

**The University of Texas System
Institutional Compliance Program**

Charles G. Chaffin, System-wide Compliance Officer and Director of Audits
The University of Texas System

Original Submission Abstract

The U.T. System Administration, and its component institutions, have designed and implemented a comprehensive program that provides the real-time status of compliance with all applicable laws, rules, regulations, policies, and procedures unique to higher education. The objective is to make compliance risk management an integral part of the everyday activities of all the employees in the U. T. System. While several higher education institutions have implemented programs for extremely high-risk operations, the U. T. System has implemented a program to ensure compliance in all operations including student financial aid, basic research, clinical research, medical billing, environmental health and safety, endowments, student activities, intercollegiate athletics, human resources, and financial matters. By training 70,000 employees to do the “right thing,” conducting risk assessments, and monitoring activities to reduce risk, the program changed the institutional culture from management by “directives and edicts” to risk management by the “right” individuals who are held accountable. This evolution is evident by the increase in questions before action is taken, the decrease in “surprises” to executive management and the Board of Regents related to the instances of non-compliance, and in the general attitude of employees to the management of risks.

Introduction of the Organization

The University of Texas System (U. T. System) is comprised of sixteen virtually autonomous institutions under a single board of regents. The sixteen institutions range in size from less than 5,000 students to over 50,000. Of the sixteen, nine are academic institutions, six are health related, and one is the central administration unit that provides common services to the other fifteen institutions or components, as they are known within the system. The nine academic components include a comprehensive flagship institution with significant graduate programs, research, and a major intercollegiate athletic program; several mid-size institutions that have some graduate programs and associated research; and several small institutions whose primary focus is on undergraduate instruction. The six health-related components include one of the world's leading cancer hospital and research centers, three other hospitals, and numerous medical-related schools. The central administration functions include construction management of all capital projects, self-insurance for medical practitioners, employees and facilities, a virtual university, issuance of bonded debt, and endowment management. Other U.T. System demographics include 150,000 students, 70,000+ employees, 5+ billion-dollar annual operating budget, and a 13 billion-dollar endowment.

The Problem and the Challenge

Over several years in the mid 1990s, U. T. System experienced a number of high profile internal control failures in areas that were believed to have adequate systems to ensure compliance with all external laws, rules and regulations, and all internal policies and procedures. These failures resulted in the loss of assets, loss of reputation with the public and funding authorities, and extensive damage control. As a result in early 1998,

the Board of Regents of The University of Texas System (Board) directed executive management to establish an on-going, everyday assurance process that would ensure that the university system and all of its components were operating in compliance with the appropriate internal and external requirements.

At that time, U. T. System and each component institution had a long-standing internal audit function in place. This was an active function that during the period of the failures had led a comprehensive initiative to educate managers about their management responsibilities and about internal control. However, this initiative was seen as an internal audit charge and a change in the collegial culture was not accomplished. Consequently, the only time there was a true assessment of whether or not processes, functions, or individuals were following the rules was when internal audit performed work in an area. This periodic assurance work in any area was too intermittent to catch most problems before they became front-page news stories.

The challenge was to design, implement, and operate an effective institutional (corporate) compliance system throughout U. T. System so that executive management could provide the Board a real-time assessment of the compliance profile of the system. The University of Texas System Director of Audits was charged with completing this challenge.

Design of the Best Practice Initiative

In January 1998, there was a complete absence of information and experience on the design and application of a comprehensive compliance program for institutions of higher education. The only existing body of knowledge available dealt with the health-related

activities of institutions of higher education. This absence of a model to follow was a major factor in the approach taken by the U. T. System in designing its program.

The first step was to appoint an ad hoc committee to design the program and develop a process for implementation of the program. The committee was comprised primarily of representatives from the administration side of the institutions and only existed until the program plan was developed and accepted by executive management.

