HOW TO CONDUCT A SELF-EVALUATION OF YOUR COMPLIANCE AND ETHICS PROGRAM

June 25-28, 2017
Session 6A: Tuesday, June 27, 2017 11:00 AM - 12:15 PM

Leyda L. Benitez
Villanova University
Villanova, Pennsylvania

Kenneth J. Liddle
Rice University
Houston, Texas

Robert F. Roach
New York University
New York, New York

I. Introduction

A. General Standards for Compliance

To be effective, a University's compliance and ethics program must promote an organizational culture that values a commitment to compliance with the law and ethical behavior. There are a number of compliance program elements that are necessary to establish and maintain an effective compliance program.[1]

First, there must be an overall compliance and ethics program and governance structure. A University's governing body must be knowledgeable about the content and operation of the compliance program and exercise reasonable oversight with respect to its implementation and effectiveness. This oversight may be exercised through an appropriate committee of the Board, such as an Audit and Compliance Committee. Also, a specific individual should be appointed to exercise day-to-day operational authority for the compliance program. This individual should report to a high- level organizational executive (often the chief executive officer) and also periodically to the board or its Audit and Compliance Committee.

Second, a University should have policies and procedures that address specific areas of compliance risk. Ideally, compliance policies and procedures should be integrated into existing organizational policies, all of which should be consistent with applicable laws, regulations, and other best practices and standards.

Third, a University should provide a program of compliance and ethics training and education. Training should be delivered in a manner that is appropriate and accessible to the audience, including faculty, staff, and students.

Fourth, an effective compliance program should provide for lines of communication regarding compliance concerns and risks. These lines of communication can be in the form of various compliance committees and working groups, but typically include an "anonymous" compliance reporting line. Anonymous reporting lines can be hosted internally or by an outside independent organization. They can be web-based or use traditional telephone reporting lines.

[1] United States Sentencing Commission, *Guidelines Manual*, §8B2.1 (Nov. 2016).

The compliance officer or other appropriate personnel, such as internal auditor, should investigate reported compliance concerns and take remedial action when appropriate. There should be a policy of non-retaliation for all those who report compliance concerns in good faith. The compliance officer should make periodic reports to the Board regarding compliance reporting line activities.

Fifth, a University must conduct periodic audits of internal compliance controls and periodic reviews of the overall effectiveness of the compliance program. The organization should develop corrective action plans to address any deficiencies identified through compliance audits and reviews.

Sixth, the University should conduct periodic risk assessments to identify areas of potential compliance risk. Such assessments allow the University to focus scarce resources on the greatest risks. Where an area of compliance risk is identified, the University should develop appropriate internal controls to mitigate the risk.

Finally, the University must not only focus on mere regulatory compliance, but must strive to foster an organizational culture that values ethical behavior.

B. How to Make Ethics a Part of Your Program and Institutional Culture

In higher education, the process of building an effective compliance program starts with a handicap – the name. Look at any dictionary and you will see a definition that typically defines "compliance" as *"submission, obedience, and conformance" of "fealty to command."*[2] An ethics and compliance program based primarily on mandated submission and obedience will not be well received at most American Universities.

Instead of submission and obedience, a University's compliance program should be based upon an ethical culture that reflects the norms or beliefs of the University community. This culture is shaped by the organization's leadership and is often expressed in terms of "shared values" and "guiding principles." In turn, these values are reinforced by systems and procedures implemented throughout the organization. Together, these values, guiding principles, systems and procedures form a University's compliance program. It is the responsibility of an organization's leadership to:

> *Define and give life to an organization's guiding values, to create an environment that supports ethically sound behavior, and to instill a sense of shared accountability among employees . . . The need to obey the law is viewed as a positive aspect of organizational life, rather than an unwelcomed constraint imposed by external authorities.*[3]

---

[2] *See e.g.*, http://www.dictionary.com/browse/compliance?s=t

[3] Lynn Sharpe Paine, *Managing for Organizational Integrity*, Harvard Business Review (March-April 1994)

Thus, a university's values should embrace a desire to fulfill its academic mission with integrity and include a commitment to establishing systems and procedures designed to ensure that the university's legal, regulatory and ethical responsibilities are fulfilled.

As social beings we are guided by values and ideals that are often shared with our peers. The goal of shared value based compliance is that the community engages in self-governance according to chosen standards that reflect *organizational* values & standards. These are driven by leadership (*i.e.* they are *not driven* by lawyers, but are *guided* by lawyers who advise leaders on their legal and ethical obligations). Such values are integrated by management into organizational systems, and provide guidance that enables rather than commands responsible conduct. If members of the community are socially motivated to follow the rules, they will do so because they share organizational beliefs. Thus, their behavior is voluntary – they defer rather than simply comply. Surveillance and sanctioning are less necessary and people are more likely to continue to follow rules "when no one is watching."[4]

One mechanism for fostering a compliance program through shared values is through "compliance committees" composed of key university stakeholders and representatives of academic and administrative functions across the University. (See *e.g.* sample compliance committee charters in the Appendix hereto). In Section IV we will discuss how to assess the effectiveness of your Compliance Committees.

