Contrasting Roles and Responsibilities—Corporate Compliance and Internal Audit

By Mark P. Ruppert, CPA, CIA, CISA, CHFP

The focus group of Health Care Compliance Association (HCCA) and Association of Healthcare Internal Auditors (AHIA) members continues to explore opportunities to better define and explain auditing and monitoring, clarify the roles of compliance and internal audit functions as they address issues within their healthcare organizations, and develop guidance and reference materials on key aspects of health care auditing and monitoring processes.

The *Seven Component Framework developed by the AHIA/HCCA focus group* for compliance auditing and monitoring is comprised of the following activities:

- Perform a risk assessment and determine the level of risk
- Understand laws and regulations
- Obtain and/or establish policies for specific issues and areas
- Educate on the policies and procedures and communicate awareness
- Monitor compliance with laws, regulations, and policies
- Audit the highest risk areas
- Re-educate staff on regulations and issues identified in the audit

This article provides the focus group's view regarding the roles and responsibilities of the corporate compliance and internal audit functions. There is no attempt to address the merits of having separate or combined corporate compliance and internal audit functions. Whether the functions are separate or combined, the roles and responsibilities remain essentially the same for each function, though each approach provides reciprocal advantages and disadvantages to an organization, which can best be summarized as follows:

- With separate compliance and internal audit functions, collaboration is more challenging, but functional independence is assured.
- In combined compliance and internal audit shops, collaboration is assured, but functional independence is more challenging.

The focus group categorized the different roles and responsibilities for comparative purposes. This categorization and comparison is summarized in a matrix as Exhibit A to this article. Twenty-two comparative categories were identified: requirement, purpose, reporting, internal authority, span of responsibility, professional standards, high level focus, primary focus from a risk standpoint, activity focus, relationship to management,

Exhibit A

Key Roles and Responsibilities of Corporate Compliance and Internal Audit – Discussion Points

	Internal Audit	Corporate Compliance
Requirement:	• May be required if the organization must comply with Sarbanes-Oxley. • Otherwise, Internal Audit is implemented as an organizational governance/business decision and best practice.	• Federal Sentencing Guidelines • May be required if the organization is under a corporate integrity agreement (CIA). Otherwise, OIG guidance is advisory. • May be required if the organization must comply with Sarbanes-Oxley.
Purpose:	• Provide independent appraisals of governance, risk and control. • Review the reliability and integrity of financial and operation information. • Ensure the safeguarding of assets. • Review operations for consistency with operational goals and objectives. • Recommend operating improvements. • Audit annually the compliance program.	Prevent Fraud and Abuse: • Encourage the use of internal controls to efficiently monitor adherence to applicable statutes and regulations. • Effect change as necessary in the organization to achieve regulatory compliance. • Ensure that compliance policy and procedure exist. • Provide compliance training. • Implement a hotline. Protect and Secure PHI: • Implement HIPAA Privacy Standards. • Implement HIPAA Security Standards.
Reporting:	Independent Reporting to the Board or a Committee of the Board.	Independent Reporting to the Board or a Committee of the Board.
Internal Authority:	Board Approved Charter.	• Board Approved Compliance Program. • May also have a Board Approved Compliance Committee Charter.
Span of Responsibility:	Access to entire organization.	Access to entire organization.