The second step was to get expert assistance. It is not productive to have the ad hoc committee or support staff try to wade through all of the documents that are available about compliance (at the corporate level) or ethics or medical compliance. The most effective course for educating the ad hoc committee, and the course taken by U.T. System, was to obtain outside help from an expert. As we were starting our compliance journey, there was only one outside expert with higher education experience, Lisa Murtha, former compliance officer at the University of Pennsylvania. Ms. Murtha conducted several educational sessions with members of the ad hoc committee. These sessions provided the ad hoc committee with the knowledge necessary to complete the development of *An Action Plan to Ensure Institutional Compliance* (Action Plan).

Step three was to adopt an operating philosophy and goals and objectives for the compliance program. The operating philosophy for the U.T. program was stated in the first sentence of the Action Plan, the document that sets forth the design of the compliance program, namely, to ensure U.T. System compliance with applicable laws,

regulations, policies, and procedures. This is an all-inclusive statement. It includes specific federal, state, and local laws and their interpretive regulations and rules; and, it also includes all internal policies and procedures, both Regent and management imposed. This makes the program apply to every employee in all aspects of their university activities. The goals and objectives can be summarized in the following statement:

Provide a proactive program that minimizes noncompliance.

Step four was to actually write the document that would guide the institutional compliance program. There was a single author and multiple exposures to the entire ad hoc committee before a final product was obtained. It was then submitted to executive management for approval and finally to the Board for their approval and adoption. There was a three-month time lapse from the Chairman's charge to implement a program until the presentation of the Action Plan to the Board.

Implementation of The University of Texas System Institutional Compliance Program

The implementation of U. T. System's Institutional Compliance Program has gone through several stages which, in hindsight, we will label as Building the Infrastructure, Creating Awareness, Managing the Critical Risks, and Appraisal and Renewal. In the beginning, though, they were represented by individual steps in a single action plan. A plan whose authors believed could be completed within one year. This was an overly optimistic goal as evidenced by the fact that the program is now in its fifth year, and all steps of the Action Plan have not been implemented at all components. The lesson here

is that implementation of an institutional compliance program is a long-term project, five to seven years, that is intended to have permanent, long-term results.

A detailed discussion of the first three and a half years of the U.T. implementation effort can be found in the book *Effective Compliance Systems: A Practical Guide for Educational Institutions* authored by David B. Crawford, Charles G. Chaffin, and Scott Scarborough and is available from The Institute of Internal Auditors, Inc. That document contains a step-by-step approach to implementing an effective institutional compliance system in higher education. The following information on implementation represents a summary of the information and can serve as a road map to more detailed information in the book. In addition, implementation steps taken since publication of the book are included.

BUILDING THE INFRASTRUCTURE

The building of the initial infrastructure for compliance began immediately upon approval of the Action Plan by the Board. This phase of implementation took approximately six months to accomplish at each component and was generally performed by employees borrowed from existing departments. Dedicated resources were minimal, except in those health-related components that chose to hire full-time compliance officers and create a formal compliance function. The initial tasks included (1) appointing an institutional compliance officer, (2) establishing an institutional compliance committee, and (3) in our more complex compliance environments, establishing a separate compliance function or office.

The essential elements of an effective compliance program dictate that the compliance officer be a member of the executive management team of the institution. As we began our compliance program, we had two choices for designating a compliance officer. Each component president could designate a current direct report, such as the chief business officer or the chief legal officer, to also be the compliance officer; or, each president could create a new full-time position of compliance officer. In practice, most U.T. component institution presidents elected to assign to a current member of senior management the responsibilities of compliance officer, usually the chief business officer. This proved to be effective from the standpoint of providing immediate activity in compliance and also from the standpoint of knowledge of risks and controls. However, it also had a drawback; that is, most members of the university community saw the compliance program as another business process control with no applicability to the academic sector of the institution. So, though we were able to “jump start” the compliance program, we soon learned that the program plateaued until the Compliance Officer represented the entire university.