One additional important reason a University may wish to make ethics an integral part of its institutional compliance program is accreditation. In a recent accreditation review of New York University, the Middle States Commission on Higher Education sought to determine whether:

> *In the conduct of its programs and activities involving the public and the constituencies it serves, the institution demonstrates adherence to ethical standards and its own stated policies, providing support for academic and intellectual freedom.*[5]

The evaluation team considered various factors in the course of its study such as: whether the University had clear policies and procedures that were readily available for all members of the community; whether the University's Office of Compliance was effective in its reports, analysis and overall operations; whether University's compliance committees worked effectively to identify potential risks and concerns; whether the Office of Compliance and the University's compliance committees had direct access to the Audit and Compliance Committee of the Board of trustees; and whether University's Leadership demonstrated through clear communication and behavior a commitment to promoting ethical behavior and culture.

---

[4] For further reading, *see also,* Weaver, Trevino, *Compliance and Values Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior*, Business Ethics Quarterly (April 1999); Joshua Joseph, *Integrating Ethics and Compliance Programs: Next Steps for Successful Implementation and Change*, Ethics Resource Center (2001).

[5] Report to the Faculty, Administration, Trustees and Students Of New York University, New York, New York by An Evaluation Team representing the Middle States Commission on Higher Education Prepared after review of the Self-Study Report and a visit to the campus on March 24-27, 2014.

II. Starting a Higher Education Compliance Program

Once the decision has been made that an institution needs a compliance program, it is important to carefully think through exactly how that program will integrate into the existing compliance landscape. Even institutions currently lacking a defined program will find that they likely already have many of the components in place (*e.g.*, a hotline, certain policies, some training). It is also important to think through how the program will be structured, reporting relationships, levels of authority, and integration with other important stakeholders (including Internal Audit, Risk Management, and General Counsel).

A. Structural Considerations and Reporting Relationships[6]

There is no single model for a compliance program in higher education. Determining the right one for your institution will require an understanding of your objectives, your culture, and your current compliance environment.

Program Type	How does it work?	Considerations and Criticisms
No Central Compliance Program	Each functional office is responsible for their own area	There is no coordination, and no oversight. It is likely that areas are being overlooked. It is hard to respond to issues that cross functions
Compliance Committee Only	A group of leaders meet regularly to discuss concerns and respond to issues	This provides for improved communication among leadership, but without direction or ownership it is unlikely to be effective at addressing complicated areas of overlap
Central – Dependent	There is a defined program, set up within an existing office (typically General Counsel), coordinated by an individual who may or may not have authority over other areas	This provides improved communication and better management of overlapping compliance areas. It may be hard to settle disputes, and the individual will lack structural independence or objectivity as relates to their own office. Can be used in conjunction with a Compliance Committee
Central – Independent or Federated	There is a defined program, led by a Director of Compliance or Chief Compliance Officer, who is accountable to the Board or President/Chancellor and who has a level of oversight/authority over other areas of compliance (in conjunction with those areas)	This provides for improved communication and management of overlapping areas of compliance. This type of program retains the greatest degree of independence and objectivity, and thus likely provides the Board and senior leadership with a greater level of confidence in any recommendations. Can be used in conjunction with a Compliance Committee

[6] For further reading on the subject, *see, e.g.*, *Building an Effective Compliance Program: An Introductory Guide* (NACUA 2015); Nathan A. Adams, *Academic Compliance Programs: A Federal Model with Separation of Powers*, 41 J.C. &U.L. 1 (2015).

However the program is set up, reporting relationships should be clearly defined as they relate to any individual with compliance responsibilities. Typically, an individual with functional compliance responsibility will report to the senior leader over that area; and the individual with institutional compliance responsibility will report to both the President (and other senior leaders) and the appropriate Board of Trustees committee.

It is important to have a firm understanding of the relationship between the institutional compliance program and the Office of General Counsel. Historically, many programs were set up under the General Counsel; either as an additional duty of one of the staff attorneys or as a separate office, reporting to the General Counsel.

Relationship with OGC	Discussion
Compliance is the responsibility of someone in the Office of General Counsel	Maximizes privilege, but minimizes emphasis on openness, documentation, and remediation. Compliance is likely to take a back seat to other more pressing matters day to day. There is no real distinction between legal and compliance
Compliance is independent, but reports to the General Counsel	Can be effective, however it places privilege in a precarious position. This relationship is growing disfavored in the corporate world, though still prevalent in higher education
Compliance is independent, and does not report to the General Counsel	Privilege does not apply, though it may still be used when necessary (*e.g.* by having compliance prepare a report on behalf of the GC). This relationship will maximize openness, documentation and remediation, and is generally preferred by compliance professionals

Finally, consideration should be given to the integration of institutional compliance with complementary offices and programs, such as Internal Audit, Enterprise Risk Management, Policy Management, and Insurance. Each of these programs should be thought of as an input for the compliance program (providing important information about risk) and as an output (receiving briefings on institutional performance against related objectives). Where these programs do not yet exist, the institutional compliance program may be instrumental in establishing them.

B. The Initial Risk Assessment and Work Plan

Once important foundational decisions have been made, the first order of business for a new compliance program is usually to gather an understanding of the institution's culture, and current strengths and weaknesses as they relate to compliance. The "Three Tiered Compliance Risk Assessment" is one methodical approach to surveying the landscape, and developing the program's first work plan.

