportunities
- Rationalize capital

The strength of enterprise risk management is that it is a tool that management can modify to use based on the size and complexity of the organization in order to create an effective and efficient process.

The COSO Enterprise Risk Management Framework

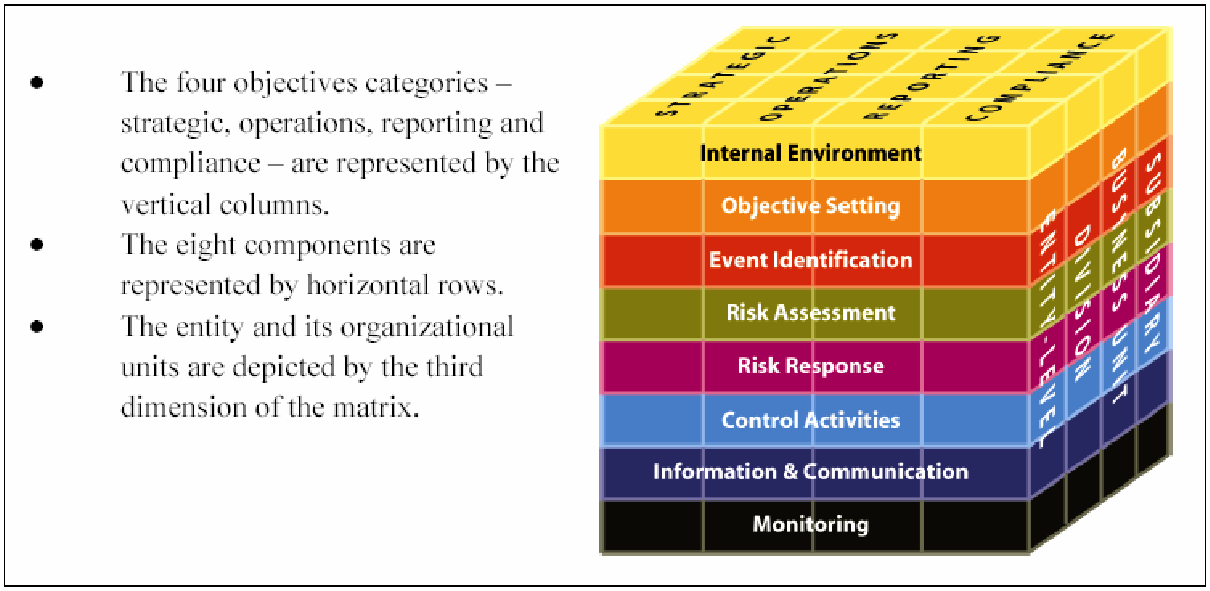
The model used to address the research question - assess the implementation of enterprise risk management principles in Texas state agencies is the new draft COSO *Enterprise Risk Management Framework* model. The COSO *Enterprise Risk Management Framework* (2003) is based on the 1992 COSO *Internal Control - Integrated Framework* and has been enhanced with three additional categories. The

COSO *Enterprise Risk Management Framework* is divided into eight components, four objective categories and four organizational units. The eight components are:

- Internal Environment
- Objective Setting
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communication
- Monitoring

This is shown graphically in the model below.

Chart 3.1 Enterprise Risk Management Framework



- The four objectives categories – strategic, operations, reporting and compliance – are represented by the vertical columns.
- The eight components are represented by horizontal rows.
- The entity and its organizational units are depicted by the third dimension of the matrix.

(Graphic source: COSO ERM model 2003, p. 16)

The model in Chart 3.1 has a cube shape to indicate that it is scalable. An organization can apply the principles in the model from a subsidiary, business unit, or division level focus. The COSO *Enterprise Risk Management Framework* can also be used for strategic planning, operations, reporting or compliance level reporting.

The COSO *Enterprise Risk Management Framework* is useful at programmatic levels as well as enterprise-wide uses. For instance, an agency could implement enterprise risk management techniques on a division-by-division basis and eventually be able to make assessments on an entity-wide level.

Internal Environment[19]

Internal environment is the first component in the COSO *Enterprise Risk Management Framework* and is the overarching theme in internal control development. Internal controls are an integral part of the COSO *Enterprise Risk Management Framework*. The internal environment comprises many sub-components, including an entity's ethical values, competence and development of personnel, management's operating style and assignment of authority and responsibility. The internal environment is often based on "tone at the top" from executive management.

Internal environment is evidenced by the existence of current policies and procedures. The first sub-component of internal environment is risk management philosophy. Simply put this implies that the organization's leadership has a philosophy about risk management and communicates it to the staff. Such a philosophy assists the organization in effectively recognizing and managing risk.

The second sub-component of internal environment is risk appetite, which is the amount of risk the organization is willing to accept without mitigation or managing the risk. The third sub-component of internal environment is the risk culture of the organization. Risk culture is related to risk management philosophy and risk appetite of the organization.

[19] Information in this section is from COSO ERM Exposure Draft, 2003, p. 19-28, Brune, April 2003, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

Other sub-components of internal environment include governance activities of the board of directors; the integrity and ethical values of the organization, the commitment to competence, management's philosophy and operating style, organizational structure, assignment of authority and responsibility, human resources policies and practices, and difference in internal control environment.

In his 2003 article in *Internal Auditor* magazine, Funston discusses the need for an effective control environment by stating "In the aftermath of last year's corporate debacles and governance meltdowns, stakeholders are demanding greater transparency about the risks an enterprise faces and a commensurate level of assurance about the robustness of the organization's risk-management processes and the achievability of its business, reporting, and compliance objectives" (2003, p. 59).

The similarity of the Turnbull Report (Implementing Turnbull, 1999, p.3) to the COSO enterprise risk management document merits a discussion of its own. As mentioned in Chapter 2, the Turnbull Report is an internal control model from Great Britain that contains a great deal of similarity to the COSO *Enterprise Risk Management Framework*. Table 3.2 compares the Turnbull guideline to the COSO *Enterprise Risk Management Framework.*

Table 3.2: Comparison Turnbull Report to the COSO *Enterprise Risk Management Framework*

Turnbull Report	Enterprise Risk Management Framework
Obtain management buy-in at all levels of the organization	Internal Environment
Identify clear company objectives	Objective Setting
Prioritize the risks to the achievement of the objectives	Objective Setting
Establish a clear risk to the achievement of the objectives	Risk Assessment

Turnbull Report	Enterprise Risk Management Framework
Establish a clear risk management policy and control strategies	Internal Environment Event Identification Risk Assessment Risk Responses
Consult throughout the business	Information and Communication
Improve the business culture where appropriate	Internal Environment
Monitor continuously	Monitoring
Incorporate Turnbull in your management and governance processes	Internal Environment
Aim to obtain business improvement.	Objective Setting

Overall the internal environment is the backbone of an organization's policies and procedures and governance style. Without an effective internal environment in place the rest of the model will not function effectively.

Objective Setting[20]

Objective setting is a key concept in management theory. An organization cannot meet an objective that has not been articulated. Within the context of the established mission or vision, management establishes strategic objectives, selects strategy and establishes related objectives, cascading through the enterprise and aligned with and linked to the strategy. For example, a business objective could be a goal to ensure that every telephone call is answered within one minute.

The sub-components for objective setting include strategic objectives, related objectives, selected objectives, risk appetite, and risk tolerance. Strategic objectives are self-explanatory – they are high-level goals that support the mission statement of an organization. Related objectives include operations, reporting, compliance and

[20] Information in this section from COSO ERM Exposure Draft, 2003, p. 29-37, Chabrow, Garvey, 2001, Funston 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

safeguarding of assets. Selected objectives align and support the organization and support management decisions and priorities. Risk appetite and risk tolerance are based on an organization's risk management philosophy and risk culture.

Similarly, the balanced scorecard model expands older financial reporting models and adds indicators of future performance. The model links the organization's vision statement to objectives and measures of performance. The objectives and measures are split into four subgroups: financial, customer, internal business process and learning and growth. These four perspectives are the framework for the balanced scorecard as espoused by Kaplan and Norton (1996, pages 7-8). This viewpoint supports the COSO *Enterprise Risk Management Framework*.

Senge, in his book *The Fifth Discipline,* discusses team learning as the "process of aligning and developing the capacity of a team to create the results its members truly desire" (1990, p. 236). This statement relates to the COSO *Enterprise Risk Management Framework* concept of objective setting.

Osborne and Gaebler also discuss how entrepreneurial government models foster "'competition' and focus on 'results', not rules" (1992, p. 19). Entrepreneurial government doesn't measure results based on the budget, but based on how well the government entity met its goals and objectives (performance measures and outcomes) (p. 19-20). Implementing entrepreneurial government involves flexibility and empowering employees to do things differently in order to better achieve the desired outcomes. This viewpoint supports the premises of the COSO *Enterprise Risk Management Framework.*

Objective setting is the formal process an organization uses to set its mission, goals, and objectives, and as such should be included in the control model. Without planning where the organization is going, the organization cannot assess if it met its goals and objectives. There is an old saying “failing to plan is planning to fail.” Objective setting is the key planning portion of the model that allows the organization to set its objectives.

Event Identification[21]

Event identification can also be called risk event identification. An event is an incident or occurrence flowing from an internal or external factor that could cause a positive or negative impact to the organization. As part of event identification, management considers external and internal factors that affect event occurrence. One example of a risk to the objective identified above – answering the telephone within one minute - would be lack of staff. Management would identify common reasons for there to be a shortage of staff: e.g. hiring difficulties, turnover, illness, or inclement weather.

The sub-components for event identification are positive or negative events, factors influencing strategy and objectives, methodology and techniques, event interdependencies, event categories, and risks and opportunities. The first of these positive or negative events is self-explanatory. The second sub-component, factors influencing strategy and objectives, is also fairly self-explanatory. It includes both internal and external events that could keep the organization from meeting its objectives. The next sub-component, methodologies and techniques, is the way an organization identifies and categorizes event identification. The methodologies and techniques can look both to the future and to the past to identify an event. Event interdependencies

[21] Information in this section from COSO ERM Exposure Draft, 2003, p. 38-46, Brune, August 2003, Chabrow, Garvey, 2001, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

acknowledge that risk events do not happen in a vacuum. One event can trigger another event. Organizational planning should plan for more than one event occurring simultaneously. Event categories assist the agency in managing groups of risks in order to better assess appropriate levels of risk response. Risks and opportunities are other words for negative impact and positive impact of events on an organization.

Funston discusses the importance of event identification and risk responses in the governance process. Funston states, “Using enterprise risk management, organizations can systematically identify potential exposures, take corrective action early, and learn from those actions to better achieve objectives” (2003, p. 59). Event identification and subsequent risk responses are key to assisting the organization in achieving its objectives.

Chabrow and Garvey discuss the importance of risk event identification in light of the tragedy that occurred on September 11th, 2001. “Until September 11, an executive’s worst nightmare might have involved the loss of a key building to fire or a natural disaster such as an earthquake or tornado. But the thought of hundreds of employees dying in a terrorist attack was unfathomable, as was the notion that a single event could indefinitely interrupt such basic business necessities as telecommunications and transportation” (2001, p.38 1/8). This scenario highlights the need for increased focus by business and government on all phases of risk management including components of the COSO *Enterprise Risk Management Framework* risk event identification, risk assessment and risk response (p.38 6-7/8). Chabrow and Garvey also discuss internal environment (p.38 2/8), control activities (p.38 6-7/8), information and communication (p.38 2/8) among management and staff and oversight or monitoring (p.38 6/8) of the plans.

Senate Bill 147 that was enacted by the Legislature and vetoed by the governor during the 78th Texas legislative session would have required state agencies to not only identify risk events, but also assess the likelihood and impact of the risks and adopt risk management strategies. The bill would have also required regular reports on agency risk management activities to an oversight agency. The reason the bill was vetoed was listed as the deleterious impact on small state agencies. However passage of this bill indicates an acceptance of risk management principles in the Texas Legislature.

Event identification is a key management component of overall risk management that allows an organization to identify events that could impact the organization achieving its mission and objectives. This information is then used in assessing the likelihood and impact of the risk in risk assessment and in designing the appropriate risk response to dealing with the risk. These three sections of the COSO *Enterprise Risk Management Framework* are closely interlinked. As a key component of risk management event identification should be included as a component of the control model.

Risk Assessment[22]

Risk assessment enables an organization to put risks in the context of likelihood that the risk will impact the organization achieving its objectives. Risk assessment allows an entity to consider how potential events might affect the achievement of objectives.

To apply risk assessment principles to the example about answering the telephone in the event identification section above, management would first assess the risk of each

[22] Information in this section from COSO ERM Exposure Draft, 2003, p. 47-52, Brune, August 2003, Chabrow, Garvey, 2001, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

of the identified reasons for a shortage of staff. In central Texas, approximately once or twice a year there are ice storms that keep staff members living in remote areas from reporting for work. This inclement weather prevents travel approximately two workdays each year and impacts 25% of the staff. According to COSO model, management should assess the event from two perspectives: likelihood and impact.