The second piece of the compliance infrastructure is the compliance committee. In our initial implementation effort, most components appointed a large institutional compliance committee. Members were chosen because they were managers of areas of the university where it was perceived that there were significant compliance risks. This produced committees with from ten to twenty

members. The committee was viewed as an information gathering and advisory body. Time has taught us that the Institutional Compliance Committee is most effective when it is composed of only those line managers who report directly to the president. We have renamed this the Executive Compliance Committee. The three major duties of this committee are to provide appropriate resources for the compliance program, to ensure appropriate action for noncompliance issues brought to its attention, and to provide overall policy guidance for the program.

As we evolved to the executive compliance committee model, we also developed a set of supporting committees to deal with information gathering and dissemination. The first is the Compliance Working Committee, which is composed of the responsible parties for each compliance area of the institution. This committee performs data gathering and analysis for the executive compliance committee. Additionally, a member of the compliance working committee may chair a subcommittee for their area of responsibility. The subcommittees perform such tasks for the high risks as (1) risk assessments, (2) development of monitoring, specialized training, and reporting plans, and (3) certain assurance activities.

The final step in creating a compliance infrastructure is the establishment of a compliance office or function to support the compliance officer and compliance committee. While the compliance function at each institution is unique, we found that there are four major organizational approaches to a compliance function at an

institution of higher education. They are (1) no compliance function, (2) informal compliance function, (3) coordinator compliance function, and (4) robust compliance function. All four exist within the U.T. System. The two characteristics that appear to affect the choice of compliance function type are the complexity of the compliance environment of the institution and who is the compliance officer. With a full-time compliance officer and a complex compliance environment, experience shows us that a robust compliance function will be established. This function will have a dedicated staff and formal structure. The other end of the spectrum, no compliance function, is usually the chosen path when the compliance environment is very simple (no research, NCAA, medical-related activities) and the compliance officer is also the chief business officer. In this structure, current institutional employees from existing departments provide support for the compliance officer, and there is no formal organization or dedication of resources. As our compliance program has matured, we have observed the gradual movement away from the no compliance function type with most components establishing a formal compliance office under the direction of a full-time compliance coordinator who reports to the compliance officer.

CREATING COMPLIANCE AWARENESS

Once the compliance infrastructure was in place, the implementation effort shifted to informing all employees about the initiative and their responsibilities in the program. We call this the Awareness phase of implementation. It involves three major activities. They are (1) developing a Standard of Conduct Guide (our name

for a Code of Conduct), (2) developing a General Compliance Training program for all employees based upon the Standard of Conduct Guide, and (3) establishing a confidential-reporting mechanism. This phase can take from three months to several years to complete. The amount of resources necessary to complete the phase depends upon the kinds (faculty, administrators, professionals, clerical, blue collar) and numbers of employees you must reach with the awareness program. Major incremental costs include contracts with external parties to provide the confidential-reporting mechanism, production costs for training media, and acquisition costs for a compliance training record keeping system.

Step one in this phase is the development of a code of conduct. This may be the most significant roadblock to establishing an effective compliance program. Two major issues evolved as the U.T. System attempted to accomplish this task. First, we had to determine if the code of conduct was to be new policy or merely a summary of current policy. Second, we had to find a label for this product that did not elicit strong negative reaction from any facet of the institutional community.

We decided the content of our code of conduct would be taken from existing policies, procedures, laws, rules and regulations governing operations. The resulting document included all compliance issues that were not specific to particular jobs or job areas. For each issue, we stated the requirements in understandable language, cited the specific law, rule, regulation, policy, or

procedure that gave rise to the issue, and provided contact information in case more in-depth information was needed.

Step two involves developing a curriculum and delivery mechanism for informing all institution employees about their responsibilities in the compliance program.

This training is known as General Compliance Training because it is intended for every employee of the institution, including faculty. The curriculum should be based upon the information included in the Standards of Conduct Guide. Special effort must be expended to ensure that the information included in the training plan is accurate and properly presented. We found that this means the content of the training program should be subjected to several levels of review.

Development of the content and the review process can take from a few weeks to as long as six months, depending upon the desired involvement from the various facets of the university family.