1. High Level Compliance Risk Review

As a starting point, Compliance should lead a review against the elements for an effective compliance and ethics program (*i.e.* the U.S. Federal Sentencing Guidelines).[7] Use this process to engage leadership on the

subject of culture and ethics, and discussing a Code of Conduct. As a first step towards assessing functional compliance, many institutions develop a Compliance Matrix[8] which identifies a responsible party for each regulatory area. You will find that certain areas lack clear ownership, either because everyone says "*not my job*" or because multiple people say "*no, that is my job.*" One of the most valuable roles that compliance can play in the early stages of a program is finding homes for these orphans, and playing mediator or judge for these custody battles. The matrix should be publically available, and kept up to date.

If you will have a Compliance Committee, you should consider involving them in the elements review, matrix, and discussions on a code of conduct. Aside from being interesting and engaging subject matter, it will also help to establish early on that compliance is distinct from legal or internal audit.

2. Mid-Level Compliance Risk Review

Early in the program Compliance should meet with the individual responsible for each of the functional compliance areas to assess the basic function and risk in that area. It is important that these meetings be productive, and perhaps slightly provocative, by venturing well beyond "what keeps you up at night." The goal is to understand the basic program and the risk, while demonstrating that institutional compliance is a resource. To do that, Compliance must be knowledgeable about the law, the recent history at the institution (including government action, litigation, internal/external audit findings), current events, and any policies and procedures.

Through this series of meetings Compliance should keep copious notes, and begin outlining areas of deficiency or areas where compliance systems are immature. Compliance should discuss these concerns and possible changes with the individuals responsible for that area (unless there is a reason not to do so) and then with the appropriate leadership or committee.

3. The Detailed Compliance Regulatory Review

At some point, Compliance (in conjunction with Internal Audit and others) should review the university's performance against individual regulations. Obviously, this type of detailed compliance review is time consuming.

---

[7] For one approach to such a review, see Evaluation of Corporate Compliance Programs Department of Justice (2017). Another approach is the Institute of Internal Auditors Practice Guide: Evaluating Ethics-related Programs and Activities (2012).

[8] For examples of a Compliance Matrix, *see, e.g.*, Rice; Washington and Lee.

One way to simplify the process is to have the functional compliance area do a regulatory self-review and present it to Compliance (or perhaps the Compliance Committee), including citations and source documents.

It is worth noting that while the Three Tiered Compliance Risk Assessment is one approach, it is not the only approach. Further, the program may start out with certain priorities already established by the Board or senior leadership (*e.g.* as is often the case if the program is being established in response to a government action, settlement agreement, or other high profile incident).

III. Assessing Your Overall Compliance Program Using Maturity Models

While the Federal Sentencing Guidelines set forth basic elements of an effective compliance program, they make clear that: no single compliance program design fits every organization, and an organization's industry, size, structure and mission all influence program design and operation. Thus, while the Federal Sentencing Guidelines direct us to have an "effective" program, they do not provide any direct guidance on how to measure the effectiveness of your compliance program. There are a number of practical challenges to measuring the effectiveness of your program:

- It is easier to track compliance program activities than results.
- It is difficult to determine which compliance activities drive results.
- It is difficult to assess employee and management behavior objectively and consistently over time.
- Useful benchmarks for accurate comparison are generally unavailable.

This is where organizational "Maturity Models" can help.[9] The concept of a *Capability Maturity Model (CMM)* refers to the degree to which an organization's processes have been formalized, implemented and integrated into an organization's operations. CMMs have been developed for many fields and areas.[10] With a CMM we hope to provide:

- A useful means for assessing your compliance program against recognized standards.
- A method for identifying "next steps" required to advance your compliance program.
- A process for measuring progress against internal and external benchmarks.
- A tool that can be used to measure progress in specific compliance areas and projects or your overall compliance program.

---

[9] The concept of Capability Maturity Models was developed at Carnegie Mellon in the 1980. See http://sce.uhcl.edu/helm/REQ_ENG_WEB/My-Files/mod1/cmm/cmmintro.htm

[10] See, *e.g.*, CMM for software at https://www.sei.cmu.edu/reports/93tr024.pdf; Risk Management at http://riskmaturitymodel.org/; IT Architecture at http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap27.html; Scientific Data Management at https://crowston.syr.edu/sites/crowston.syr.edu/files/CMM%20for%20DM%20to%20share.pdf