The sub-components for risk assessment include: inherent and residual risk, likelihood and impact, methodologies and techniques, and correlation. The first sub-component inherent and residual risks are the risks associated with managing risk. Inherent risk is the risk of not taking action to manage a risk. Residual risk is the risk to the organization that remains after an action has occurred to manage a risk. The second sub-component is likelihood and impact. Likelihood is the possibility that something will occur. Impact represents the effect that the event occurred. The third sub-component, methodology and techniques, is the qualitative and quantitative methods that organizations use to analyze risk. The last sub-component in the risk assessment section is correlation. Correlation is management's analysis of how risk events work together when sequences of events occur together. This can include testing scenarios or stress testing organizational structure to locate the weak points.

As noted above, Senate Bill 147 from the 78th Texas Legislature would have required state agencies to assess the likelihood and impact of the risks. Similarly, the balanced scorecard model recognizes that organizations should balance expected returns with management and control of risk. Many organizations include objectives in their financial perspective that addresses the risk dimension of their strategy. In general, the balanced scorecard concept uses risk management as an overlay or an additional objective that complements the strategy the business unit has chosen (Kaplan, Norton, 1996, pages 50-51).

Risk Assessment is a key management component and should be included as a component of the control model. It allows management to document in a standardized manner the likelihood and impact of an event occurring that was identified in the event identification section of the model.

Risk Response[23]

Risk response is how management plans to respond to various risk events. Management identifies risk response options and considers their effect on event likelihood and impact, in relation to risk tolerances and costs versus benefits, and designs and implements response options.

Using the example about telephone answering above, management develops a plan or risk response to use in the case of inclement weather. This could entail adding a message to an automated telephone answering system that explains the inclement weather conditions impacting the workforce and advising callers that there is a longer than usual wait time – this same system could route callers who can wait to either leave a message or call back in a few days when the weather improves. Another strategy could be to bring in workers from other departments who do not usually answer the phones to answer questions that they can answer and to take call back information for questions they cannot answer. Risk responses need to be evaluated on a cost/benefit basis. Is the cost of the risk response appropriate for the level of loss to the organization if the event occurs?

[23] Information in this section from COSO ERM Exposure Draft, 2003, p. 53-59, Brune, August 2003, Chabrow, Garvey, 2001, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

The sub-components involved in risk response are: identify risk responses; evaluate possible risk responses, select responses, iterative process, and portfolio view. The first sub-component identifies risk response as avoidance, reduction, sharing or acceptance. These are the only actions management can take in responding to risk. The second sub-component, to evaluate the possible risk responses, to pick the risk response with the result of achieving a residual risk in accordance with the organization's risk culture and risk tolerance. Evaluating possible risk responses to inherent risk requires consideration of risks resulting from the response itself. This may prompt an iterative process where management, before finalizing a decision, considers the risk arising from the response itself. The third sub-component is to select the risk response. Selecting the risk response is the action of making a decision to reduce anticipated risk likelihood and impact. The fourth sub-component is portfolio view. Portfolio view requires each department to assess risks individually. Executive management uses this information to balance overall risks to the organization. Use of portfolio view may result in a negative impact to one department, but will result in an overall reduced impact to the organization as a whole.

Brune describes the need to test risk responses in her August 2003 article on "Protecting People". Brune states that audit groups should consider evaluating the business continuity plan, especially in light of the SARS epidemic (p. 2). This article ties the need to have three components of the COSO *Enterprise Risk Management Framework* event identification, risk assessment and risk response documented in a business continuity plan. As noted above, Senate Bill 147 from the 78th Legislature would have required state agencies to adopt risk management strategies. Funston (p. 62) has an in-depth discussion of risk management including the need for risk management policy, event identification, and risk planning (response). Funston (pgs. 62-63) also discusses the importance of communicating the plan across the organization. “The right information needs to get to the right people at the right time” (p. 62).

Risk responses are the activities that address risks identified in event identification and assessed in risk assessment above. These three components are interrelated and when applied in a balanced manner ensure that the organization is responding to risks in a planned manner, and as such all three components should be included in the control model. Considerations in applying risk responses are the event likelihood and impact, the risk tolerances and costs/benefit of applying the risk response.

Control Activities[24]

Control activities are also referred to as internal controls or management controls. Control activities are the policies and procedures that help ensure risk responses are properly executed. They usually involve two components: a policy establishing what should be done, and procedures to implement the policy (COSO, 2003, p. 12).

In the telephone-answering example above, the control activities could include performing additional training of staff who might be called upon to answer the telephones in the event of inclement weather. Based on cost/benefit analysis, control activities to manage the risk of inclement weather could involve use of a remote work location where employees who live in another area can go to perform their job duties close to their homes.

[24] Information in this section from COSO ERM Exposure Draft, 2003, p. 60-67, Brune, August 2003, Chabrow, Garvey, 2001, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

There are five sub-components associated with control activities. They are: integration with risk response, types of control activities, controls over information systems (e.g. general controls and application controls), and entity-specific controls. The first sub-component, integration with risk response, relates to building controls directly into management practices. The second sub-component, types of control activities, encompasses policies, procedures, preventative controls, detective controls, manual controls and automatic controls. The third sub-component, general controls, relates to controls over information technology systems. The fourth sub-component, application controls, include controls over computer or manually generated data: completeness, accuracy, authorization and validity. The fifth sub-component is entity-specific and encompasses strategies and objectives, operating environment, and the complexity of the organization.

Similarly, in using the balanced scorecard, management control systems are established to ensure that the organization's management and staff operate in compliance with the plan established by senior management (Kaplan, Norton, 1996, page 16).

Brune describes the control environment in public companies in her April 2003 article. Brune states "The U.S. Securities and Exchange Commission (SEC) has defined disclosure controls as, "controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files under the Exchange Act is recorded, processed, summarized and reported, within the time periods specified in the [SEC's] rules and forms" (pages 1-2). Brune describes both internal environment as well as control activities components of the COSO *Enterprise*

Risk Management Framework. The control activities are steps taken in the internal environment to ensure compliance with SEC rules.

Key control activities, which include both the policy to achieve and the procedures to implement the policy, are a key component of any management system and should be included in the control model.

Information and Communication[25]

Information and communication means that pertinent information is captured and relayed to individuals who need it to perform their jobs. Pertinent information from internal and external sources must be identified, captured and communicated in a form and within a timeframe that enable personnel to carry out their responsibilities.

In the telephone-answering example above, there are several forms of information and communication that must occur. First of all, the plan to deal with the identified event must have been communicated to employees. If inclement weather is expected, employees need to know if there is a telephone number or their supervisor to call to know whether or not they are required to report to work. Additionally, there needs to be a process in place to ensure that critical functions are appropriately supervised in the event of absence of normal supervisors. If answering telephone calls is a higher priority than processing cases, and inclement weather keeps a large enough portion of the call-taking staff from reporting, then there needs to be a mechanism to identify the best alternative call responders from other departments and notify them of their temporary reassignment.

[25] Information in this section from COSO ERM Exposure Draft, 2003, p. 68-78, Chabrow, Garvey, 2001, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

The sub-components of information and communication are information, strategic and integrated systems and communication. The first sub-component, information, includes all types of information including internal, external, manual, computerized, formal, informal, and information system architecture. The second sub-component, strategic and integrated systems, encompasses the type of information: strategic, operational, past and current, level of detail, timeliness and quality. The third sub-component communication includes internal, external, entity-wide, expectation and responsibilities, framing and means of transmission.

Communication and Information are key components of management theory. The balanced scorecard model provides a basis for communicating and gaining commitment to the organization's strategy between different management layers in the organization (Kaplan, Norton, 1996, page 13). Senge asserts that the "first leadership design task concerns developing vision, values, and purpose or mission" (1990, p. 343) of the organization. These are methods of communicating the organization's orientation to the entire staff of an organization. Similarly, Funston refers to the communication of risks as a "risk nervous system" (2003, p. 61). Information and communication are key management tools in managing any organization and as such are key components of the COSO *Enterprise Risk Management Framework*. Methods must be in place to ensure that relevant information from internal and external sources must be identified, captured and communicated to staff to allow them to perform their jobs.

Monitoring[26]

Monitoring is a process that assesses the presence and functioning of enterprise risk management concepts over time. Ongoing and separate monitoring ensures that enterprise risk management continues to be applied at all levels and across the entity. Monitoring is a normal, ongoing management activity. Each situation needs to be monitored, and after the risk event occurs an "after action report" needs to be compiled and reviewed. The question should always be asked, "How could the organization respond better next time?" If errors occurred, they should be identified and addressed.

The sub-components of monitoring include ongoing, separate evaluations and reporting deficiencies. The first sub-component, ongoing monitoring, includes real-time, built-in and day-to-day operational monitoring. The second sub-component, separate evaluations, includes the scope, frequency, self-assessments, internal audit and the extent of documentation in a unit. The third sub-component is reporting deficiencies. This includes: ongoing reporting, reporting to external parties, reporting protocols and alternate channels of reporting.

If internal environment is the overarching theme of the COSO *Enterprise Risk Management Framework*, then monitoring is the most important management component in the COSO *Enterprise Risk Management Framework*. Failure to monitor is an invitation to fraud and errors occurring. In the context of contract monitoring, Osborne and Gaebler discuss the issue of accountability using steering and rowing metaphors. "Steering requires people who see the entire universe of issues and possibilities and can

[26] Information in this section from COSO ERM Exposure Draft, 2003, p. 79-87, Chabrow, Garvey, 2001, COSO, 1992, Funston, 2003, Kaplan, Norton, 1996, Osborne, Gaebler, 1992, Senge, 1990, Texas SAO, 2003, Turnbull, ICAEW, 1999, Tex. S.B. 147, 78th Leg. R.S. (2003).

balance competing demands for resources. Rowing requires people who focus intently on one mission and perform it well" (1992, p. 35). What Osborne and Gaebler imply is that competition and flexibility allow managers to respond to change and require accountability for quality performance. This is a method of monitoring.

Monitoring is the final key component of any management structure and should be included in the control model. If no one verifies information or holds staff accountable for reaching objectives then there is no method of determining if objectives were really met. Monitoring must be in place at all levels of the organization on an ongoing basis to ensure the organization's objectives are met.

Conceptual Framework

Table 3.3 links the concepts in the COSO *Enterprise Risk Management Framework* to the literature. As noted, there is considerable consensus in the literature about the components of an internal control framework and control activities. This is evidenced by the spectrum of the literature in the table supporting the concepts. The literature types include a nearly enacted bill from the 78th Texas Legislature, a law in Great Britain, and joint committee research reports and journal articles. This breadth and depth of support serve to validate the concepts in the model.

Table 3.3: Linking the COSO *Enterprise Risk Management Framework* to the Literature

Characteristics of the COSO *Enterprise Risk Management Framework*	**Literature Source**
Internal Environment[27] includes: • Risk Management Philosophy • Risk Appetite • Board of Directors • Organizational Structure • Assignment of Authority and Responsibility	COSO ERM Exposure Draft, 2003, p. 19-28 Brune, April 2003. COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)
Objective Setting[28] includes: • Strategic Objectives • Related Objectives includes ○ Operating Objectives ○ Reporting Objectives ○ Compliance Objectives • Risk Appetite • Risk Tolerances	COSO ERM Exposure Draft, 2003, p. 29-37 Chabrow, Garvey, 2001 Funston 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)
Event Identification includes: • Risk Event Identification • Factors Influencing Strategy and Objectives • Event Identification Methodologies and Techniques • Event Interdependencies • Event Categories • Distinguishing Risks and Opportunities	COSO ERM Exposure Draft, 2003, p. 38-46 Brune, August 2003 Chabrow, Garvey, 2001 COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)

[27] Risk Culture, Integrity and Ethical Values of the Organization, Commitment to Competence, Management's Philosophy and Operating Style, Human Resource Policies and Practices, and Difference in Environment and Their Implication are other components of Internal Environment that are not contained in the survey.

[28] Selected Objectives is another component of Objective Setting that is not contained in the survey.

Characteristics of the COSO *Enterprise Risk Management Framework*	**Literature Source**
Risk Assessment includes: - Context for Risk Assessment - Inherent and Residual Risk - Estimating Likelihood and Impact - Qualitative and Quantitative Methodologies and Techniques - Correlation of Events	COSO ERM Exposure Draft, 2003, p. 47-52 Brune, August 2003 Chabrow, Garvey, 2001 COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)
Risk Response includes: - Identify Risk Responses - Evaluating Possible Risk Responses - Selected Responses - Iterative Process - Portfolio View	COSO ERM Exposure Draft, 2003, p. 53-59 Brune, August 2003 Chabrow, Garvey, 2001 COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)
Control Activities[29] includes: - Types of Control Activities - Controls over Information Systems o General Controls o Application Controls - Entity Specific	COSO ERM Exposure Draft, 2003, p. 60-67 Brune, August 2003 Chabrow, Garvey, 2001 COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)

[29] Integration with Risk Response is another component of Control Activities that is not included in the survey.