In addition to deciding upon the training program content, we also formed a committee to explore the various methods of training delivery and to recommend the approach for our program. Web-based training was chosen as the primary method of delivery for most of our employees. Content could be highly controlled, tracking of completion could be easily accomplished, and each employee could take the training at their individual speed and essentially when they wanted to do it (within a designated time period). However, as we began delivering this training, we found there was still a need to have face-to-face

sessions for those employees who were not comfortable using computers or did not have computers available. The final consideration in deciding on the primary delivery mechanism deals with the number of employees that must be trained. The larger and more diverse your employee population, the more likely your training delivery mechanism will be some form of web-based training.

The final step in creating awareness of the compliance program within the institutional setting is to establish a confidential-reporting mechanism. Several techniques such as on-campus answering machines or mailboxes were tried, but we ultimately found that the most effective method was to contract with an external provider of confidential-reporting services. This method provides a trained, live person to receive calls on a 7/24/365 basis and ensures the confidentiality of the caller. Cost is usually based upon the size of the employee universe. The mechanism for receiving confidential information must be supplemented by a triage process within the institution. We established a triage team, which included human resources, internal audit, the compliance officer or coordinator, and legal. This team reviews every incident report and determines what actions are taken.

Creating awareness of the compliance program was the first major task of the new institutional compliance infrastructure. It is the foundation upon which all other activities are built. The timeline for completing the initial awareness phase can run from six months to years depending upon the culture of your institution, the

size of the employee universe, the acceptance of faculty, and the resources allocated to getting the job done. It must be successfully completed for you to be successful with the remainder of your compliance program implementation.

The awareness phase involves a significant allocation of employee time, two to three hours for every employee plus the time of those who developed the awareness training. In addition, it will involve the cost of producing the presentation media, which can run from very little to very expensive depending upon the use of outside vendors.

MANAGING THE CRITICAL RISKS

As the awareness phase became operational, we embarked upon the implementation of the core of our compliance program, managing the mission critical compliance risks. This phase of implementation can be divided into two steps. Risk assessments and risk management plans.

Risk assessments were performed using the self-assessment methodology. Initial assessments were conducted in the identified risk areas of the institution. From these area risk assessments, the compliance officer, compliance committee, and compliance working committee selected the compliance risks most critical to the success of the institution. These risks became the primary concentration of the institutional compliance program. Identified compliance risks that were not chosen as institution critical continued to be the responsibility of the appropriate

operational manager. This step will take from three months to a year depending upon the decentralization of your institution and the emphasis placed on the compliance program by executive management. It is a people-intensive exercise that requires very little in terms of incremental dollar resources.

Because of the multiple institution nature of our system, we also established ad hoc committees for each risk area that was common to several components.

These include medical billing, clinical research, basic research, environmental health and safety, student financial aid, athletics, human resources, endowments, and fiscal matters. These committees developed a generic risk assessment for their area of expertise. These risk models are used by the individual component compliance programs to validate their independent risk assessments. This has proved to be an effective vehicle for sharing knowledge, new exposures and risks, and best practice solutions to risk management problems.

Once the institutional critical-risk list was established, we began the process of developing risk management plans for each risk. A risk management plan includes (1) the designation of a single responsible party, (2) development of a monitoring plan, (3) development of a specialized training plan, and (4) development of a reporting plan. We have some risks for which all of these tasks were accomplished within a six-month period. We have other risks where the process has taken several years. The length of time necessary to produce an appropriate risk management plan for a risk depends upon the risk area's previous

experience with risk management, the operating philosophy of the risk area's management, and culture and/or organizational structure of the institution as a whole.

Designation of a single responsible party for a mission critical risk may be the most difficult part of implementing a risk management plan. There can only be one responsible party. If a single party cannot be identified, then you probably have more than one risk or an organizational problem. Accountability is essential in an effective compliance program, so you cannot skip over this step in implementation. Two defining characteristics of a responsible party for a risk are (1) authority to allocate resources to manage the risk and (2) knowledge necessary to manage the risk.