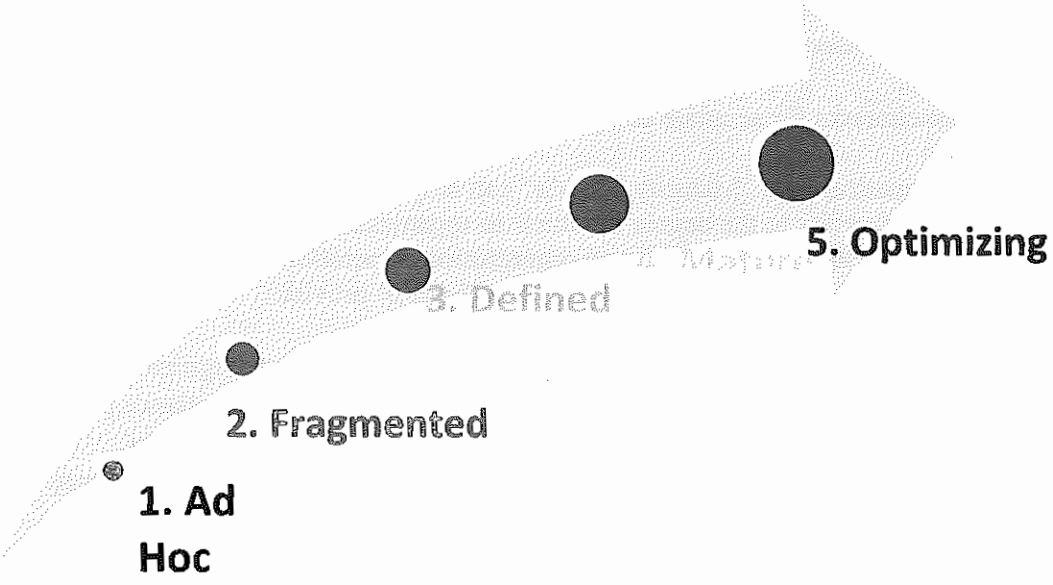
Using existing concepts, we have developed a CMM for Compliance that describes the general "stages of maturity" for University compliance processes following the elements of an effective compliance program as set forth in the Federal Sentencing Guidelines.

A. Compliance as an Afterthought

Many organizations have "bolted on" compliance programs that are separate and apart from their "business" operations. They have not integrated a focus on compliance risk management within operational and decision making processes. The overall results are fragmented compliance programs that are complicated to operate and difficult to coordinate, manage, and monitor. These systems also tend to be reactive rather than planned or strategic.

B. Compliance CMM Maturity Levels

A Compliance CMM focuses on integration of your compliance programs into organizational business processes by analyzing the "maturity" of your program with levels that range from *ad hoc* practices, to formally defined steps, to managed with result metrics, to active optimization of processes. As an organization moves up the maturity model, ownership spreads across the organization and becomes embedded within the very culture of the organization.



Existing CMM for various processes and industries generally vary in the number of "maturity" levels they use – usually three to five. They also use somewhat different descriptive labels for the levels of organizational maturity. We have developed a Compliance CMM with five levels of maturity and apply the most frequently used labels for our maturity levels:

*1. **Ad Hoc:*** Procedures are usually informal, incomplete and inconsistently applied.
*2. **Fragmented:*** There are some compliance controls in place, but they are not consistent across the organization. Often limited to certain areas or managed in "silos" (*e.g.* EHS, Finance, Research, etc.).
*3. **Defined:*** Compliance controls and procedures are documented and standardized across the organization.
*4. **Mature:*** Compliance procedures are an integral part of business processes and periodic reviews are conducted to assess the effectiveness of the program.
*5. **Optimized:*** Regular review and feedback are used to ensure continuous improvement towards optimization of compliance processes; elements are often automated, which are more effective at preventing compliance failures and ultimately less costly than manual controls focusing on detection.

C. Compliance CMM focused on the Elements of an Effective Program

Our Compliance CMM sets forth a methodology for determining the overall maturity of a University compliance program by using maturity modeling concepts to analyze the extent to which the University has implemented the compliance program elements set forth in the Federal Sentencing Guidelines.

1. Structure and Accountability

We begin our analysis by examining the extent to which your University's leadership promotes a culture of compliance and supports compliance by providing adequate program resources relative to the University's size and complexity. We also examine whether the compliance program structure facilitates distributed responsibility for compliance throughout the organization enterprise-wide coordination, oversight and accountability.

compliance structure.	board discourage noncompliance but are not consistent in follow through.	A compliance structure has been established, with accountability assigned to key risk area officers.	Compliance risk assessments and mitigation plans are completed by risk area officers on a regular, timely and consistent basis.	Network of compliance officers representing every significant operation is in place and they meet regularly to coordinate compliance activities.
There is no independent oversight.	Accountability is broadly understood but not formally documented. Oversight and monitoring are inconsistent.	A senior compliance committee exists, including representatives of key organizational areas.	Reporting by risk area officers to the chief compliance officer is timely and consistent.	The senior compliance committee considers compliance a strategic priority. Compliance risk scenarios have been identified, assessed and mapped to compliance controls, which are updated at least annually.
Accountability is not defined.	A senior compliance committee may exist, but compliance activities are reactive and in silos.	A chief compliance officer or other individual with day to day responsibility for compliance is appointed.	The senior compliance committee meets at least quarterly, receives regular reports from the chief compliance officer and actively plans for compliance contingencies.	The board/audit committee and executive management show a demonstrated commitment to compliance throughout the organization.
Compliance risks are not understood.	Compliance risks are understood but not formally documented.	A process is in place for identifying compliance risks and developing mitigation plans by assigned risk area officers.	The chief compliance officer has independent and direct access to the board or audit committee and makes regular reports on compliance activities to the board/ audit committee.	Compliance, risk management and internal audit have implemented integrated work plans. Integrated functions are supported by automated processes.

2. Compliance Policies and Procedures

When assessing your compliance program you must examine your University's policy process. Do you have established processes for developing compliance policies? Do you adequately track changes in law and organizational activities, the impact of changes on your policies over time, and revise and update University policies in a timely and effective manner? Are policies readily accessible to the University community and widely disseminated throughout your organization? Consider the following factors in assessing the maturity of your compliance policy process.