Characteristics of the COSO *Enterprise Risk Management Framework*	**Literature Source**
Information and Communication includes: - Information - Strategic and Integrated Systems - Communication	COSO ERM Exposure Draft, 2003, p. 68-78 Chabrow, Garvey, 2001 COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)
Monitoring includes: - Separate Evaluations - Ongoing Evaluations - Reporting Deficiencies	COSO ERM Exposure Draft, 2003, p. 79-87 Chabrow, Garvey, 2001 COSO, 1992 Funston, 2003 Kaplan, Norton, 1996 Osborne, Gaebler, 1992 Senge, 1990 Texas SAO, 2003 Turnbull, ICAEW, 1999 Tex. S.B. 147, 78th Leg. R.S. (2003)

As indicated in the literature reviewed in Table 3.3 above, the eight components of the COSO *Enterprise Risk Management Framework* are components of general management theory. For example, Kaplan and Norton (2001) state that the balanced scorecard approach to management theory provides a framework to analyze the strategy for value creation from four perspectives: financial, customer, internal business process and learning and growth. The balanced scorecard method is about setting objectives, developing criteria and measuring performance in organizations.

Peter Drucker has written extensively about management theory. In a compendium of his works published in 2001 he addresses the three tasks of management:

- Establishing the specific purpose and mission of the institution
- Making work productive and the worker effective
- Managing social impacts and social responsibilities (p. 34)

While these three tasks of management don't tie directly to the eight components of the COSO model, the first task is the second component of the COSO *Enterprise Risk Management Framework* - objective setting. In this same book, Drucker devotes an entire chapter to this topic (pages 112-126). The message of this chapter is that management should have the information they need to manage their own performance and receive it in a timely manner to effect change necessary to achieve desired results (p.122). This in effect uses other components of the COSO *Enterprise Risk Management Framework* like monitoring and information and communication.

Osborne and Gaebler note that governments need to be accountable to their citizens. Accordingly decentralized government entities have to "articulate their missions, create internal cultures around their core values, and measure results" (Osborne, Gaebler, 1992, p. 254). These steps are similar to the concepts in both the COSO *Enterprise Risk Management Framework* and the balanced scorecard model.

The examples above indicate that the COSO *Enterprise Risk Management Framework* is linked to general management theory development over time. The COSO *Enterprise Risk Management Framework* is not something new; it is based on solid management principles and is just a new way of coordinating them into one integrated model.

Summary of the Enterprise Risk Management Framework

All of the components in the COSO *Enterprise Risk Management Framework* are based on tried and true management theory in the common body of knowledge. Over time these components appear and reappear in slightly different forms in management and accounting literature as well as management theories. As shown in this chapter, the components of the model may be organized differently, but the meaning stays constant.

The COSO *Enterprise Risk Management Framework* can be considered an ideal management control system because it encompasses the full range of components necessary to manage risk and assist an organization in achieving its objectives. It encompasses the financial internal control systems required by Sarbanes-Oxley as well as components that address risk management on all levels of an organization. The model is scalable and can be used to assess a small part of an organization or the entire organization as a whole.

The next chapter discusses the methodology used to address the research question, the GAIN survey used as the benchmark, the administration of the survey to Texas state agencies, and the interpretation of the results of the survey.

Chapter 4 - Methodology

This chapter describes the methodology used to answer the research purpose – to assess the implementation of COSO *Enterprise Risk Management Framework* principles in Texas state agencies against the Global Auditing Information Network (GAIN) survey performed by the *Internal Auditor* magazine. The GAIN survey response is used as a benchmark to assess the implementation status of Texas state agencies. The survey was provided to the internal audit directors of Texas state agencies through the State Agency Internal Audit Forum[30]. Approximately 40 agencies[31] were identified as possible respondents, 15 state agencies responded, a 38% response rate.

Survey Development and Use of GAIN Survey as a Benchmark

The Global Auditing Information Network (GAIN) is a service provided by the Institute of Internal Auditors. GAIN provides its members with a fast method of surveying chief audit executives (CAE) throughout the world. The GAIN survey for *Internal Auditor* magazine was posted on August 25, 2003 and 5,433 invitations to respond were sent out to CAEs meeting the criteria given by the surveyor. A total of 381 (7% response rate) responses were received. Because of the newness of the COSO *Enterprise Risk Management Framework,* the GAIN survey results provided the best and most convenient benchmark to use to measure the implementation of COSO *Enterprise*

[30] The study and survey were presented at the January 16, 2004 State Agency Internal Audit Forum (SAIAF) meeting with a follow up request sent out on the SAIAF list serve. Several follow up messages were sent to the SAIAF list serve to enhance survey response.

[31] The possible respondents included the health and human service agencies, which were undergoing consolidation. Most health and human service agencies were unable to fill out the survey, which reduced the response rate of the survey.

Risk Management Framework principles. The Institute of Internal Auditors has approximately 90,000 members worldwide.

Linking the Survey Questions to the Conceptual Framework

When comparing the GAIN survey[32] to the model in Table 3.3 it is evident that the GAIN survey is not a completely accurate representation of the COSO *Enterprise Risk Management Framework* because the GAIN survey does not include all the components and the sub-components of the model. Table 4.1 connects each question in the GAIN survey to a recognized management principle in the COSO *Enterprise Risk Management Framework.*

Table 4.1: Operationalization: Linking the Survey Questions to the Conceptual Framework – Internal Environment[33]:

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Risk Management Philosophy	A1 - The organization views risk management as a means of preserving and creating value. A2 - There is an overall risk management policy set out in a board-approved statement. A6 - Managers and personnel at all levels are involved in periodic review or planning exercises, which lead them to identify, source and quantify risks.

[32] Contact with *Internal Auditor* magazine editor indicates that two practitioners prepared the survey with extensive experience in enterprise risk management.

[33] Risk Culture, Integrity and Ethical Values of the organization, Commitment to Competence, Management's Philosophy and Operating Style, Human Resource Policies and Practices, and Difference in Environment and Their Implication are other components of Internal Environment that are not contained in the survey.

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
- Board of Directors	A3 - The board considers risk management a regular part of its oversight agenda. A4 - The board constructively engages management on plans and performance.
- Risk Appetite	A5 - The organizations attitude and approach to risk is clear and consistent with the level of risk (appetite) it is prepared to take.
- Assignment of Authority and Responsibility	A7 - There is a senior management committee that oversees risk management.
- Organizational Structure	A8 - There is a senior executive responsible for risk management

Table 4.2: Operationalization: Linking the Survey Questions to the Conceptual Framework – Objective Setting[34]

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
- Strategic Objectives	B1- The organization defines goals and objectives for the enterprise as a whole. B2 - An effective strategic planning process is in place to formulate strategies that will enable the organization to achieve its business objective.
- Related Objectives o Operating Objectives o Reporting Objectives o Compliance Objectives	B3 - Business strategies are clearly articulated with objectives linked to each.

[34] Selected Objectives is another component of Objective Setting that is not contained in the survey.

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
- Risk Appetite	B4 - The risk identification process is designed to make a clear link between the organization's objectives and the associated risks. B5- Risk to the achievement of objectives is evaluated to ensure it does not exceed the levels of risk determined by the Board as acceptable.
- Risk Tolerances	B6- Acceptable tolerance limits on the risk to the achievement of key objectives have been determined. B7 - Management uses meaningful performance measures in monitoring results against other set tolerances.

Table 4.3: Operationalization: Linking the Survey Questions to the Conceptual Framework – Event Identification

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
- Factors Influencing Strategy and Objectives	C1 - Data on the business operating environment – political, economic, etc., events is captured and regularly evaluated in terms of their potential impact upon the organization's business objectives. C3 - Events are linked to and risk evaluated by individual objective.
- Risk Event Identification	C2 - A portfolio of events that could affect the achievement of objectives – internal and external – has been prepared. C5- Responsibilities and accountables for risk identification are clearly defined and understood.

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Event Identification Methodologies and Techniques	C4 - Goals and objectives for identifying events and the related risks exist and are communicated to all segments of the organization.
• Event Interdependencies	C6 - Risk is considered in terms of not just isolated events but also inter-related events.
• Event Categories	C7 - Events are categorized into useful groups to facilitate the aggregation of information for purposes of assessing risks.
• Distinguishing Risks and Opportunities	C8 - The organization evaluates events in the context of the potential upsides (opportunities) as well as the downside (risks).

Table 4.4: Operationalization: Linking the Survey Questions to the Conceptual Framework – Risk Assessment

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Context for Risk Assessment	D1 - Prior to assessing risks, management examines the impact of potential future events relevant to its business (i.e. entity size, complexity of operation, degree of regulation, etc.).
• Inherent and Residual Risk	D2 - Risk is considered in terms of both inherent and residual risk.

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Estimating Likelihood and Impact	D3- Key risks are considered within a standard framework, e.g. likelihood and consequences of risk occurring. D5 - Management gives consideration to both near term risk impacts as well as those that are further out in time which impact strategic direction. D6 - Appropriate methodologies are in place to allow the organization to measure the impact of identified risks on objectives with some degree of accuracy. D7 - The costs (including resources allocated) and benefits of risk mitigation are taken into account in the evaluation of risk acceptability. D8 - There is a periodic review process to ensure that the organization's risk assessments remain current.
• Qualitative and Quantitative Methodologies and Techniques	D4 - Risk assessment criteria, e.g. likelihood, are articulated and applied consistently.
• Correlation of Events	D9 - Scenario analysis techniques are used to assess the potential impact of events combining.

Table 4.5: Operationalization: Linking the Survey Questions to the Conceptual Framework – Risk Response

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Identify Risk Responses	E1 - The full range of available risk management options – avoid, reduce, share, accept – is considered when formulating risk responses.

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
- Selected Responses	E2 - When considering alternative responses, management considers the impact on risk significance and likelihood.
- Evaluating Possible Risk Responses	E3 - Alternative responses are evaluated in terms of the resulting costs and benefits.
- Iterative Process	E4 - There are clear guidelines as to how decisions following on from risk assessment are to be made and at what level.
- Portfolio View	E5 - The organization measures risk management outcomes or results.

Table 4.6: Operationalization: Linking the Survey Questions to the Conceptual Framework – Control Activities [35]

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
- Types of Control Activities	F1 - There is an appropriate balance of preventative and detective controls in place, with emphasis on preventative controls when appropriate. F2- Controls are considered in terms of efficiency as well as effectiveness.
- Controls over Information Systems o General Controls o Application Controls	F3 - Control activities include effective controls over information technology management, information technology infrastructure, security management, software development and maintenance. F4 - Controls are effective in ensuring the completeness, accuracy and validity of data processed.

[35] Integration with Risk Response is another component of Control Activities that is not included in the survey.

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Entity Specific	F5 - Management considers the impact of significant organizational, structural or managerial changes on risk, risk responses and the related control activities before implementing them.

Table 4.7: Operationalization: Linking the Survey Questions to the Conceptual Framework – Information and Communication

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Information	G1 - Appropriate information is identified and captured to identify, assess and respond to risk and manage the business, obtained from appropriate internal and external sources, generated manually and electronically and is in appropriate formal and informal formats.
• Strategic and Integrated Systems	G2 - Information is provided for decision-making at the appropriate depth and with the appropriate timeliness. G3 - Information quality is evaluated in terms of e.g., level of detail of the content – Timeliness, Currency, Reliability, Accessibility, and Level of Detail.
• Communication	G4 - There are clear upward lines of communication to report risk incidents. G5 - Communications in the organization, both formal and informal, are effective in raising the risk awareness.

Table 4.8: Operationalization: Linking the Survey Questions to the Conceptual Framework – Monitoring

Characteristics of the COSO Enterprise Risk Management Framework	Survey Questions
• Separate Evaluations	H5 - Process and risk owners periodically self assess their performance and report the results of their self-assessment upward to appropriate managers.
• Ongoing Evaluations	H1 - The required information is available to allow for proper monitoring of risk throughout the company. H3 - A monitoring process is built into the execution of the business process. H4 - Day-to-day monitoring takes place daily through ongoing supervision and oversight.
• Reporting Deficiencies	H2 - Appropriate real time ongoing monitoring processes are in place to measure performance and provide early warning or detect and report deviations from established norms immediately to the appropriate managers.

Benchmarking Criteria

The results of the survey in Appendix 2 contain raw response data (frequency counts only). For comparability to the GAIN survey these results have been converted into a percentage of responses for each question in Chapter 5. For the purpose of this study, the GAIN survey responses are considered to be the benchmark to assess the level of implementation of each component of the model. There are five possible responses to the survey:

1. Don't Know
2. Disagree – Not Happening or no Plans
3. Planned – Will be Introduced

4. Partly Agree – In Place Localized Only
5. Fully Agree – In Place Enterprise Wide

For the purpose of this study the evaluation concentrates on the percentage responses for "fully agree" and "partly agree" only. This determination was made only to evaluate the differences in the percentages of "fully agree" and "partly agree" responses. Both responses indicate a positive level of acceptance of the principles of COSO *Enterprise Risk Management Framework*.