The responsible party is charged with preparing the remainder of the risk management plan; namely, the monitoring plan, the specialized training plan, and the reporting plan. Most responsible parties need significant help and training in performing these tasks the first time. Use of your institution's internal audit department and compliance function as trainers and leaders is essential. During our implementation, we conducted general training sessions on the building of risk management plans and provided individual help to responsible parties on specific parts of their risk management plan. This is the most difficult part of the implementation process. Operational personnel sometimes believe this requires new activities on top of what they already do. In reality, the development of the

risk management plan is simply a codification of actions they are already taking or need to take.

The monitoring plan is a structured presentation of the policies and procedures used to control a risk. The only time new work is created for operational personnel is when their current policies and procedures do not include the necessary actions to control the risk. Likewise, specialized training plans are a formal presentation of that training which is necessary for the employees executing the process (staff and managers) to have in order to properly perform their job duties. Once again, this should not include any new training unless the employees are not currently receiving the information they need to effectively do their jobs. The reporting plan is the most likely area of the risk management plan to produce new tasks for operational personnel. However, this is generally the result of current lack of upward reporting of results of risk management activities. In a well designed process, exception and activity reporting will already be an integral part of the process controls, so that the implementation of a compliance program should have little work impact on employees.

The most significant resource required for implementing the risk management phase is the time of current employees. Risk management plans must be prepared by the employees involved in the process with the help of support groups like internal audit and the compliance function. This resource is usually not incremental, but rather a redirection of resources already budgeted.

APPRAISAL AND RENEWAL

The appraisal and renewal phase of our implementation includes three distinct steps; namely, addressing instances of non-compliance, on-going assurance regarding the management of mission critical compliance risks, and periodic assessments of the compliance program. In reality, we implemented on-going assurance activities and periodic assessments of the compliance program prior to completing all of the awareness and managing the critical risks implementations. While this may appear to be premature, we deemed it essential to have real-time assessments of our progress in the compliance program.

Addressing non-compliance is the “make or break” activity in any compliance program. All else is futile if employees from “the boardroom to the basement” do not perceive there is a negative consequence for failure to comply with applicable requirements. This is a very difficult step to implement in a collegial community because of the historical absence of accountability. The main task in this step is to ensure that all employees understand that addressing instances of non-compliance is the responsibility of line management in the process where the non-compliance occurs. It is not the responsibility of the new compliance officer or the compliance committee. We discovered during our implementation process that instances of non-compliance are most consistently dealt with in those processes where there is a pre-defined set of consequences of non-compliance. Non-compliance happens in the process and must be dealt with in the process for

any compliance program to be effective. The first line of defense against non-compliance is in operations.

The most effective way to ensure that operations continually manages the compliance risks that are critical is on-going assurance provided as the process functions. We implemented a hierarchy of on-going assurance activities to provide real-time assessments to management of the status of compliance in our institution. The lowest level of assurance is a certification by a manager or employee that they have performed their duties as required. This signed self-assessment provides the base of our on-going assurance and may be the only assurance strategy used for less critical risks. Inspections are the next level of assurance, and they represent reviews of risk management activities by upper management or representatives of upper management. This is a management function and not a governance function. We refer to these as oversight controls, and they are the highest level of control in a monitoring plan for a risk.

Practically, they are usually performed by the compliance function, internal audit, or other staff unit such as environmental health and safety. Agreed-upon procedures are specified assurance activities performed for the compliance program or a responsible party by internal audit. They are a consulting engagement and not an audit, and the information is reported only to line management. The final two assurance strategies we implemented are audits and peer reviews.

There are two types of audits conducted for the compliance program. The more traditional is an information validation audit, where internal audit validates the compliance data being reported from a responsible party to the compliance committee and senior management. The other is an audit of the design of the compliance program. We have completed several design audits of our program and made program revisions based upon the findings. In the area of information validation audits, we have found it most productive to delay these types of audits in a high risk area until either an inspection or an agreed-upon-procedure assurance activity indicates the risk management plan is sufficiently in place to produce information that can be audited.