Some compliance policies exist.	Compliance policies exist but may not be complete and are not consistently documented.	Policies for all significant compliance areas are published, in a consistent format and readily available.	Policies are widely available and easily found on the organization's website (internal or external). There are additional mechanisms for easy identification (e.g. web search functions). Policies identify executive and day-to-day responsible officers for questions.	Compliance policies are monitored and the results used to improve policies.
Employees may be informed about policies, but communication is sporadic and availability inconsistent.	Employees are provided guidance on the organization's policies; however communications are sporadic or undocumented.	The organization has formal processes in place to communicate compliance policies.	Compliance policies and the consequences of non-compliance are communicated regularly, at least annually. Policy compliance is monitored and assessed.	Changes and improvements are made to messaging and communication techniques in response to periodic assessments. New and amended policies are communicated shortly after changes are approved.
Processes for approval and subsequent review are informal, sporadic and inconsistent.	Procedures for approval of policies and subsequent review exist but are not formally documented nor consistently followed.	There is a formal policy development and approval process that identifies executive owners and day-to-day responsible officers. Subsequent review occurs, but monitoring for compliance with the process does not occur or is sporadic and undocumented.	Policies are reviewed regularly to ensure compliance with regulatory changes. Monitoring of compliance with the policy review process is formal and documented.	Legislation is proactively monitored to ensure that new and amended policies are implemented in a timely fashion. Legislation services are utilized. The policy management and monitoring process may be automated.

3. Training and Communication

Effective lines of communication regarding compliance are critical if a University desires to develop and sustain a culture of compliance. The maturity of a University's compliance program can be measured by assessing the degree to which its communications and training program are planned and the breadth and depth of its content and distribution. The degree to which communication responsibilities are distributed throughout the University and assigned to those persons responsible for ensuring day-to-day regulatory compliance is also important.

The means of communication should be varied and tailored to the needs of the targeted audience and there should be a process for tracking ongoing communications and training programs (with appropriate audit trails) as well as the degree to which compliance information is received and understood (through assessment and certification processes).

training is not provided; however, compliance information may be communicated by informal means.	The organization provides compliance training but it is sporadic or in silos.	Compliance training is provided throughout the organization as needed in a scheduled and timely fashion. Training metrics may not be collected and reported to executives or the Board in a regular or consistent fashion.	An enterprise wide compliance training program exists and is monitored by management and responsible officers. The organization identifies persons needing training in key compliance areas and monitors their participation. Training metrics are collected and reported to executives and the board at least annually.	A program of compulsory compliance training is implemented. Automation is used in program delivery and monitoring. Competency assessments and certification programs are implemented in key compliance areas. Monitoring and metrics are used to continuously improve training.
There is no formal compliance communication program.	Occasional communication about compliance may occur, but it is sporadic and informal.	Compliance communications such as newsletters, email blasts, posters and other methods are used. There is no formal documented compliance communication program.	The organization has developed a formal compliance communication plan that is documented and updated at least annually.	Compliance monitoring and metrics are used to continuously improve the compliance communication plan.

4. Monitoring

A compliance monitoring program should include day-to-day monitoring of compliance that is distributed among responsible administrators throughout the University as well as periodic independent monitoring of compliance by auditors and/or centralized compliance office. Deficiencies should be addressed through remedial action plans with regular reporting to high-ranking University officials who have oversight responsibility.

Monitoring of compliance program elements and risks are informal and ad hoc.	Monitoring of compliance program elements and risks exist but may not cover all all aspects	Monitoring of compliance program cover all relevant elements and risks.	Monitoring of compliance cover all program elements and risks.	Monitoring is coordinated and integrated into Compliance, IA and Risk Management Functions.
Guidance on monitoring is not formally provided or documented	Some guidance provided but not fully documented.	Monitoring is fully documented.	Monitoring is fully documented and includes both ongoing monitoring by risk owners and independent monitors (e.g. compliance officer or IA)	Formal integrated monitoring plans are developed at least annually by Compliance, IA and Risk Management. Monitoring plans are reviewed and approved at least annually by executives and Board.
			Monitoring results with corrective action plans are reported to executives and Board	Metrics arising from monitoring activities are developed, reported and utilized to drive continuous improvement in the Compliance Program. Automation is used when possible.

5. Risk Assessment

Finally, an established risk management process, using a recognized methodology (such as COSO or ISO 31000) should guide a University's compliance program. Ideally, the compliance risk management process should be implemented enterprise-wide with distributed responsibility and ownership; use agreed-upon, standardized risk assessment criteria, documented mitigation plans, and ongoing monitoring, and have established methods for reporting and oversight.

Compliance Risks may have been identified, but not as a result of any formal process.	Employees may be aware of and consider various compliance risks.	Processes have been implemented for risk identification, assessment and reporting.	All formal processes for compliance risk management have been implemented throughout the organization and are formally documented through a risk register or other means.	Compliance, Risk Management and Internal Audit have integrated risk management processes that are improved continuously through ongoing monitoring. Risks are customized by jurisdiction.
A compliance risk assessment has not likely been completed or risk formally documented.	Risk assessments may be conducted regularly, but are not part of a regular risk management program and may not cover all areas.	A formal risk management process has been adopted, such as ISO 31000 or COSO ERM.	All risks are assessed at least annually. Mitigation plans are monitored by risk owners and reviewed by an independent department (e.g. compliance or internal audit).	Executive management and the board regularly review the risk program and provide leadership for key strategic and institutional risks.
			The results of risk management process are reported at least annually to executive management and the board.	Automation for the risk management process may be implemented.