Chapter 6 takes the assessment one step further and assesses the risk to Texas state agencies based on the criteria in Table 6.1. Tables 6.2 – 6.9 assess the responses of Texas state agencies for each of the 52 questions and determine if the item surveyed is "high", "medium" or "low" risk to Texas state agencies. There were nine (18%) responses rated as "high" risk and 26 (50%) responses rated as "low" risk to Texas state agencies.

Survey Administration

The survey of Texas State agencies was administered to a small group of internal audit directors from the State Agency Internal Audit Forum (SAIAF). Approximately 25 state agencies[36] were represented at the January 16, 2004 SAIAF meeting where the survey and research project were presented. The survey was also sent out to on the SAIAF listserv, which includes internal audit directors from all Texas state agencies. Fifteen surveys were returned to the researcher. This is approximately a 38% response rate of the target population.

[36] Based on a review of the State Auditor's Office internal audit contact list, there are a total of about 40 entities (not including higher education) that could participate in the survey.

Internal Audit Directors at several agencies involved in the health and human service consolidation stated that they declined to participate in the survey because of the organizational changes caused by the consolidation. A compilation of the results of the survey is presented in Appendix 2. Survey respondents were allowed to respond anonymously. Five of the responses were anonymous. Survey respondents were also asked to identify their agency by size, and they reported:

Table 4.9 Agency Size[37] of Survey Respondents

Size of Agency	Number of Responses
Small	3
Medium	8
Large	4
Total Number of Responses	**15**

Limitations of the Study

The limited population and response rate is a significant limitation to this study. As such, no statistical significance should be placed on the results of this survey. It is merely an indicator of the responses of the 15 respondents and not a true, overall assessment of all Texas state agencies. Another limitation of the study was the unanticipated impact of health and human service agencies consolidation on the total number of survey respondents. The small number of survey results may mask biased survey responses. The survey may overstate the use of COSO *Enterprise Risk Management Framework* principles in Texas state agencies because only those agencies that are implementing portions of the model may have responded to the survey. The GAIN survey may contain limitations. For example, the organizations that responded

[37] Agency size is determined in general by two factors - number of employees (FTE's) and budget size. For instance, according to HB 2485, small agencies have a budget of less than $10 million per year and/or less than 100 employees. The large agencies are generally considered to be 16 agencies that are members of the State Agency Coordinating Board, which includes TxDOT, TYC, TEA, TWC, TDPS, TDCJ, TCEQ, and TBPC.

may be more heavily weighted toward organizations that are implementing enterprise risk management. These limitations should be considered in evaluating the results of the survey.

Summary of Methodology

The methodology chapter discussed the Global Auditing Information Network (GAIN) survey. The GAIN survey was administered to Texas state agencies, and fifteen Texas state agencies, responded to the survey. The limitations of the survey were discussed in this chapter. The next chapter presents the results of the survey.

Chapter 5 – Results

This chapter presents the results of the survey. The responses appear according to the component and sub-component of the COSO *Enterprise Risk Management Framework,* and a narrative reviews the survey responses for each section. The results are presented by the components and sub-components from the Conceptual Framework in Table 4.1. The overall results are summarized in Table 5.9. The assessment is based on the total of the percentage of "partly agree" and "fully agree" responses to the survey questions, comparing the Texas state agency responses and the GAIN survey responses.

As noted in Chapter 4 – Methodology, only fifteen (38%) of the agencies eligible to participate in the survey responded to the survey. Appendix 2 contains the survey responses by question. These responses indicate 59% of the Texas state agencies surveyed responded positively, on average, to the survey questions. Similarly, these responses indicate 56% of the GAIN organizations surveyed responded positively, on average, to the survey questions. As noted in the methodology chapter, these results are presented for comparison purposes only and are not statistically relevant. The GAIN survey also indicates a slightly smaller percentage of "don't know" responses and a much larger percentage of "planned to be implemented" responses. Detailed comparisons based on percentage of positive responses per question are presented below. Appendix 3 contains graphical comparisons for each survey question. The graphical comparisons highlight the differences between Texas state agencies responses and GAIN agency responses.

Internal Environment

Acceptance of the COSO *Enterprise Risk Management Framework* component Internal Environment is measured by survey responses to questions regarding five sub-components. Table 5.1 shows the results of the internal environment section of the survey. The table indicates that 57% of responding Texas state agencies responded that they “partly agree” or “fully agree” that internal environment principles are implemented in their agency. This percentage is within 5% of the 54% reported for GAIN organizations.

Table 5.1: Comparison of Survey Results for Internal Environment

Characteristics of the Internal Environment of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Risk Management Philosophy			
Risk management preserves and creates value.	80%	68%	12%
Organization has a formal risk management policy.	20%	38%	-18%
Management and staff involvement in assessing risk.	73%	48%	25%
Average Risk Management Philosophy	58%	51%	7%
Board of Directors			
Board level involvement in risk management.	40%	58%	-18%
Board level involvement in planning.	67%	75%	-8%
Average Board of Directors	54%	67%	-13%
Risk Appetite			
Organization has a consistent approach to acceptable risk levels.	80%	56%	24%
Assignment of Authority and Responsibility			
Senior management committee oversees risk.	40%	44%	-4%
Organizational Structure			
Senior executive oversees risk.	53%	47%	6%
Average Internal Environment	57%	54%	3%

Objective Setting

Acceptance of the COSO *Enterprise Risk Management Framework* component Objective Setting is measured by survey responses to questions regarding four sub-components. Table 5.2 shows the results of the objective setting section of the survey. The table indicates that 60% of Texas state agencies indicate that they "partly agree" or "fully agree" that objective setting principles are implemented in their agency. This percentage is within 5% of the 59% reported for GAIN organizations.

Table 5.2: Comparison of Survey Results for Objective Setting

Characteristics of the Objective Setting component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Strategic Objectives			
Organization defines enterprise-wide goals and objectives.	93%	88%	5%
An effective strategic planning process is in place.	80%	85%	-5%
Average Strategic Objectives	87%	87%	0%
Related Objectives			
Business strategies are clearly stated and linked with objectives.	73%	77%	-4%
Risk Appetite			
Risk identification process links objectives and the associated risks.	60%	45%	15%
Risks are evaluated to ensure they do not exceed acceptable levels of risk.	20%	39%	-19%
Average Risk Appetite	40%	42%	-2%
Risk Tolerances			
Acceptable tolerance limits on the risk to the achievement of key objectives have been determined.	20%	35%	-15%
Management uses meaningful performance measures in monitoring results.	73%	46%	27%
Average Risk Tolerance	47%	41%	6%
Average Objective Setting	60%	59%	1%

Event Identification

Acceptance of the COSO *Enterprise Risk Management Framework* component Event Identification is measured by survey responses to questions regarding six sub-components. Table 5.3 shows the results of the event identification section of the survey. The table indicates that 51% of Texas state agencies indicate that they “partly agree” or “fully agree” that event identification principles are implemented in their agency. This percentage is higher than the 44% reported for GAIN organizations.

Table 5.3: Comparison of Survey Results for Event Identification

Characteristics of the Event Identification component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Factors Influencing Strategy and Objectives			
Data on the business operating environment is evaluated in terms of their potential impact upon the organization’s business objectives.	71%	72%	-1%
Events are linked to risk and evaluated by individual objective.	43%	35%	8%
Average Factors Influencing Strategy and Objectives	57%	54%	3%
Risk Event Identification			
A portfolio of events that could affect the achievement of objectives – internal and external – has been prepared.	50%	42%	8%
Responsibilities and accountability for risk identification are clearly defined and understood.	50%	39%	11%
Average Risk Event Identification	50%	41%	9%
Event Identification Methodologies and Techniques			
Goals and objectives for identifying events and the related risks exist and are communicated to the organization.	36%	31%	5%
Event Interdependencies			
Risk is considered in terms of isolated and inter-related events.	62%	45%	17%
Event Categories			
Events are categorized into groups to assessing risks.	36%	36%	0%
Distinguishing Risks and Opportunities			
Events are evaluated for both potential upsides (opportunities) as well as downsides (risks).	57%	55%	2%
Average Event Identification	51%	44%	7%

Risk Assessment

Acceptance of the COSO *Enterprise Risk Management Framework* component Risk Assessment is measured by survey responses to questions regarding five sub-components. Table 5.4 shows the results of the risk assessment section of the survey. The table indicates that 59% of Texas state agencies indicate that they "partly agree" or "fully agree" that risk assessment principles are implemented in their agency. This percentage is higher than the 50% reported for GAIN organizations.

Table 5.4: Comparison of Survey Results for Risk Assessment

Characteristics of the Risk Assessment component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Context for Risk Assessment			
Management examines the impact of potential future events.	73%	64%	9%
Inherent and Residual Risk			
Risk is considered in terms of both inherent and residual risk.	67%	55%	12%
Estimating Likelihood and Impact			
Key risks are considered within a standard framework.	73%	56%	17%
Management considers both near term and long term risk impacts.	80%	61%	19%
Methodologies are in place to allow the organization to measure the impact of identified risks.	53%	38%	15%
The costs and benefits of risk mitigation are taken into account in the evaluation of risk acceptability.	47%	50%	-3%
There is a periodic review process to ensure that the organization's risk assessments remain current.	47%	49%	-2%
Average Estimating Likelihood and Impact	60%	51%	9%
Qualitative and Quantitative Methodologies and Techniques			
Risk assessment criteria, e.g. likelihood, are articulated and applied consistently.	53%	47%	6%

Characteristics of the Risk Assessment component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Correlation of Events			
Scenario analysis techniques are used to assess the potential impact of events combining.	40%	29%	11%
Average Risk Assessment	59%	50%	9%

Risk Response

Acceptance of the COSO *Enterprise Risk Management Framework* component Risk Response is measured by survey responses to questions regarding five sub-components. Table 5.5 shows the results of the risk response section of the survey. The table indicates that 47% of Texas state agencies indicate that they “partly agree” or “fully agree” that risk response principles are implemented in their agency. This percentage is within 5% of the 46% reported for GAIN organizations.

Table 5.5: Comparison of Survey Results for Risk Response

Characteristics of the Risk Response component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Identify Risk Responses			
The full range of available risk management options is considered when formulating risk responses.	47%	50%	-3%
Selected Responses			
When considering alternative responses, management considers the impact on risk significance and likelihood.	60%	60%	0%
Evaluating Possible Risk Responses			
Alternative responses are evaluated in terms of the resulting costs and benefits.	47%	60%	-13%

Characteristics of the Risk Response component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Iterative Process			
Clear guidelines exist about risk assessment decision making.	40%	29%	11%
Portfolio View			
The organization measures risk management outcomes or results.	40%	32%	8%
Average Risk Response	47%	46%	1%

Control Activities

Acceptance of the COSO *Enterprise Risk Management Framework* component Control Activities is measured by survey responses to questions regarding three sub-components. Table 5.6 shows the results of the control activities section of the survey. The table indicates that 76% of Texas state agencies indicate that they "partly agree" or "fully agree" that control activities principles are implemented in their agency. This percentage is within 5% of the 78% reported for GAIN organizations.

Table 5.6: Comparison of Survey Results for Control Activities

Characteristics of the Control Activities component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Types of Control Activities			
There is a balance of preventive and detective controls in place.	73%	80%	-7%
Controls are considered in terms of efficiency as well as effectiveness.	87%	81%	6%
Average Types of Control Activities	80%	81%	-1%
Controls over Information Systems			
Control activities include effective controls over information technology.	87%	82%	5%

Characteristics of the Control Activities component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Controls are effective in ensuring the completeness, accuracy and validity of data processed.	80%	85%	-5%
Average Controls over Information Systems	84%	84%	0%
Entity Specific			
Management considers the impact of changes on risk management before implementing the changes.	53%	63%	-10%
Average Control Activities	76%	78%	-2%

Information and Communication

Acceptance of the COSO *Enterprise Risk Management Framework* component information and communication is measured by survey responses to questions regarding three sub-components. Table 5.7 shows the results of the information and communication section of the survey. The table indicates that 61% of Texas state agencies indicate that they “partly agree” or “fully agree” that information and communication principles are implemented in their agency. This percentage is within 5% of the 65% reported for GAIN organizations.

Table 5.7: Comparison of Survey Results for Information and Communication

Characteristics of the Information and Communication component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Information			
Appropriate information is identified and captured to identify, assess and respond to risk and manage the business.	53%	64%	-11%
Strategic and Integrated Systems			

Characteristics of the Information and Communication component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Timely information is provided for decision-making at the appropriate depth.	67%	71%	-4%
Information quality is evaluated in terms of the level of detail of the content.	60%	62%	-2%
Average Strategic and Integrated Systems	64%	67%	-3%
Communication			
There are clear upward lines of communication to report risk incidents.	60%	66%	-6%
Communications in the organization are effective in raising the risk awareness.	67%	61%	6%
Average Communication	64%	64%	0%
Average Information and Communication	61%	65%	-4%

Monitoring

Acceptance of the COSO *Enterprise Risk Management Framework* component Monitoring is measured by survey responses to questions regarding three sub-components. Table 5.8 shows the results of the monitoring section of the survey. The table indicates that 68% of Texas state agencies indicate that they “partly agree” or “fully agree” that monitoring principles are implemented in their agency. This percentage is higher than the 56% reported for GAIN organizations.