Peer reviews are a major source of appraisal and assurance within our compliance program. Peer reviews provide the advantage of experts in an area reviewing the area, rather than auditors with general knowledge reviewing the area. They also allow for the exchange of information among peers. Finally, they vastly expand the available resources for the highest level of assurance, external assurance. We do not have enough auditors to audit every high-risk area. Consequently, the ability to use teams of external experts in specific risk areas allows us to provide maximum assurance regarding the management of mission critical risks. The cost of peer reviews is generally limited to actual expenses of team members.

The final step in our appraisal and renewal phase of implementation is a self-assessment. We have implemented a self-assessment process for the compliance

committee and compliance program. This process allows the program to examine its accomplishments against its plan and to renew the program. Our self-assessment strategy can take one of two paths. If the self-assessment indicates substantial completion of the compliance Action Plan, then the compliance committee and compliance officer will arrange for an external peer review of the program. If the self-assessment indicates significant gaps in accomplishing the compliance Action Plan, the compliance committee and compliance officer will prepare a plan to close those gaps. After an appropriate time lapse, they will then do a new self-assessment to determine if a peer review is appropriate. Whether internal self-assessment or external peer review, the result is adjustments and improvements in the compliance program. We call it renewal.

IMPLEMENTATION SUMMARY

We ask that you keep two things in mind about the implementation of U. T. System's Institutional Compliance Program. First, it was actually sixteen separate implementations; one at each academic and each health-related component and one at the system administration function. As a result, we have encountered a variety of potential roadblocks that can be encountered with implementation of a compliance program in higher education. Additionally, it means we have implemented a compliance program that is applicable to any size or complexity of educational institution. Second, the implementation process in reality has no final completion date. It is a continuous process in which we plan, do, appraise, plan, do, and appraise.

Benefits

Specific dollar benefits are hard to identify. What is the value of not having negative publicity? What is the value of minimizing damage control activities? However, there are cultural and organizational benefits that are very apparent.

Two stand out. First, we can document an increased incidence of questions and consultations between employees and subject matter experts about whether or not a proposed transaction or activity is compliant. This increased awareness of the consequence of actions by employees is a firm indicator that the compliance program is affecting the day to day thinking of the institution. Second, we can document a culture shift in some of our component institutions. This is a shift from management by decree to management by knowledge. The right people have the right information to make the right decision in a real-time situation. The ultimate indicator is the presence or absence of our institution from the front page of the newspaper. It is the absence of calls from members of the Board of Regents asking for explanations of issues about which we have no knowledge.

However, we have been able to quantify certain program benefits. After experiencing a \$17 million fine due to medical billing errors prior to 1998, we have dramatically reduced our error rate and have avoided being audited by the OIG during the past five years. Our safety program has received several awards and has become a model for the State of Texas. Our workers compensation claims have dropped during the past five years, and we estimate that we have saved over \$10 million during this period of time. In addition, we have significantly reduced our fines from the EPA and other regulatory bodies.

During the next year, we will develop a system to capture the quantifiable benefits of “doing the right thing.”

The real benefit is that, through first our internal control program and second our compliance program, we have set the stage to become the first educational system to develop an enterprise-wide risk management and accountability program.

Retrospect

How we approach the implementation of the compliance program in year five is different from how we approached it in year one. During the process, we learned a great deal through trial and error, failure, and subsequent exploration. We have outlined ultimately what we found during our five-year journey to be the best practices for the implementation of a comprehensive compliance program. We expect the program will continue to evolve and mature as more institutions of higher education implement comprehensive compliance programs and a sharing of information and best practices occurs.

Through our textbook and by hosting two national compliance conferences, we have begun to share our program nationally with other educational institutions. In retrospect, we should have begun the sharing process earlier so that we could have partnered with more higher education institutions nationally at the beginning.