Exhibit A Continued

	Internal Audit	Corporate Compliance
Professional Standards:	Professional Standards: • Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing (SPPIA) • AICPA Generally Accepted Auditing Standards (GAAS) • ISACA Standards IIA Code of Ethics Certified Internal Auditor (CIA) Certified Information Systems Auditor (CISA)	Primarily evident in the Federal Sentencing Guidelines and the OIG Compliance Program Guidance. Additionally, guidance is evident relative to: • HIPAA • Stark • Others like JCAHO, state, etc… • HCCA Code of Ethics • HCCA Compliance Certification Program • Health Ethics Trust and related certification
High Level Focus:	Corporate Governance, Risk and Control: IIA Definition - "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."	Corporate Governance, Ethics and Risk from a Regulatory Compliance Perspective. Preserving corporate integrity and adherence to a code of organization ethics.
Primary focus from a risk standpoint:	Driven by audit planning, which is based upon an organization-wide risk assessment.	Driven by federal and state fraud and abuse investigative agendas, to include Stark, AKS, Intermediate Sanctions, and HIPAA Investigations. Also, by the law, ethics and other regulatory requirements, with consideration of the OIG work plan.
Activity Focus:	Audit/project based, periodic assurance based on concurrent or retrospective reviews.	On-going monitoring and evaluation of the ethical culture and compliance with laws, regulations, policies and procedures. Also, ongoing training related to the above.
Relationship to Management:	Independent with no operational responsibilities. Does not own policies. Consults on policy and other matters related to governance risk and control. ***Management is responsible for implementing internal controls.***	Independent, but with operational responsibility for administering the corporate compliance program. (i.e., owns the compliance program). Individual with operational responsibilities may also be assigned responsibility for corporate compliance; if possible, best practice is for a compliance function to be independent of operational responsibilities. May own policies (hotline, etc.). Consults on policy and other regulatory compliance matters. ***Management is responsible for ensuring compliance with laws, rules and regulations.***
Training Responsibility:	Not responsible for corporate training. May provide training in certain areas i.e. training on the audit process; training to expand knowledge on issues identified as part of an audit.	Responsible for ensuring that new employees/management are oriented on the compliance program, that continuing employees/management undergo annual training on selected topics, and that employees in high risk areas receive appropriate specialized training. Also updates management and the Board on new laws, regulations and government activities.
Auditing:	Auditing is a primary internal audit function. Internal Audit projects are completed in accordance with professional standards.	Compliance can complete audits of operations for which it does not have operational responsibility. However, Compliance audits are not governed by formal audit standards. Typically, compliance officers are responsible for ensuring that management appropriately monitors their staff.
Monitoring:	Not typically an Internal Audit role.	Typical component of compliance program though often completed by departmental management and reported to Compliance. Compliance officer is responsible for ensuring that such management appropriately monitors their staff.
Expertise:	Primarily with internal controls.	Primarily in regulatory matters.
Impact on Internal Audit plan:	Creates and executes.	Provides advice and consultation. Provides input on the types of compliance risk that should be considered in audits.
Impact on Compliance Plan:	Provides advice and consultation. Audits compliance program implementation and evaluates effectiveness.	Creates and executes.
Risk Assessment:	Assesses risk in developing its annual audit plan and in planning individual audit projects. Evaluates the risk management processes in the organization.	Assesses compliance risk in developing its annual work plan.
Follow-up:	Formal follow-up of recommendations made in reports to determine if management has responded accordingly.	Documented follow-up regarding resolution of hotline calls and reported compliance issues.
Investigation:	Typically responsible for investigating fraud, irregularities and other accounting related improprieties. Coordinates activities with Compliance, Legal , Security, IT, HR and other areas as deemed necessary to effectively conduct the investigation. May complete investigations on its own accord, at the request of the Board or Management. Typically supports the Compliance Officer in investigating non-HR related hotline complaints.	Typically responsible for ensuring that all hotline calls and other complaints/inquiries made to the Compliance officer are addressed and resolved in an appropriate manner. May coordinate with or obtain direct assistance from Internal Audit, Legal , Security, IT, HR and other areas as deemed necessary to effectively conduct the investigation. May complete investigations on its own accord, at the request of the Board or Management.
Hotline:	Best Practice	Component of the OIG Model Compliance Program.
Information Systems:	Audits new systems implementation and existing systems controls.	Provides input on necessary compliance controls relative to new systems implementation and existing systems controls. Coordinates with Privacy Officer to ensure proper HIPAA privacy and security controls are in place.
Internal Controls	Evaluate the effectiveness of internal controls.	Understand and encourage the use of internal controls.

training responsibility, auditing, monitoring, expertise, impact on internal audit plan, impact on compliance plan, risk assessment, follow-up, investigation, hotline, information systems, and internal controls. This of course highlights the complexity of attempting to discern the roles and responsibilities, though once addressed it's actually quite easier than it seems.