Table 5.8: Comparison of Survey Results for Monitoring

Characteristics of the Monitoring component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies - Partly Agree Plus Fully Agree (15 responses) %**	**GAIN Survey - Partly Agree Plus Fully Agree (381 responses) %**	**Difference Between Texas State Agencies and GAIN Survey %**
Separate Evaluations			
Process and risk owners use self-assessment and report the results of their self-assessment to appropriate managers.	53%	39%	14%
Ongoing Evaluations			
Information is available to allow for monitoring of risk throughout the company.	67%	57%	10%
A monitoring process is built into the execution of the business process.	67%	59%	8%
Day-to-day monitoring takes place daily through ongoing supervision and oversight.	80%	75%	5%
Average Ongoing Evaluations	71%	64%	7%
Reporting Deficiencies			
Real time ongoing monitoring processes are in place.	73%	52%	21%
Average Monitoring	68%	56%	12%

Summary of Results

Table 5.9 summarizes the results of the survey of Texas state agencies and the GAIN survey. The results indicate, on average, a slightly higher amount of acceptance of enterprise risk management principles. However, due to the small sample size, these results are not statistically valid. The results suggest that enterprise risk management principles are in place in Texas state agencies in similar percentages as the GAIN survey respondent organizations.

Table 5.9: Summary of the Assessment of Status of Texas State Agencies Implementation of Enterprise Risk Management Principles

Components of the COSO *Enterprise Risk Management Framework*	**Assessment**	**Texas State Agencies (% Of Responses)**	**GAIN Survey (% Of Responses)**
Internal Environment	Within + 5%	57%	54%
Objective Setting	Within + 5%	60%	59%
Event Identification	Higher	51%	44%
Risk Assessment	Higher	59%	50%

Components of the COSO *Enterprise Risk Management Framework*	**Assessment**	**Texas State Agencies (% Of Responses)**	**GAIN Survey (% Of Responses)**
Risk Response	Within + 5%	47%	46%
Control Activities	Within - 5%	76%	78%
Information and Communication	Within - 5%	61%	65%
Monitoring	Higher	68%	56%
Overall Assessment	Within + 5%	**59%**	**56%**

The individual results in each component and sub-component point to subtle differences in the way Texas state agencies are implementing principles of enterprise risk management compared to GAIN survey organizations. Chapter 6 will identify several areas for improvement in Texas state agencies in areas where Texas state agencies are implementing COSO *Enterprise Risk Management Framework* principles at a lower rate than GAIN agencies.

Chapter 6 – Recommendations and Conclusion

This chapter includes an overall conclusion about the status of implementation of enterprise risk management principles in Texas state agencies. Table 6.1 shows how each survey question was evaluated. For each question, responses appear as high or low-risk to the State of Texas. There were nine survey responses that fell into the highest risk category for Texas state agencies. Overall the results indicate that Texas state agencies are implementing enterprise risk management principles at a similar rate to other organizations as compared to the Institute of Internal Auditors GAIN survey.

Complete results are in Tables 6.2 – 6. 9. As noted in prior chapters, the low response rate of Texas state agencies means that the results are not statistically significant. However, they do indicate a trend. The results of both the Texas state agency and GAIN survey may be biased because agencies that are implementing principles of enterprise risk management may have been more inclined to participate in the surveys.

Table 6.1: Evaluation Criteria[38]

Priority Level	**Criteria**	**Number**	**Percentage**
High Priority	Texas is lower than GAIN, positive response rate is less than 50%	9	17%
Medium Priority	Texas is higher than GAIN, positive response rate is less than 50% Or Texas is lower than GAIN, positive response rate is higher than 50%	17	33%
Low Priority	Texas is higher than GAIN, positive response rate is higher than 50%	26	50%

[38] Responses that fell within +/- 5% are evaluated for high, medium or low priority based on the Texas percentage being higher or lower than the GAIN responses.

Table 6.2: Internal Environment

Characteristics of the Internal Environment of the COSO *Enterprise Risk Management Framework* and Survey Questions	Texas State Agencies vs. GAIN Survey	Texas has at least a 50% positive response rate?	Priority Level
Risk Management Philosophy			
Risk management preserves and creates value.	Higher	Yes	Low
Organization has a formal risk management policy.	**Lower**	**No**	**High**
Management and staff involvement in assessing risk.	Higher	Yes	Low
Board of Directors			
Board level involvement in risk management.	**Lower**	**No**	**High**
Board level involvement in planning.	Lower	Yes	Medium
Risk Appetite			
Organization has a consistent approach to acceptable risk levels.	Higher	Yes	Low
Assignment of Authority and Responsibility			
Senior management committee oversees risk.	**Within - 5%**	**No**	**High**
Organizational Structure			
Senior executive oversees risk.	Higher	Yes	Low
Average Internal Environment	Within + 5%	Yes	Low

The results in Table 6.2 for internal environment indicate three areas of high concern for Texas state agencies. These include a need for a formal agency-wide risk management policy, board level involvement in risk management activities, and formation of a senior management committee with the responsibility for overseeing risk management. Texas state agencies should consider these issues when assessing the overall agency internal environment.

Table 6.3: Objective Setting

Characteristics of the Objective Setting component of the COSO *Enterprise Risk Management Framework* and Survey Questions	Texas State Agencies vs. GAIN Survey	Texas has at least a 50% positive response rate?	Priority Level
Strategic Objectives			
Organization defines enterprise-wide goals and objectives.	Within + 5%	Yes	Low
An effective strategic planning process is in place.	Within - 5%	Yes	Medium
Related Objectives			
Business strategies are clearly stated and linked with objectives.	Within - 5%	Yes	Medium

Characteristics of the Objective Setting component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Risk Appetite			
Risk identification process links objectives and the associated risks.	Higher	Yes	Low
Risks are evaluated to ensure they do not exceed acceptable levels of risk.	**Lower**	**No**	**High**
Risk Tolerances			
Acceptable tolerance limits on the risk to the achievement of key objectives have been determined.	**Lower**	**No**	**High**
Management uses meaningful performance measures in monitoring results.	Higher	Yes	Low
Average Objective Setting	Within + 5%	Yes	Low

The results in Table 6.3 for objective setting indicate two areas of high concern for Texas state agencies. These include methods for evaluating risks and assessing risk tolerance. Texas state agencies should consider these issues when assessing the overall objective setting process.

Table 6.4: Event Identification

Characteristics of the Event Identification component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Factors Influencing Strategy and Objectives			
Data on the business operating environment is evaluated in terms of their potential impact upon the organization's business objectives.	Within - 5%	Yes	Medium
Events are linked to risk and evaluated by individual objective.	Higher	No	Medium
Risk Event Identification			
A portfolio of events that could affect the achievement of objectives – internal and external – has been prepared.	Higher	Yes	Low
Responsibilities and accountability for risk identification are clearly defined and understood.	Higher	Yes	Low
Event Identification Methodologies and Techniques			
Goals and objectives for identifying events and the related risks exist and are communicated to the organization.	Within + 5%	No	Medium
Event Interdependencies			
Risk is considered in terms of isolated and inter-related events.	Higher	Yes	Low
Event Categories			
Events are categorized into groups to assessing risks.	Within + 5%	No	Medium

Characteristics of the Event Identification component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Distinguishing Risks and Opportunities			
Events are evaluated for both potential upsides (opportunities) as well as downsides (risks).	Within + 5%	Yes	Low
Average Event Identification	Higher	Yes	Low

The results in Table 6.4 for event identification indicate no areas of high concern for Texas state agencies.

Table 6.5: Risk Assessment

Characteristics of the Risk Assessment component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Context for Risk Assessment			
Management examines the impact of potential future events.	Higher	Yes	Low
Inherent and Residual Risk			
Risk is considered in terms of both inherent and residual risk.	Higher	Yes	Low
Estimating Likelihood and Impact			
Key risks are considered within a standard framework.	Higher	Yes	Low
Management considers both near term and long-term risk impacts.	Higher	Yes	Low
Methodologies are in place to allow the organization to measure the impact of identified risks.	Higher	Yes	Low
The costs and benefits of risk mitigation are taken into account in the evaluation of risk acceptability.	**Within - 5%**	**No**	**High**
There is a periodic review process to ensure that the organization's risk assessments remain current.	**Within - 5%**	**No**	**High**
Qualitative and Quantitative Methodologies and Techniques			
Risk assessment criteria, e.g. likelihood, are articulated and applied consistently.	Higher	Yes	Low
Correlation of Events			
Scenario analysis techniques are used to assess the potential impact of events combining.	Higher	No	Medium
Average Risk Assessment	Higher	Yes	Low

The results in Table 6.5 for risk assessment indicate two areas of high concern for Texas state agencies. These include cost/benefit analysis of risk mitigation and the review process for risk assessment. Texas state agencies should consider these issues when assessing the overall risk assessment process.

Table 6.6: Risk Response

Characteristics of the Risk Response component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Identify Risk Responses			
The full range of available risk management options is considered when formulating risk responses.	**Within - 5%**	**No**	**High**
Selected Responses			
When considering alternative responses, management considers the impact on risk significance and likelihood.	Within + 5%	Yes	Low
Evaluating Possible Risk Responses			
Alternative responses are evaluated in terms of the resulting costs and benefits.	**Lower**	**No**	**High**
Iterative Process			
Clear guidelines exist about risk assessment decision-making.	Higher	No	Medium
Portfolio View			
The organization measures risk management outcomes or results.	Higher	No	Medium
Average Risk Response	Within + 5%	No	Medium

The results in Table 6.6 for risk response indicate two areas of high concern for Texas state agencies. These include a consideration of the full range of responses in risk management planning and evaluating alternative responses based on cost/benefit criteria. Texas state agencies should consider these issues when assessing the overall risk response process.

Table 6.7: Control Activities

Characteristics of the Control Activities component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Types of Control Activities			
There is a balance of preventive and detective controls in place.	Lower	Yes	Medium
Controls are considered in terms of efficiency as well as effectiveness.	Higher	Yes	Low

Characteristics of the Control Activities component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Controls over Information Systems			
Control activities include effective controls over information technology.	Within + 5%	Yes	Low
Controls are effective in ensuring the completeness, accuracy and validity of data processed.	Within - 5%	Yes	Medium
Entity Specific			
Management considers the impact of changes on risk management before implementing the changes.	Lower	Yes	Medium
Average Control Activities	Within - 5%	Yes	Medium

The results in Table 6.7 for control activities indicate no areas of high concern for Texas state agencies.

Table 6.8: Information and Communication

Characteristics of the Information and Communication component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Information			
Appropriate information is identified and captured to identify, assess and respond to risk and manage the business.	Lower	Yes	Medium
Strategic and Integrated Systems			
Timely information is provided for decision-making at the appropriate depth.	Within - 5%	Yes	Medium
Information quality is evaluated in terms of the level of detail of the content.	Within - 5%	Yes	Medium
Communication			
There are clear upward lines of communication to report risk incidents.	Lower	Yes	Medium
Communications in the organization are effective in raising the risk awareness.	Higher	Yes	Low
Average Information and Communication	Within - 5%	Yes	Medium

The results in Table 6.8 for information and communication indicate no areas of high concern for Texas state agencies.

Table 6.9 Monitoring

Characteristics of the Monitoring component of the COSO *Enterprise Risk Management Framework* and Survey Questions	**Texas State Agencies vs. GAIN Survey**	**Texas has at least a 50% positive response rate?**	**Priority Level**
Separate Evaluations			
Process and risk owners use self-assessment and report the results of their self-assessment to appropriate managers.	Higher	Yes	Low
Ongoing Evaluations			
Information is available to allow for monitoring of risk throughout the company.	Higher	Yes	Low
A monitoring process is built into the execution of the business process.	Higher	Yes	Low
Day-to-day monitoring takes place daily through ongoing supervision and oversight.	Within + 5%	Yes	Low
Reporting Deficiencies			
Real time ongoing monitoring processes are in place.	Higher	Yes	Low
Average Monitoring	Higher	Yes	Low

The results in Table 6.9 for monitoring indicate no areas of high concern for Texas state agencies.

Summary of Recommendations and Conclusions

Two large Texas state agencies are implementing COSO *Enterprise Risk Management Framework* principles. Due to the small number of survey results, statistically relevant conclusions cannot be drawn about the status of implementation of enterprise risk management principles in Texas state agencies as compared to the Institute of Internal Auditors GAIN survey.

The results in Table 5.9 suggest that Texas state agencies who responded to the survey are implementing COSO *Enterprise Risk Management Framework* principles at a similar rate to organizations that responded to the GAIN survey. As noted in Tables 6.1 – 6.8, there are nine areas that are a high-risk to Texas state agencies. The nine high-risk areas are:

- ♦ Organization has a formal risk management policy.

