

Compliance and Internal Audit: A Dangerous Combination?

By

Urton Anderson CIA, CCEP

and

Sheryl Vacca, CCEP, CHC-F, CHRC, CHPC

A recent column in the February 2011 issue of the *Internal Auditor* by Catherine Henry - "Governance Perspective: Too Close for Comfort" – addresses the relatively common practice of combining the internal audit and the compliance/ethics functions. Citing a 2009 study of 560 compliance professionals from both public and privately-held organizations, 12.2% reported that the organization's compliance/ethics officer was also the head of internal audit. This was slightly higher than the other common practice of assigning the compliance/ethics role to General Counsel (R. Walker, "Compliance and Ethics Officer Positioning," *Compliance and Ethics Professional*, December 2009, pp 46-51). Henry brings up a number of concerns surrounding combining the internal audit and the compliance/ethics functions. These concerns include not only the expected auditor independence and objectivity issues but arguments that the combination weakens the effectiveness of compliance and ethics as well. Her conclusion is that whatever advantage the combination of the two functions might bring to the organization, the dangers to the longer term interest of the organization and its stakeholders make such a combination ill advised.

For higher education the issue of dual responsibility is of particular concern as the practice of combining the functions has been particularly common in the university setting as a quick Google or Bing search on "Office of Audit and Institutional Compliance" will illustrate. Susan Keller ("Building a Compliance Program in Higher Education Institutions without a Compliance Officer," *College & University Auditor*, Spring 2009, p 7) argues that the IA function is a natural driver for development of an institution-wide compliance functions in universities because in the very decentralized governance structure in higher education it is one of the few groups with university-wide view of risk and control. IA, she notes, is also uniquely positioned to gather, analyze and share information across the institution. In her article, she describes how IA at three major universities has driven the successful development of the compliance function in those respective institutions, with each still keeping the two functions combined.

Others have presented additional benefits to a combined function. In combined compliance and internal audit functions collaboration to achieve the responsibilities of both groups is excellent. This collaboration is critical as there are indeed shared roles and responsibilities between the two functions. Ruppert ("Contrasting Roles and Responsibilities – Corporate Compliance and Internal Audit," *New Perspectives*, Summer 2006) identifies the following commonalities when both functions follow best practices:

- Functional reporting to the organization's board typically through an audit or compliance committee.
- Board established authority via approved charter and programs.
- Administrative reporting to the CEO.
- Access to the entire organization per board directive.

- Recognized and communicated understanding that management is responsible for internal control including compliance and that corporate compliance and internal audit is not.
- Have the authority to conduct investigations.
- Are risk based.
- As cost centers the functions are not designed to contribute to the bottom line but can identify cost savings and improve organizational processes.

Ruppert's point that these are commonalities when both functions are following best practices is an important qualification. In particular this implies that both functions are independent of operations. While for internal audit the need for the function to be independent from operating responsibilities for the area has long been recognized in professional standards; however, the notion of an organizational-wide compliance function independent from operations is a relatively newer practice in higher education.

From an organizational perspective combining the functions has the clear benefit of reducing administrative burden on the CEO or other senior manager to whom the functions would report. A combined function would also make more efficient use of board members time by streamline reporting to the audit/compliance committee. But an even great benefit may come from the improvement in organizational governance by enabling the board members to more effectively meet their responsibilities for oversight of ethics and compliance as well as for overall risk management and internal control. Combining the functions also increases the likelihood that the organization would adopt a common risk management and control framework, further improving the effectiveness of senior management and the board oversight of the organization. For operating managers there is also the benefit of reducing assurance fatigue since a combined function dramatically improve the coordination of auditing and monitoring activities.

At the University of California, we have tried to integrate the risk assessment process with IA and Compliance to leverage efficiencies of the process. Both IA and Compliance develop their own plan but the process of risk assessment is done together, i.e., interviews, collection of related information, etc.. This helps to also enhance viewpoints from each of the perspectives and identify areas which may be common for focus on the new year plan for IA and Compliance.

While there are many similarities in responsibilities between the internal audit function and the compliance function there also key differences. The internal audit function's primary role in the organization is to provide independent, objective assurance to senior management and the board that risks are being managed to an acceptable level, particularly those risks that management has elected to address through internal controls. These risks include the risk that organization will not follow legal and regulatory requirements or will violate the organization's values and internal policies, the same risks with which compliance is concerned. However, the IA function also has concerns over risks regarding the reliability and integrity of financial and operation information, the risks that the organization's assets are not safeguarded, and the risks that the organization will not achieve its strategic and operating objectives.