When looking at the first several categories of roles and responsibilities, especially related to formal standards, the Focus Group identified that internal audit has more history as a profession, and its work is governed by formal standards for the conduct of its work. Thus, internal audit has been accepted and understood by industry boards and executives before corporate compliance programs were conceived. While corporate compliance and internal audit certifications and codes of ethics exist, corporate compliance activities are not yet governed by widely acknowledged standards. From this context then the roles can best be identified, understood and applied by looking first at similarities and then at uniqueness.

Similar Roles and Responsibilities

Corporate compliance and internal audit functions are best served by being independent of the operations they assess. To achieve independence, proper governance, lines of reporting and authority, organizational placement, and organizational access are key to the success of both functions. Since both compliance and audit are focused on helping the organization achieve responsible and effective corporate governance and ethics, best practice corporate compliance and internal audit functions should:

- Report functionally to the organization's board, typically through an audit or compliance committee. This reporting relationship provides each function with the necessary authority to effectively address its responsibilities.
- Function relative to a board-approved program or charter. A board-approved charter documents the established authority.
- Report administratively to the organization's CEO. This reporting relationship ensures that functional administration and resource allocation is not inappropriately influenced by operational areas subject to corporate compliance and internal audit activities.
- Have access to the entire organization per board direction, typically identified in the board-approved program or charter. Compliance and internal audit professionals must have open access to the records and personnel of the organization to ensure unbiased results.
- Recognize and communicate that management is responsible for compliance, and corporate compliance is not. Management is responsible for ensuring its activities comply with applicable laws, rules, and regulations. This fact should be identified in the board-approved program or charter.
- Recognize and communicate that management is responsible for internal controls, and internal audit is not. Management is responsible for ensuring that appropriate internal controls are implemented to meet organizational mission and strategic objectives. This fact should be identified in the board-approved program or charter.
- Have the authority to conduct investigations. In many cases, compliance and audit collaborate to conduct investigations. Depending upon the nature of the investigation, either function may work on their own or in collaboration with other functions like human resources, information technology, legal, and security.

Both functions are also cost centers of an organization, that is, functions that are not designed to contribute directly to the financial bottom line. While both functions often identify cost-saving or revenue-enhancing opportunities, neither should carry that as their primary role. Since they are cost centers, functional resources are limited. Both functions best serve their organizations with these limited resources by fulfilling their responsibilities through focus on the priority or highest risk areas.

Risk assessment is a key component of both functions. Risk assessment involves the application of a methodical process for identifying key risks that face the organization. Both corporate compliance and internal audit address corporate level risk, governance, and control. As defined by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, internal control is broadly 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 in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Internal audit has more history as a profession and its work is governed by formal standards.

Each function addresses corporate level risk, governance and control, and a risk assessment helps each function prioritize resources to effectively address the most important matters. However, the compliance risk assessment is focused on regulatory and other compliance related matters and the internal audit risk assessment is focused on internal control related matters, including controls that affect compliance. Because there is some overlap, coordination of planning efforts typically improves the risk assessment results thereby benefiting both functions as well as the organization.

The focus group issued a previous article that specifically addressed the completion of a compliance risk assessment. You may reference that article for additional details.

Unique Roles and Responsibilities

Exhibit A identifies in detail by category the uniqueness of each function. Exhibit B summarizes the unique roles of each function deemed most notable by the Focus Group.