- Board level involvement in risk management.
- Senior management committee oversees risk.
- Risks are evaluated to ensure they do not exceed acceptable levels of risk.
- Acceptable tolerance limits on the risk to the achievement of key objectives have been determined.
- The costs and benefits of risk mitigation are taken into account in the evaluation of risk acceptability.
- There is a periodic review process to ensure that the organization's risk assessments remain current.
- The full range of available risk management options is considered when formulating risk responses.
- Alternative responses are evaluated in terms of the resulting costs and benefits.

Texas state agencies should consider these issues when assessing overall risk management and in policymaking decisions for Texas state agencies. The lack of a formal risk management policy is the most important risk for Texas state agencies to address. A formal policy assigns roles and responsibilities and provides criteria to use in assessing implementation of policy.

Additional research is needed in this area to further determine the applicability and usefulness of COSO *Enterprise Risk Management Framework* principles to Texas state agencies. This study is a snapshot assessment for a small group of Texas state agencies. It would be useful to study the implementation of COSO *Enterprise Risk Management Framework* principles over time.

Another potentially useful area of possible research would be to assess the current status of health and human service agencies use of the COSO *Enterprise Risk Management Framework* principles and monitor it over time. The consolidation of the Texas health and human service agencies requires a high degree of organizational change. The consolidation of the health and human service agencies is very high-risk to Texas because it impacts a large number of residents of the state and affects a large dollar amount of public funds.   Funston points out that “Increased vulnerability typically is associated with a high degree of change in the operating and regulatory environment, personnel, processes, or systems…” (Funston, 2003, p. 60). Monitoring the risk management activities during the period of change could assist decision makers in managing the risk associated with the consolidation of the health and human service agencies.

Bibliography

A Perspective on Control Self-Assessment, Professional Practices Pamphlet 98-2, Institute of Internal Auditors, Altamonte Springs, Florida, 2002.

Brune, Christina, "Exploring New Territory,*" AuditWire*, Institute of Internal Auditors, Vol. 25, Number 2, March/April 2003, pages 1-2.

Brune, Christina, "Protecting People," *AuditWire,* Institute of Internal Auditors, Vol. 25, Number 4, July/August 2003, pages 1-2.

Chabrow, Eric and Martin J. Garvey, "Playing for Keeps -- Business continuity and disaster recovery have soared in importance since Sept. 11th. Is your company ready for the unexpected?" *Information Week*, 2001, p. 38[39].

Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management Framework*, Exposure Draft for Public Comment, www.erm.coso.org, 2003.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control – Integrated Framework.* 1992.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) website www.coso.org, home page, retrieved April 24, 2004.

Cushing, Karl, "When Disaster Strikes," *Computer Weekly*, March 28, 2002, p. 2001.[40]

Drucker, Peter F., *The Essential Drucker,* HarperCollins, 2001.

Funston, Rick, "Creating a Risk-Intelligent Organization," *Internal Auditor Magazine*, April 2003, Vol. LX: 11, pages 59-63.

Gauthier, Stephen J., *Evaluating Internal Controls: A Local Government Manager's Guide* Chicago, Illinois, GFOA, 1996.

Global Auditing Information Network (GAIN), Institute of Internal Auditors, www.gain2.org.

Graves, Sharon M., Bill Longenecker, Treba L. Marsh, and Heidi Milstead, "Evaluating Internal Controls: Control Self-Assessment in Government," *Government Finance Review,* Vol. 19, No. 3, June 2003, pages 40 – 45.

[39] Article obtained from the Internet. Page numbers will not be correct – 8 printed pages.

[40] Article obtained from the Internet. Page numbers will not be correct – 7 printed pages.

Hubbard, L, *Control Self-Assessment: A Practical Guide,* Institute of Internal Auditors, Altamonte Springs, Florida, 2000.

IIA Ottawa Chapter, Arthur Anderson LLP, *Control Self-Assessment: Experience, Current Thinking, and Best Practices,* Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida, 1996.

Implementing Turnbull: A Boardroom Briefing, Center for Business Performance, The Institute of Chartered Accountants in England and Wales 1999.

Internal Control – Guidance for Directors on the Combined Code, Institute of Chartered Accountants in England and Wales, 1999

Institute of Internal Auditors, Global Auditing Information Network (GAIN), www.gain2.org. A web based survey tool sponsored by the IIA.

Institute of Internal Auditors, *The Professional Practices Framework*, January 2004, www.theiia.org.

Institute of Internal Auditors, *The Sarbanes-Oxley Act of 2002: Summary of Key Provisions of Interest to Internal Auditor* online publication www.theiia.org.

Jordan, Glenda S., *Control Self-Assessment: Making the Choice*, Institute of Internal Auditors, Altamonte Springs, Florida, 1995.

Kaplan, Robert S. and David P. Norton, *The Balanced Scorecard*, Harvard Business School Publishing Corporation, Boston, 1996.

Kaplan, Robert S. and David P. Norton, *The Strategy-Focused Organization*, Harvard Business School Publishing Corporation, Boston, 2001.

Kirchner, Terri A., and Douglas E. Ziegenfuss, "Audit's Role in the Business Continuity Process," *Disaster Recovery Journal*, Spring 2003, pages 56-60.

Mahadeva, Mano "Enterprise Risk Management – A Holistic Approach to Risk Management," *Today's CPA*, September/October 2003, page 6.

"Managing Risk from the Mailroom to the Boardroom", *Tone at the Top*, Institute of Internal Auditors, 2003, pages 1-3.

McNamee, David, and Georges M. Selim, *Risk Management: Changing the Internal Auditor's Paradigm*, The Institute of Internal Auditors, Altamonte Springs, Florida, 1998

McNamee, David, *Business Risk Assessment*, The Institute of Internal Auditors, Altamonte Springs, Florida, 1998

Osborne, David and Ted Gaebler, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector,* Plume, Penguin Books, New York, 1992.

Senge, Peter M., *The Fifth Discipline: The Art & Practice of The Learning Organization*, Bantam Doubleday Dell, New York, 1990.

Shields, Patricia M., "The Community of Inquiry: Classical Pragmatism and Public Administration," *Administration and Society*, November 2003, pages 510-538.

Shields, Patricia M., "A Pragmatic Teaching Philosophy", *Journal of Public Affairs Education*, 2003, pages 7-12.

Tex. S.B. 147, 78th Leg., R.S. (2003)

Texas Commission on Environmental Quality, Office of Internal Audit, *The TCEQ FY 2004/2005 Biennial Audit Plan*, October 2003, Report 03-111.

Texas State Auditor's Office, *State Auditor's Report on Major areas of Risk Facing Texas State Government*, January 2003, Report 03-387 www.sao.state.tx.us

Texas State Board of Public Accountancy, "Looking at Sarbanes-Oxley," *Board Report*, October 2003, Vol. 80, pages 1-5.

Thomas, William "The Trials and Tribulations of Sarbanes-Oxley 404," *Today's CPA*, November/December 2003, page 7.

United States General Accounting Office, *Government Auditing Standards*, June 2003.

Appendix 1 - Survey Document

Following is the survey document that was sent to Texas State Agencies.

SURVEY QUESTIONS:

Agency Name (optional): ______________________________________
Contact information (optional):__________________________________
Agency Size (mark one/required): small medium large

1. If your agency is using enterprise risk management or control self-assessment, please give an example of a typical project.

2. If your agency has decided not to use enterprise risk management or control self-assessment please describe the process that was used to make the decision.

(Please mark one box per question with an "**X**")

Survey Question	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned - Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise-Wide**
A – Internal Environment					
1. The organization views risk management as a means of preserving and creating value.					
2. There is an overall risk management policy set out in a board approved statement.					
3. The board considers risk management a regular part of its oversight agenda.					
4. The board constructively engages management on plans and performance.					
5. The organizations attitude and approach to risk is clear and consistent with the level of risk (appetite) it is prepared to take.					

Survey Question	Don't Know	Disagree – Not Happening or No Plans	Planned - Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise-Wide
6. Managers and personnel at all levels are involved in periodic review or planning exercises, which lead them to identify, source and quantify risks.					
7. There is a senior management committee that oversees risk management.					
8. There is a senior executive responsible for risk management.					
B- Objective Setting					
1. The organization defines goals and objectives for the enterprise as a whole.					
2. An effective strategic planning process is in place to formulate strategies that will enable the organization to achieve its business objective.					
3. Business strategies are clearly articulated with objectives linked to each.					
4. The risk identification process is designed to make a clear link between the organization's objectives and the associated risks.					
5. Risk to the achievement of objectives is evaluated to ensure it does not exceed the levels of risk determined by the Board as acceptable.					
6. Acceptable tolerance limits on the risk to the achievement of key objectives have been					

Survey Question	Don't Know	Disagree – Not Happening or No Plans	Planned - Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise-Wide
determined.					
7. Management uses meaningful performance measures in monitoring results against other set tolerances.					
C – Event Identification					
1. Data on the business operating environment – political, economic, etc., events is captured and regularly evaluated in terms of their potential impact upon the organization's business objectives.					
2. A portfolio of events that could affect the achievement of objectives – internal and external – has been prepared.					
3. Events are linked to and risk evaluated by individual objective.					
4. Goals and objectives for identifying events and the related risks exist and are communicated to all segments of the organization.					
5. Responsibilities and accountables for risk identification are clearly defined and understood.					
6. Risk is considered in terms of not just isolated events but also inter-related events.					
7. Events are categorized into useful groups to facilitate the aggregation of information					

Survey Question	Don't Know	Disagree – Not Happening or No Plans	Planned - Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise-Wide
for purposes of assessing risks.					
8. The organization evaluates events in the context of the potential upsides (opportunities) as well as the downside (risks).					
D – Risk Assessment					
1. Prior to assessing risks, management examines the impact of potential future events relevant to its business (i.e. entity size, complexity of operation, degree of regulation, etc.).					
2. Risk is considered in terms of both inherent and residual risk.					
3. Key risks are considered within a standard framework, e.g. likelihood and consequences of risk occurring.					
4. Risk assessment criteria, e.g. likelihood, are articulated and applied consistently.					
5. Management gives consideration to both near term risk impacts as well as those that are further out in time which impact strategic direction.					
6. Appropriate methodologies are in place to allow the organization to measure the impact of identified risks on objectives with some degree of accuracy.					

Survey Question	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned - Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise-Wide**
7. The costs (including resources allocated) and benefits of risk mitigation are taken into account in the evaluation of risk acceptability.					
8. There is a periodic review process to ensure that the organization's risk assessments remain current.					
9. Scenario analysis techniques are used to assess the potential impact of events combining.					
E – Risk Response					
1. The full range of available risk management options – avoid, reduce, share, accept – is considered when formulating risk responses.					
2. When considering alternative responses, management considers the impact on risk significance and likelihood.					
3. Alternative responses are evaluated in terms of the resulting costs and benefits.					
4. There are clear guidelines as to how decisions following on from risk assessment are to be made and at what level.					
5. The organization measures risk management outcomes or results.					
F – Control Activities					

Survey Question	Don’t Know	Disagree – Not Happening or No Plans	Planned - Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise-Wide
1. There is an appropriate balance of preventative and detective controls in place, with emphasis on preventative controls when appropriate.					
2. Controls are considered in terms of efficiency as well as effectiveness.					
3. Control activities include effective controls over information technology management, information technology infrastructure, security management, software development and maintenance.					
4. Controls are effective in ensuring the completeness, accuracy and validity of data processed.					
5. Management considers the impact of significant organizational, structural or managerial changes on risk, risk responses and the related control activities before implementing them.					
G – Information and Communication					
1. Appropriate information is identified and captured to identify, assess and respond to risk and manage the business, obtained from appropriate internal and external sources, generated					

Survey Question	Don't Know	Disagree – Not Happening or No Plans	Planned - Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise-Wide
manually and electronically and is in appropriate formal and informal formats.					
2. Information is provided for decision-making at the appropriate depth and with the appropriate timeliness.					
3. Information quality is evaluated in terms of e.g., level of detail of the content – Timeliness, Currency, Reliability, Accessibility, Level of Detail.					
4. There are clear upward lines of communication to report risk incidents.					
5. Communications in the organization, both formal and informal, are effective in raising the risk awareness.					
H – Monitoring					
1. The required information is available to allow for proper monitoring of risk throughout the company.					
2. Appropriate real time ongoing monitoring processes are in place to measure performance and provide early warning or detect and report deviations from established norms immediately to the appropriate managers.					
3. A monitoring process is built into the execution of the business process.					

Survey Question	Don't Know	Disagree – Not Happening or No Plans	Planned - Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise-Wide
4. Day-to-day monitoring takes place daily through ongoing supervision and oversight.					
5. Process and risk owners periodically self assess their performance and report the results of their self-assessment upward to appropriate managers.					