IV. How to Assess Specific Elements or Components of Your Program

A. Compliance Functional Areas

In assessing the effectiveness of functional areas of compliance, the institutional compliance officer should work in close collaboration with university representatives who have operational responsibility over highly regulated institutional functions. In fact, the number of compliance areas with operational and oftentimes oversight responsibilities by a single University representative continues to grow in diverse areas such as data governance, privacy and data security; equity, diversity and inclusion; export controls and Title IX Coordinators, to name a few. Working in close collaboration with these functional representatives will help to both drive the compliance and ethics program agenda and develop more comprehensive compliance efforts in the university as a whole. It is helpful to find a way to integrate these functional compliance areas in one report that has a certain level of consistency for interpretation and presentation to your senior leadership and governing board.

One way to do so is to start with a few metrics that are of general applicability, but adaptable to the compliance area in question. This information can be aggregated for reporting purposes on an annual basis. Sample metrics that compliance areas can start collecting include:

1. Policies and procedures—At least on an annual basis, functional area representatives should provide basic information regarding the number and identity of the policies and procedures they oversee, or that otherwise have an impact on their specific compliance area. If not done at the institutional level, they should indicate the process by which they review and revise these policies or make a determination of the need for new policies given a new law, rule or regulation.
2. Communication, education and training—The functional areas should provide documentation regarding the internal and external communication, education and training efforts they have engaged in during the course of the year. A common template should be used to ensure consistency. At a minimum, this would include the types of training, number of opportunities afforded and intended audience, number of attendees, and whether the offering was done in-person or online. This should also cover instances of communication around major compliance initiatives and should indicate means of communication—announcements from senior leadership, e-mail blasts, newsletters, etc.
3. Inquiries received, whether internal or external— The functional leaders should keep track of the type of inquiries handled through their offices and indicate whether these were internal (members of the University community and, if so, whether made by students) or external.[11]

[11] For example, as part of its process for verification of compliance with federal regulations, the Middle States Commission on Higher Education requests confirmation that institutions have effective policies and procedures for tracking student complaints. 34 CFR 602.16(a)(1)(ix). See Middle States Commission on Higher Education, *Verification of Compliance with Accreditation-Relevant Federal Regulations, Implementation for 2016* (2015).

4. Audits, Inspections, Monitoring, or Corrective Action— The functional leaders should be able to present, again in a consistent format, what their level of activity has been around these matters to the extent applicable to their areas.

Review of this data will allow the compliance officer to draw conclusions regarding the maturity level of that specific functional area and whether there may be certain gaps in compliance for the cluster of specific compliance risks. Over time, additional metrics and functional compliance areas should be added to the compliance and ethics program infrastructure.

B. Compliance Committees—Assessment and Methodology

In order to continue to develop a strong compliance and ethics infrastructure at your institution, you will also need to review the effectiveness of your compliance committees, including those committees dedicated towards specific compliance objectives (*e.g.* IRB, IACUC), and those dedicated to overall compliance management or oversight (*e.g.* University Compliance Committee). Any assessment should take into consideration the unique governance structure of our institutions and their reliance upon the principle of shared governance. It has long been recognized that the "variety and complexity of the tasks performed by institutions of higher education produce an inescapable interdependence among governing board, administration, faculty, students and others."[12] The existence of this interdependent relationship "calls for adequate communication among these components, and full opportunity for appropriate joint planning and effort."[13]

One way in which institutions of higher education delegate authority and responsibility is through the appointment of committees and work groups which carry out a significant number of functions on behalf of the institution whether related to the academic mission, strategic direction, human resources or faculty governance. There are also a great number of committees which carry out oversight, operational and/or monitoring responsibilities over compliance-related functions. Their members are usually appointment by the President or other senior official with due consideration provided to subject matter expertise, institutional knowledge, diversity of areas represented within the institution, and other factors. Those most often recognized as compliance committees are a by-product of law or federal regulation (*e.g.,* Institutional Review Board, Institutional Biosafety Committee, Radiation Control Committee, etc.). Others, however, carry out compliance-related functions with less of an opportunity for awareness and communication at the institutional level regarding their work and contribution to the institution's governance structure.