The compliance/ethics function in contrast works as a change agents in facilitating and assuring that management is addressing key risk areas (such as those listed above from an IA perspective) related to compliance with any rules, regulations, laws and/or policies that must be

followed. Additionally, Compliance must provide assurance that the management mechanisms put into place to resolve compliance risks effectively mitigate the potential and/or real compliance risks identified. Compliance also has the responsibility to assure that anonymous communication methods are in place for employees to raise issues without fear of retribution and/or retaliation.

Another difference in roles is that while IA may take into consideration and provide observations on the ethical culture, for an “effective” compliance program the ethical culture and regulatory compliance must be integrated. The importance of ethical culture in a compliance program has to do with:

- active leadership engagement, management control systems and processes, employee commitment and
- attract good people and encourage them to speak up without the fear of retaliation.

Presently, those higher education institutions that have enterprise wide compliance programs have adapted the “United States Sentencing Commission: Federal Sentencing Guidelines for Organizations, Chapter 8” to build their compliance program. In Chapter 8, seven elements of an effective compliance program are identified and if evident, “credit” will be given towards the sentencing for the criminal violation under consideration. The seven elements (paraphrased) are: standards of conduct, oversight, education, auditing & monitoring, communication & reporting, and enforcement & discipline. Because of the diversity of risks, the different functions and business owners in a university setting, enterprise wide compliance programs are challenging and implemented through different structural models, i.e., centralized, decentralized, hybrid central/decentralized model. Sometimes only the key risks are addressed in compliance programs, i.e., research, athletics, etc. and these programs would not be considered comprehensive in looking at all the risks of the organization.

From an internal audit perspective the issue with a combined IA and compliance/ethics function is the problems of independence of the IA function and of maintaining auditor objectivity. Some take an extreme view of independence as meaning the IA function must be free from any involvement in operational responsibilities. However such a view is not consistent with Internal Auditing Standards or with the standards for internal audit under the Government Auditing Standards as reflected in the GAO, *Government Auditing Standards* (2010 Exposure Draft).

The IIA Standards define independence as:

The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

IIA Standard 1100 states that the internal audit activity must be independent, while internal auditors must be objective. This is a subtle, yet important, distinction. Independence is an attribute of the audit function; whereas objectivity is an attribute of the individual auditor. The attribute of the internal audit function relates to its organizational independence. At the most fundamental level, independence is the ability to conduct internal audit activities without undue influence or control. Objectivity relates to the individual auditor. Standard 1120 describes objectivity of the individual auditors and states that individual auditors achieve this objectivity when they “have an impartial, unbiased attitude and avoid any conflict of interest.” The Standards reflect the notion found in the 2001 IIA Research Foundation study (Jane Mutchler,

Independence and Objectivity: A Framework for Internal Auditors) that objectivity alone is what directly produces the value of the audit. The value that independence brings to the audit table is based on its creation of “an environment that maximizes the likelihood of auditor objectivity.” In other words, in the audit environment depicted by the Standards, the Value Proposition, and related research, independence is significant because it gives the audit activity a level of autonomy that facilitates a major determinant of internal audit value — the individual auditor’s objectivity. By acknowledging that it is the individual auditor’s impartial state of mind that renders value to the audit product, not his or her abstinence from involvement in management and organizational activities, the internal audit team is free to assume a more proactive, preventive, and valuable role in the organization.

What then are the additional threats to auditor objectivity in combined functions and what safeguards can be put in place to mitigate these threats? The most significant threat is where the compliance function assumes or becomes extensively involved in management operating responsibilities. However, emphasis from the Federal Sentencing Guidelines, the enforcement community and the growing reality for compliance programs to be effective, is that there needs to be reporting to the highest levels of the organization, i.e., Board and/or CEO and that there is independence from any management functions. This is difficult for compliance because the areas where this is mostly to occur is the development of organizational policies and procedures, design and implementation of controls to address specific compliance risks, and development and delivery of specialized training of employees. To assure independence, the first safeguard that can be put in place is to have separate staff assigned to the compliance and internal audit responsibilities, staff that is not involved in the conduct of audits. A second safeguard would be to make explicit that while compliance staff can assist in developing and drafting policies and procedures, such policies and procedures are ultimately the responsibility of management and should receive management’s formal approval. A final, and most essential, safeguard is to have a periodic independent review of the effectiveness of the compliance program to provide the objective assurance the board and senior management needs to fulfill their oversight responsibilities. When audit and compliance are separate functions, internal audit can provide this assurance; but when combined it will be necessary to use assurance providers from outside the organizations.

Each organization must determine how to tailor both the compliance/ethics function and internal audit function so as to best meet the organization’s needs. In terms of combining the function, the organization must weigh the potential benefits to organizational efficiency and effectiveness against risk of compromising the assurance provided by internal audit and cost of additional safeguards. Resources are diminishing in higher education but it does not negate the need for either of these functions. They are critical to the survival of our organizations as each of these responsibilities have complimentary influences on the overall culture related to identifying and mitigating risk.