Appendix 2 - Complete Survey Results

Following are tables containing a summary of the number of responses in each category for Texas State Agencies. The agencies were allowed to respond anonymously to the survey and the 15 respondents identified the agency size as

- Small agency – 3 responses
- Medium size agency – 8 responses
- Large size agency – 4 responses

Internal Environment

Section A – Internal Environment Survey Questions	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
A 1. The organization views risk management as a means of preserving and creating value.	0	3	0	5	7	15
A 2. There is an overall risk management policy set out in a board approved statement.	2	9	1	1	2	15
A 3. The board considers risk management a regular part of its oversight agenda.	1	6	2	1	5	15
A 4. The board constructively engages management on plans and performance.	1	4	0	3	7	15
A 5. The organizations attitude and approach to risk is clear and consistent with the level of risk (appetite) it is prepared to take.	0	3	0	8	4	15
A 6. Managers and personnel at all levels are involved in periodic review or planning exercises, which lead them to identify, source and quantify risks.	0	4	0	7	4	15
A 7. There is a senior management committee that oversees risk management.	1	7	1	2	4	15

A 8. There is a senior executive responsible for risk management.	1	6	0	0	8	15
Section Total	6	42	4	27	41	120

Objective Setting

Section B – Objective Setting Survey Questions	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
B 1. The organization defines goals and objectives for the enterprise as a whole.	0	1	0	1	12	14
B 2. An effective strategic planning process is in place to formulate strategies that will enable the organization to achieve its business objective.	0	3	0	3	9	15
B 3. Business strategies are clearly articulated with objectives linked to each.	0	4	0	2	9	15
B 4. The risk identification process is designed to make a clear link between the organization's objectives and the associated risks.	1	3	2	8	1	15
B 5. Risk to the achievement of objectives is evaluated to ensure it does not exceed the levels of risk determined by the Board as acceptable.	2	8	2	2	1	15
B 6. Acceptable tolerance limits on the risk to the achievement of key objectives have been determined.	1	8	3	1	2	15
B 7. Management use meaningful performance measures in monitoring results against other set tolerances.	1	2	1	5	6	15
Section Total	5	29	8	22	40	104

Event Identification

Section C – Event Identification Survey Questions	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
C 1. Data on the business operating environment – political, economic, etc., events is captured and regularly evaluated in terms of their potential impact upon the organization's business objectives.	1	2	1	4	6	14
C 2. A portfolio of events that could affect the achievement of objectives – internal and external – has been prepared.	2	4	1	5	2	14
C 3. Events are linked to and risk evaluated by individual objective.	1	5	2	6	0	14
C 4. Goals and objectives for identifying events and the related risks exist and are communicated to all segments of the organization.	2	6	1	4	1	14
C 5. Responsibilities and accountables for risk identification are clearly defined and understood.	1	5	1	4	3	14
C 6. Risk is considered in terms of not just isolated events but also inter-related events.	0	4	1	4	4	13
C 7. Events are categorized into useful groups to facilitate the aggregation of information for purposes of assessing risks.	2	6	1	3	2	14
C 8. The organization evaluates events in the context of the potential upsides (opportunities) as well as the downside (risks).	1	4	1	4	4	14
Section Total	10	36	9	34	22	111

Risk Assessment

Section D – Risk Assessment Survey Questions	Don't Know	Disagree – Not Happening or No Plans	Planned- Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise Wide	Total Number of Responses per Question
D 1. Prior to assessing risks, management examines the impact of potential future events relevant to its business (i.e. entity size, complexity of operation, degree of regulation, etc.).	2	2	0	5	6	15
D 2. Risk is considered in terms of both inherent and residual risk.	2	3	0	6	4	15
D 3. Key risks are considered within a standard framework, e.g. likelihood and consequences of risk occurring.	0	4	0	4	7	15
D 4. Risk assessment criteria, e.g. likelihood, are articulated and applied consistently.	2	4	1	3	5	15
D 5. Management gives consideration to both near term risk impacts as well as those that are further out in time which impact strategic direction.	0	2	1	6	6	15
D 6. Appropriate methodologies are in place to allow the organization to measure the impact of identified risks on objectives with some degree of accuracy.	2	4	1	5	3	15
D 7. The costs (including resources allocated) and benefits of risk mitigation are taken into account in the evaluation of risk acceptability.	3	5	0	2	5	15
D 8. There is a periodic review process to ensure that the organization's risk assessments remain current.	1	5	2	3	4	15
D 9. Scenario analysis techniques are used to assess the potential impact of events combining.	3	6	0	4	2	15

Section Total	15	35	5	38	42	135

Risk Response

Section E – Risk Response Survey Questions	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
E 1. The full range of available risk management options – avoid, reduce, share, accept – is considered when formulating risk responses.	2	5	1	2	5	15
E 2. When considering alternative responses, management considers the impact on risk significance and likelihood.	1	4	1	5	4	15
E 3. Alternative responses are evaluated in terms of the resulting costs and benefits.	1	5	2	3	4	15
E 4. There are clear guidelines as to how decisions following on from risk assessment are to be made and at what level.	2	6	1	3	3	15
E 5. The organization measures risk management outcomes or results.	3	5	1	0	6	15
Section Total	9	25	6	13	22	75

Control Activities

Section F - Control Activities Survey Questions	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
F 1. There is an appropriate balance of preventative and detective controls in place, with emphasis on preventative controls when appropriate.	2	2	0	4	7	15
F 2. Controls are considered in terms of efficiency as well as effectiveness.	0	2	0	6	7	15
F 3. Control activities include effective controls over information technology management, information technology infrastructure, security management, software development and maintenance.	0	2	0	6	7	15
F 4. Controls are effective in ensuring the completeness, accuracy and validity of data processed.	1	2	0	8	4	15
F 5. Management considers the impact of significant organizational, structural or managerial changes on risk, risk responses and the related control activities before implementing them.	2	4	1	3	5	15
Section Total	5	12	1	27	30	75

Information and Communication

Section G - Information and Communication Survey Questions	Don't Know	Disagree – Not Happening or No Plans	Planned- Will be Introduced	Partly Agree – In Place Localized Only	Fully Agree – In Place Enterprise Wide	Total Number of Responses per Question
G 1. Appropriate information is identified and captured to identify, assess and respond to risk and manage the business, obtained from appropriate internal and external sources, generated manually and electronically and is in appropriate formal and informal formats.	2	4	1	3	5	15
G 2. Information is provided for decision-making at the appropriate depth and with the appropriate timeliness.	1	3	1	6	4	15
G 3. Information quality is evaluated in terms of e.g., level of detail of the content – Timeliness, Currency, Reliability, Accessibility, Level of Detail.	1	4	1	6	3	15
G 4. There are clear upward lines of communication to report risk incidents.	2	4	0	4	5	15
G 5. Communications in the organization, both formal and informal, are effective in raising the risk awareness.	1	4	0	6	4	15
Section Total	7	19	3	25	21	75

Monitoring

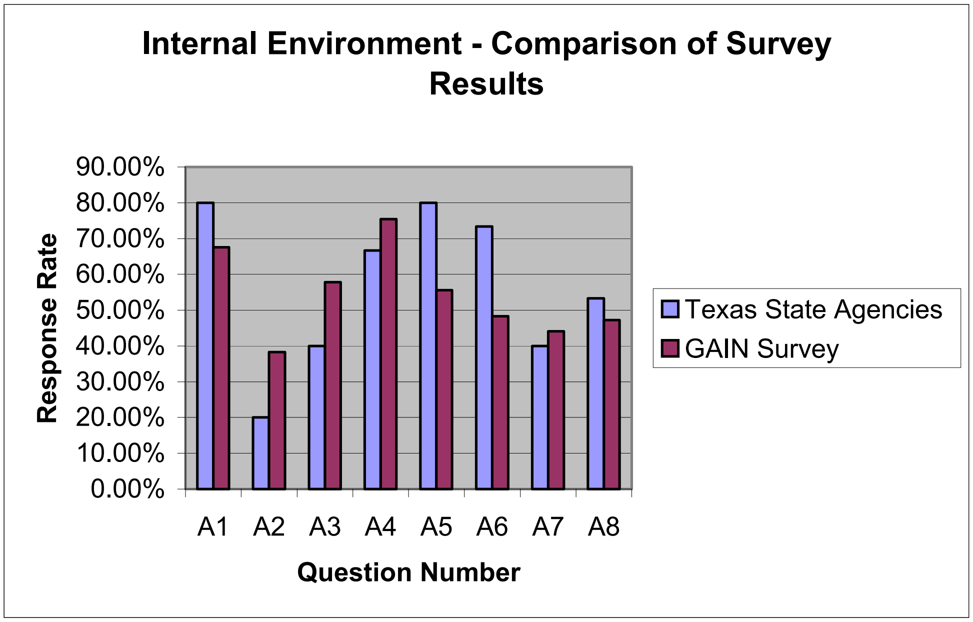
Section H – Monitoring Survey Questions	**Don't Know**	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
H 1. The required information is available to allow for proper monitoring of risk throughout the company.	2	3	0	6	4	15
H 2. Appropriate real time ongoing monitoring processes are in place to measure performance and provide early warning or detect and report deviations from established norms immediately to the appropriate managers.	1	3	0	7	4	15
H 3. A monitoring process is built into the execution of the business process.	1	2	2	5	5	15
H 4. Day-to-day monitoring takes placed daily through ongoing supervision and oversight.	1	2	0	7	5	15
H 5. Process and risk owners periodically self assess their performance and report the results of their self-assessment upward to appropriate managers.	1	4	2	4	4	15
Section Total	6	14	4	29	22	75

	Don't Know	**Disagree – Not Happening or No Plans**	**Planned- Will be Introduced**	**Partly Agree – In Place Localized Only**	**Fully Agree – In Place Enterprise Wide**	**Total Number of Responses per Question**
Texas Agency Totals	63	212	40	215	240	770

Appendix 3 – Graphical Comparison of Survey Results

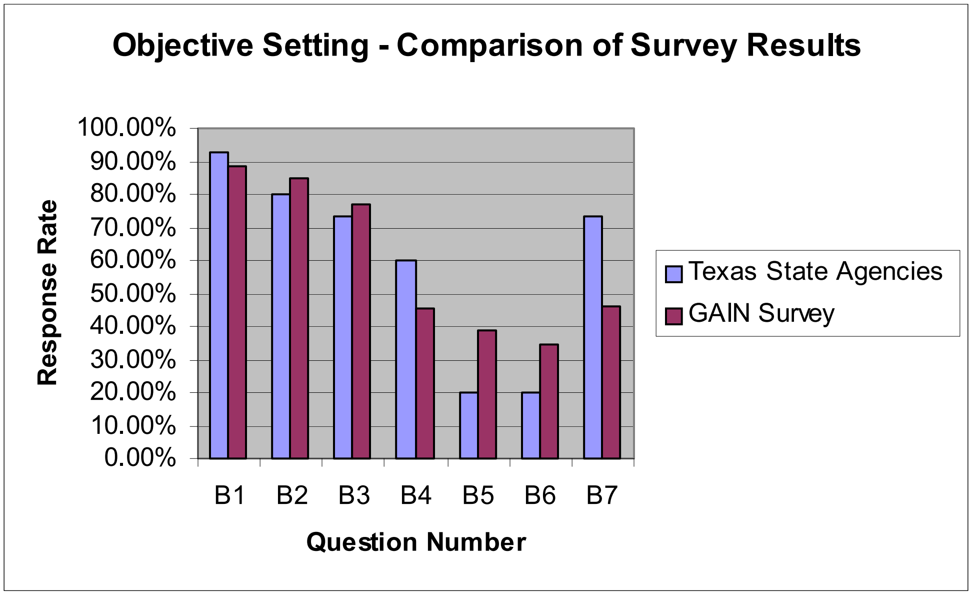
This section contains bar chart comparisons by COSO *Enterprise Risk Management Framework* component section. The graphical representation is labeled by question numbers, which correspond to the question numbers in the survey. For example, result A1 is the result for the first question in section A – Internal Environment. The results in Chapter 5 – Results are shown in order of the sub-components of the model from Table 4.1.