The work of these compliance committees or work groups has great implications toward the vitality of the principle of self-governance. As noted in a recent project by the Association of Governing Boards of Universities and Colleges (AGB), "strong shared governance is dependent not so much on formal structures as on organizational cultures in which

---

[12] American Association of University Professors, Statement on Government of Colleges and Universities (1966) available at https://www.aaup.org/report/statement-government-colleges-and-universities.
[13] *Id.*

members of the organization have a sense of ownership, responsibility, and accountability for the institution's health, vitality and relevance."[14] The AGB's project further noted that "governance that is properly aligned with strategic goals may benefit from *ad hoc* structures that recognize standing board or faculty committees are not best-suited for a given task for reasons such as timing, workload, and expertise." Thus, there is a recognition that formal committee structures such as the board may be complemented by "an increasingly common practice in addressing these major issues" through the "creation of task forces composed of those with the experience and expertise to best explore the issue and options, and make recommendations to the board and the administrative leadership. These task forces (or *ad hoc* committees) often include membership of other stakeholders in addition to board members—administrators and staff, faculty, and students, depending on the nature of the issue."[15]

In the compliance arena, these committees, task forces, or work groups (collectively "committees") have varying attributes, but for the most part fall within the following categories:

Compliance Committee	Attributes
Governance	• Committees that operate at the highest levels of fiduciary responsibility with regard to compliance matters • Examples include: o Audit and Risk or other appropriate committee(s) of the governing board o Leadership operational committee (senior leadership reporting to the President) o Faculty Senate or other faculty governance and oversight committee
Oversight of Compliance/Risk Functions	• Committees charged with oversight and/or guidance of university-wide compliance and risk functions • Members are usually appointed by the President • Examples include: o University Compliance Advisory Committee o Enterprise Risk Management and/or Risk Committees o Research Compliance Oversight Committee
Regulatory	• Committees mandated by a regulatory requirement • Usually the activity cannot take place without this committee's oversight • Appointed by the University President or other senior official • Oversight provided by Institutional Official as required by the regulations • Examples include: o Institutional Review Board o Institutional Animal Care and Use Committee o Institutional Biosafety Committee
Driven by Specific	• Though not required by law, committees are created in response to a

[14] Association of Governing Boards of Universities and Colleges, *Shared Governance: Changing with the Times* (March 2017), 6.
[15] *Id.*

Law, Rule or Regulation (implementation and non-implementation roles)	regulatory mandate • Committees are often charged with responsibility for the implementation of a new law or regulation including the conduct of gap assessment, creation of new policies, education and training, etc. • May continue to exist beyond implementation to assist institution in its ongoing compliance efforts ○ Examples include: HEOA, HIPAA, ADA

Driven by Specific Area of Compliance Risk	• Committees or work groups that are brought together for one of many reasons such as addressing a newly identified area of compliance risk or gap, implementing a corrective action plan, or creating (or strengthening) the infrastructure in place to support the activity/objective
	• Main purpose of their existence is not the implementation of new laws or regulations, but their work is definitely impacted by them
	• In almost all instances, the scope of their work cuts across divisions and subject matter expertise
	• Examples include:
	  ○ Accreditation standards-verification of compliance requirements
	  ○ Minors on Campus
	  ○ Data Governance
	  ○ Behavioral Assessment Teams
	  ○ Sexual Misconduct (including Title IX)

In order to carry out the assessments, you will first need to create a current inventory of compliance committees. Since the type and number of these committees are not usually maintained in a centralized fashion, the most expeditious way to develop this inventory is through a written request to senior leadership. The request should ask to be over-inconclusive, in order words, where there is a doubt as to whether part of the committee's function may be compliance-related, the committee should be included in the inventory for a later determination. The request should explain the purpose of this initiative and include a simple spreadsheet of the desired information points:

- Committee Name
- Chairperson
- Scope/Purpose
- Frequency of Meetings
- Policies related to scope of work
- Website Presence

Once you have the current inventory, you will need to determine the methodology that you will use to conduct the assessments. In the absence of specifically prescribed methodology for a regulatory committee, the committee should generally be allowed to determine its own effectiveness and conduct its own assessment. However, to demonstrate its effectiveness within the institution as a whole, the tool should assess effectiveness in relation to other existing

compliance committees. It is through this comprehensive assessment that the institution can learn what areas of compliance risks are being addressed and to what extent.

To create this self-assessment tool, we used principles derived from the *Internal Control—Integrated Framework* (2013) of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This Framework serves to assess whether the organization has an effective system of internal control. Internal control is defined as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operation, reporting, and compliance."[16] An effective system of internal control reduces, to an acceptable level, the risk of not achieving an entity's objective and may relate to one, two, or all three categories of objectives which consist of operations, reporting and compliance. The internal control consists of five integrated components---control environment, risk assessment, control activities, information and communication, and monitoring activities. These five components consist of seventeen principles.[17]

The self-assessment tool contains ten different areas of inquiry which are meant to map to the five components of the COSO Internal Control Framework and serve as a starting point of inquiry as to the areas of internal control that may apply to the committee's work or function as determined by the committee itself. The secondary point is to have the committee assess its own level of effectiveness in carrying out the committee's various roles. Obviously, not every university committee or work group is expected to cover the five components, but a discussion around questions based on these components is helpful in order to understand the scope of the delegated work. For example, some committees may have a role in designing and planning how to address a specific compliance risk, but absolutely no responsibility in actually implementing their own recommendations. Other committees may have a limited yet invaluable communication role, for example, an advisory committee that communicates its recommendations to a senior official, but has no role in communicating with the university community at large.

By allowing for this assessment to address and compartmentalize the various areas of control activities they may exercise, the committees are also learning and building consensus in certain instances about their roles as understood by the various committee members. The self-assessment tool asks questions in ten discrete areas:

---

[16] *See, Internal Control—Integrated Framework, Executive Summary,* Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013).