Exhibit B

Corporate Compliance	Internal Audit
Operations	
While both functions should be independent of operations…	
Corporate compliance functions own the compliance program operations, and supporting policies and processes.	Internal audit must be independent of all areas subject to audit to ensure objectivity. Professional standards prohibit internal audit responsibility for operations.
Auditing and Monitoring	
Understanding the unique roles of corporate compliance and internal audit requires an appreciation for the definitions of auditing and monitoring. The last article published by the Focus Group addressed these definitions as follows: *"Auditing is a formal, systematic, and disciplined approach designed to evaluate and improve the effectiveness of processes and related controls. Auditing is governed by professional standards, completed by individuals independent of the process being audited and normally performed by individuals with one of several acknowledged certifications. Objectivity in governance reporting is the benefit of independence."* *"Monitoring is an on-going process usually directed by management to ensure processes are working as intended. Monitoring is an effective detective control within a process."*	
Compliance ensures that auditing and monitoring for key compliance risk areas occurs. If properly governed and conducted according to professional audit standards, compliance may conduct or engage outside services for the conduct of compliance audits.	Internal audit is responsible for all internal audit activity within an organization. Given the application of formal audit methodology and reporting requirements, internal audit does not complete monitoring activities though its work can sometimes identify the need for and provide the basis for monitoring mechanisms being established.
Follow-up	
Follow-up relates to ensuring that improvement opportunities and problems identified through auditing and monitoring efforts have been addressed by the organization, typically through the efforts directed by management. Follow-up is an effective mechanism to establish management accountability for compliance and internal control. While compliance and internal audit are responsible for following up to ensure remedial actions have been taken.	
Corporate compliance documents follow-up regarding resolution of hotline calls and reported compliance issues. Follow-up reporting to the board is not specifically mandated and is therefore at the compliance officer's discretion.	Internal audit is required to ensure follow-up of recommendations made in internal audit reports to determine if management has responded accordingly. Formal tracking and reporting to the board is also required.
Compliance Program	
A formal documented compliance program is recommended by the Office of the Inspector General. Some organizations are also required to have such programs by corporate integrity agreements reached with the government due to prior significant compliance failures. Compliance and internal audit work in tandem to ensure the compliance programs are functioning and effective.	
Corporate compliance creates and executes the organization's corporate compliance program relative to its role. Management and all members of the organization are responsible for ensuring that compliance with laws, rules and regulations occurs.	Internal audit provides advice and consultation relative to the compliance program. Internal Audit is responsible for auditing compliance program implementation and evaluating program effectiveness.
Compliance Risks	
Compliance risk is the driving need for a corporate compliance program: organizations must ensure that they are taking reasonable measures to comply with applicable laws, rules and regulations, as well as their own policies. Corporate compliance and internal audit have comparable roles relative to addressing compliance risk. However…	
Corporate compliance creates and executes an annual or periodic compliance work plan that ensures compliance risks are being addressed through the use of compliance personnel and management led monitoring activities.	Internal audit addresses compliance risk as part of risk-based audits or in conjunction with corporate compliance coordination and the compliance work plan.
Information Technology	
Information technology presents significant compliance and internal control risks. In many cases such risks are one in the same. Internal auditors/ information systems auditors have been addressing information systems risk for many years and much of the current HIPAA guidance is parallel to such recommendations.	
Corporate compliance provides input on necessary compliance controls relative to new systems implementation and existing systems controls. The function also coordinates with or oversees the privacy officer (and in some cases security officer) to ensure proper HIPAA privacy and security controls are in place.	Internal audit completes audits of new systems implementation and existing systems controls to ensure mitigation of business, compliance and other risks, including HIPAA.

Conclusion

Corporate compliance and internal audit share similar roles and responsibilities, while also maintaining specific, unique roles and responsibilities. These roles and responsibilities are not structured the same in all organizations and, in some cases, are combined. Regardless of how your organization structures these important governance functions, corporate compliance and internal audit are most effective when they work in a collaborative manner, one that includes joint planning and coordination of risk assessment efforts to review for overlapping areas, coordinated reporting to management and the board on significant issues, and shared involvement in key compliance related committees, task forces and other working groups. Understanding the similarities and differences as summarized in this article should help to ensure such collaboration is deliberate and effective.

About the AHIA/HCCA Focus Group

The AHIA/HCCA focus group will continue to address compliance auditing and monitoring directives through white papers, articles, and educational initiatives. The focus group welcomes your feedback and requests to address particular matters related to auditing and monitoring. Please submit your request directly to any member of the focus group. **NP**

Members of the focus group are:

- Mark P. Ruppert
  Cedars-Sinai Health System
- Debi Weatherford
  CHAN Healthcare Auditors
- Randall Brown
  Baylor Health Care System
- Kathy Thomas
  Duke University Health System
- Debra Muscio
  Central Connecticut Health Alliance
- Jan Coughlin
  Scripps Health

Mark Ruppert, CPA, CIA, CISA, CHFP, is the director of audit services at Cedars-Sinai Health System, Los Angeles, California. He is a former chairman of the board of AHIA. He may be contacted at Mark.Ruppert@cshs.org.

Ability will never catch up with the demand for it.

— Malcolm Forbes