Graph A3.1: Comparison of Survey Results for Internal Environment



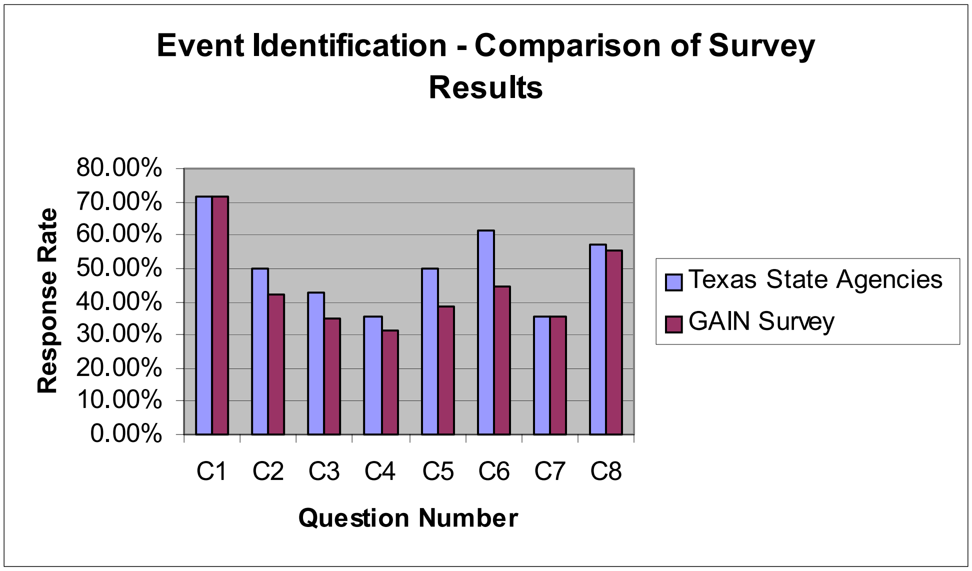
Graph A3.1 shows the range of responses in the internal environment category. For example, question A2, which asks about overall risk management policies in organizations reveals that Texas state agencies are significantly lower in implementing this component. This result indicates an area of improvement for Texas state agencies. Similarly question A3 regarding board consideration of risk in normal oversight activities indicates that Texas state agencies have room to improve in this area. Overall, for the entire internal environment category, the average responses indicate that Texas state agency responses are within 5% of GAIN survey respondents.

Graph A3.2: Comparison of Survey Results for Objective Setting



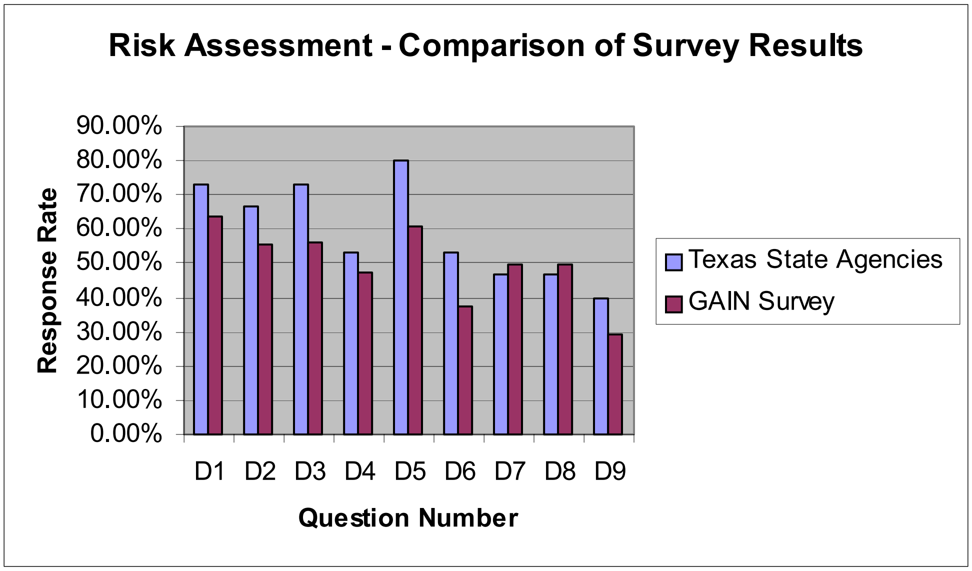
Graph A3.2 shows the range of responses in the objective setting category. For example, question B5, regarding evaluation to ensure risk does not exceed level of risk set by the board, reveals that Texas state agencies are significantly lower in implementing this component. This result indicates an area of improvement for Texas state agencies. Similarly question B6 regarding determination of acceptable limits of risk tolerance indicates that Texas state agencies have room to improve in this area. Overall, for the entire objective setting category the average responses indicate that Texas state agency responses are within 5% of the GAIN survey respondents.

Graph A3.3: Comparison of Survey Results for Event Identification



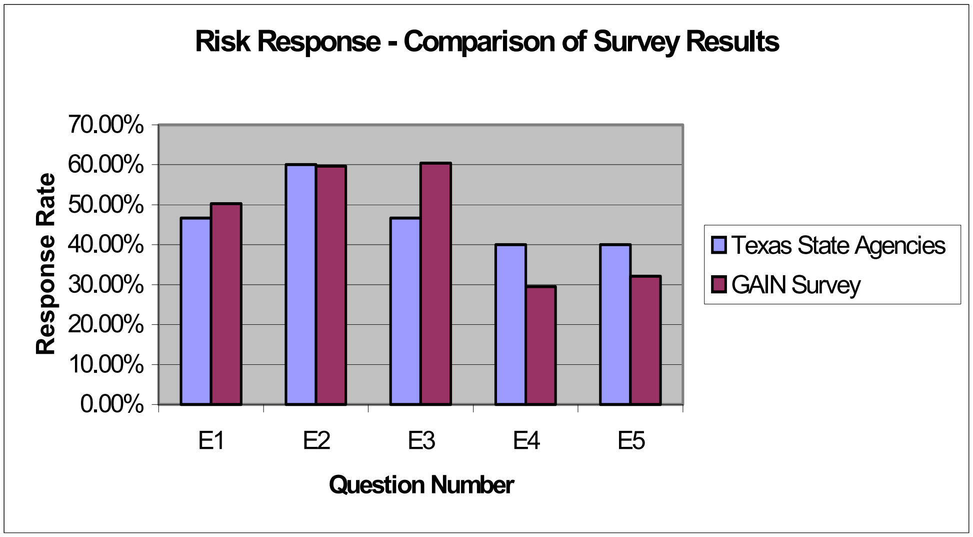
Graph A3.3 shows the range of responses in the event identification category. This section is a very positive result. Overall, for the entire event identification category the average responses indicate that Texas state agency responses are higher than the GAIN survey respondents.

Graph A3.4: Comparison of Survey Results for Risk Assessment



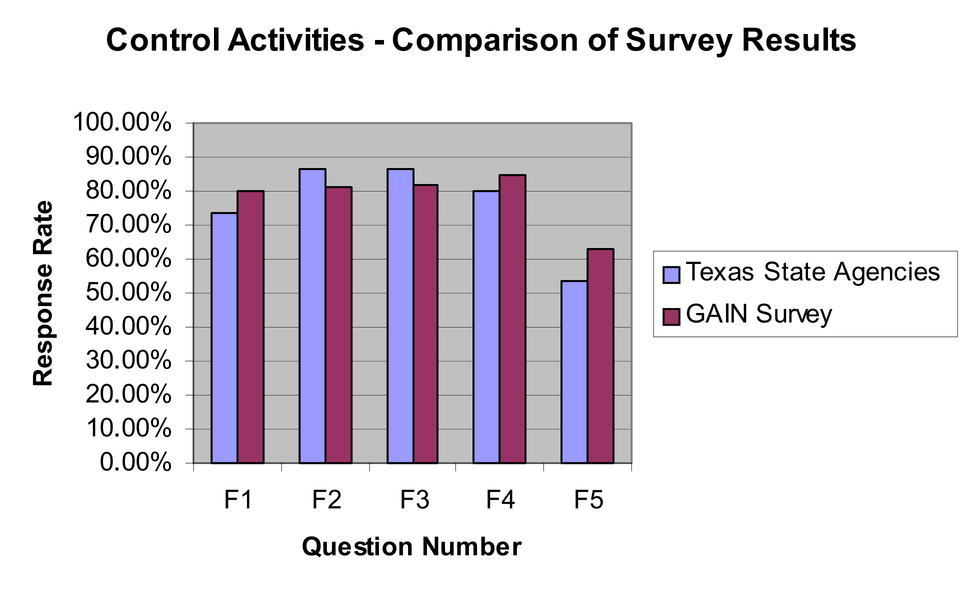
Graph A3.4 shows the range of responses in the risk assessment category. This graph reveals positive results. Texas state agencies responded at a higher rate on all questions except for questions D7 and D8. The response rates for Texas state agencies for questions D7 and D8 were very close to GAIN survey respondents. Overall, for the entire risk assessment category the average responses indicate that Texas state agency responses are higher than GAIN survey respondents.

Graph A3.5: Comparison of Survey Results for Risk Response



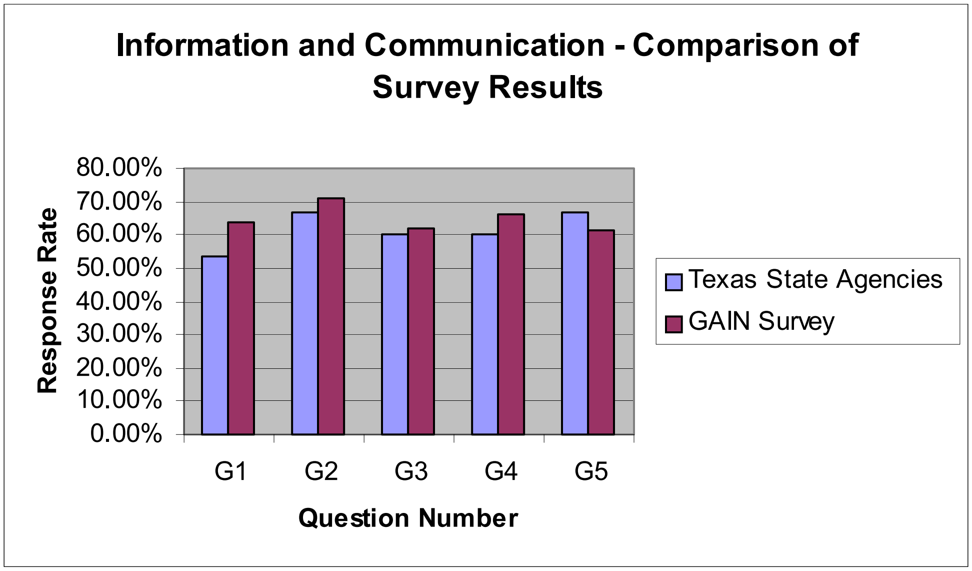
Graph A3.5 shows the range of responses in the risk response category. For example, question E3, asks about cost/benefit analysis of alternative risk responses reveals that Texas state agencies are lower in implementing this component. This result indicates an area for improvement for Texas state agencies. Overall, for the entire risk response category the average responses indicate that Texas state agency responses are within 5% of the GAIN survey respondents.

Graph A3.6: Comparison of Survey Results for Control Activities



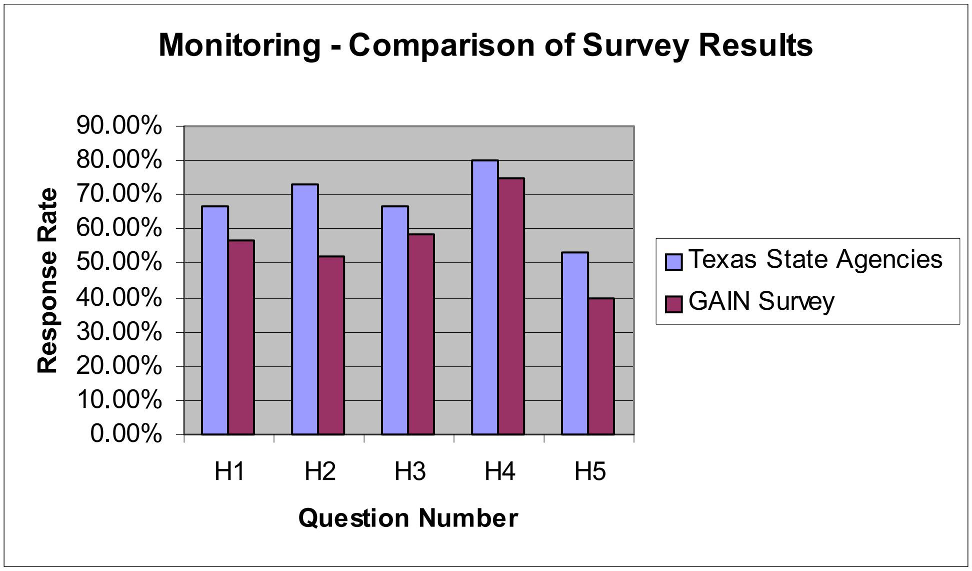
Graph A3.6 shows the range of responses in the control activities category. For example, question F5, regarding management's consideration of significant changes in the organization in its risk management activities reveals that Texas state agencies are lower in implementing this component. This result indicates an area of improvement for Texas state agencies. Overall, for the entire control activities category the average responses indicate that Texas state agency responses are within 5% of the GAIN survey respondents.

Graph A3.7: Comparison of Survey Results for Information and Communication



Graph A3.7 shows the range of responses in the information and communication category. For example, question G1, regarding gathering information for management use reveals that Texas state agencies are significantly lower in implementing this component. This result indicates an area for improvement for Texas state agencies. Overall, for the entire information and communication category the average responses indicate that Texas state agency responses are within 5% of the GAIN survey respondents.

Graph A3.8: Comparison of Survey Results for Monitoring



Graph A3.8 shows the range of responses in the monitoring category. Texas state agencies responded in a higher overall percentage on every question in the monitoring section than the GAIN survey respondents. This is a very positive result.