[17] *Id.* The Appendix includes the COSO cube, used by permission, which illustrates the *Internal Control-Integrated Framework Principles.* The COSO cube is available at: https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

Committee Role/Function	Sample Areas of Inquiry
Risk Assessment	This will include the reason why the Committee/Work Group (hereinafter "Committee") exists, is it a regulatory committee or not, is it in response to a new law, rule, regulation or policy, when was it chartered and how often does it meet, objectives, scope of work, priorities for the current and next academic year, does it have a charter, mission statement, etc.?
Design and Planning	This can be a multi-year objective or goal, but focus should be on the current and immediate next academic year: how will the Committee address the priorities identified per the criteria above?
Implementation	How will the Committee go about implementing their objectives and scope of work? Are there any challenges to doing so? How can these challenges be addressed?
Communication	Does the Committee have a role in communicating the initiatives or the scope of work assigned to them as part of their Committee structure? How are they going about doing so? Internal/external communication roles?
Education and Training	How often is education/or training provided? Are they internal/external opportunities? How are these opportunities communicated? Who is their intended and preferred audience?
Auditing/Monitoring	Does the Committee have a role in monitoring the objectives achieved? How do they determine what should/could be their role? Do they have internal/external assessments conducted for their areas of responsibility and/or Committee work? What is the Committee's role in connection with such audits or monitoring?
Information Systems	Do they use, rely upon, or wish to have access to automated tools and/or processes and, if so, to what end?
Records Retention	Who is responsible for maintaining the records of the Committee? How are they maintained? What if there is a change in Committee membership or leadership?
Testing	How do they go about testing the effectiveness of one or more of the areas that fall within the scope of responsibilities or objectives of the Committee overall, or a specific project or initiative?
Institutional Mission Support	How does the Committee's scope of work, objectives, and responsibilities support the overall mission of the University? How is this support reflected in both its oversight and operational responsibilities, if applicable?

It is envisioned that, in order to be most effective, the assessments would be carried out by either the committee chairperson or compliance officer. A preliminary meeting should take place in order to discuss various important issues such as the scope and goal of the overall initiative and the mechanics of the self-assessment tool. It is at this time that there could also be a discussion as to whether this is the best or most appropriate time to carry out the assessment or whether it should be deferred to a later date. Reasons to defer include it being a new committee, or under new leadership; or being subject to process improvements or other corrective measures. During this meeting it is also helpful to obtain preliminary information regarding the committee's mission, history, scope of work, and other pertinent introductory information which will make the assessment results easier to contextualize both from the chairperson's and the compliance officer's perspectives.

During the actual assessment, the rating for the various components should be done via a simple voting tool which ranges from (1) failing to meet objectives to (5) exceeding objectives. If certain criteria do not apply to the scope of their work, it is marked as "not applicable." Thus, each committee member then rates the effectiveness of the components that specifically apply to their committee's work or function. The compliance officer then takes the rating scores and completes a summary of the assessment which is provided to the chairperson for review prior to it being finalized.

As with other elements of a compliance program, the benefits that will result from this initiative will depend upon your institution's current infrastructure and compliance readiness. Your institution may have a current registry and a clear picture of all activities that are taking place through its compliance committees. If, however, that is not the case, there are many benefits that can be derived from conducting this initiative. First, you will get to know and understand how many compliance committees and work groups your institution has and whether there is some overlap or duplication of efforts. Conversely, there may be areas of compliance risk for which a compliance committee should exist, but does not. Second, for the committees that do exist, you can learn more about the level of activities that they are engaged in, and to what extent their activities revolve around internal controls such as recommending policies and processes, providing education and training, and communicating their recommendations to the University community at large. The metrics will help to communicate to your senior leadership, internal and external stakeholders, the scope and breadth of the work these compliance committees are undertaking.

Beyond these quantitative metrics, the more difficult to capture qualitative measures can also be helpful in strengthening the infrastructure that supports compliance at your institution. The assessment represents an opportunity to discuss compliance issues and controls around those values that are shared by the members of the committee, as led by the committee's chairperson. Through this opportunity for engagement around their role, compliance committees can be empowered to know that their work is recognized and will be presented to the institution's most senior leadership and governing board. This initiative may serve to motivate the committees toward self-improvement. For example, upon assessment, a committee may decide that it needs to revisit its charter because it is outdated (or non-existent); or more properly document education and training efforts; or request additional resources to accommodate increasing levels of work and responsibility assigned to it through its existence.

In all, the initiative may prompt committees to delve into their own governance structure and discuss whether there should be any changes or improvements made to the way they are carrying out their business. While these types of qualitative metrics are more difficult to capture or even know the extent to which they are happening, this recognition is in and of itself an element of an effective compliance and ethics program. At the end of the day, empowering these compliance committees also serves to strengthen the principle of self-governance at our institutions of higher education.

V. Appendices

A. Higher Education Compliance Resources and Links

B. Compliance Committee Charters (Samples)

C. Evaluation of Corporate Compliance Programs, Department of Justice (2017)

D. Murphy, *J. Tools for evaluating your compliance program*. Compliance and Ethics Professional (April 2017) (Society of Corporate Compliance and Ethics). Used by permission.

E. *COSO Internal Control – Integrated Framework Principles.* ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). Used by permission.