Essay Topic:

GRC has evolved rapidly in recent years and Internal Audit has taken notice.

What are the appropriate roles of Internal Audit in GRC and how does internal auditing best support those GRC efforts?

As GRC continues to evolve, which ways do you see internal auditing evolving further to keep with this trend and continue to effectively communicate to stakeholders?
Contents

Acknowledgements ........................................................................................................................................... 2
Introduction ....................................................................................................................................................... 3
Understanding the GRC Framework .................................................................................................................. 4
Internal Audit’s Role in the GRC Framework ........................................................................................................ 7
Governance and the Internal Audit Function ...................................................................................................... 8
Risk Management and the Internal Audit Function ............................................................................................ 11
Compliance and the Internal Audit Function ...................................................................................................... 13
Moving Forward: Areas of Focus in the Future of Internal Auditing ................................................................. 15  
  Analytics ......................................................................................................................................................... 15
  Cybersecurity Vulnerabilities ............................................................................................................................. 16
Conclusion ........................................................................................................................................................... 17
The LSU Flores MBA Program and the LSU Center for Internal Auditing have made a profound impact on my development as both a student and professional over the last two years. The knowledge acquired from participating in these programs is the sole reason why I am able to officially submit this essay to the Institute of Internal Auditors. I would like to thank the following individuals for their tremendous support, guidance, and motivation during my time as a Graduate student at Louisiana State University:

**Glenn E. Sumners, DBA, CIA, CFE, Director, Louisiana State University Center for Internal Auditing**

**Destin Harcus, CPA, Manager, Deloitte Advisory**

**Dana Hart, Director, Louisiana State University Flores MBA Program**

**Seth M. Thibodaux, Associate Director, Louisiana State University Flores MBA Program**

My experiences in interacting with and learning from these individuals have helped shape the work in this manuscript. I hope any knowledge gained from the following pages will benefit industry professionals in the future.
Introduction

In recent decades the business environment has experienced a number of unprecedented issues, surprises, and negative events that have increased organizations’ focus on Governance, Risk Management, and Compliance (GRC) initiatives. These occurrences have dramatically increased the roles and responsibilities of the Internal Audit Function within the organization. Events such as the collapse of Enron, the British Petroleum (BP) Oil Spill, the 2008 Financial Crisis, and the British Exit from the European Union, have shaken the industrial, financial, and environmental grounds with which these disasters were built upon. Over the years, incidents such as these have led directly to legislation which renewed the importance of governance, risk management, and compliance functions throughout the world. As the global business environment grew, so too did the regulatory environment which produced federal workplace regulations, accounting standards, and financial reforms intended to shield the public, environment, and economy from similar future disasters. Coupled with the expansion in technology, regulations abound and gave rise to the emergence of new-age organizational exposures that include but are not limited to cyber security, intellectual property, and business continuity risks. To address these risks and other issues facing organizations worldwide, many board of directors have chosen to implement an overarching framework known as ‘GRC’ that aims to integrate, validate, and optimize a firm’s governance, risk management, and compliance processes.

In an effort to recognize Internal Audit’s role in an organization’s Governance, Risk Management, and Compliance Functions, this manuscript will begin by attempting to fully explain the GRC Framework from the ground up. This explanation will showcase how the GRC Framework is established, what the framework looks like in action, and the particular benefits the GRC Framework can provide to an organization. Next, this manuscript will define and assess Internal Audit’s organizational role within the GRC Framework as a whole. With Internal Audit’s organizational role established, we will dive deeper into understanding each individual function of GRC and Internal Audit’s appropriate role in support of those functions. Throughout the following pages, readers will be provided with images and depictions that aim to better enhance their understanding of the Internal Audit Function and the GRC Framework in its entirety. To conclude, this research paper will address two key areas, analytics and cybersecurity vulnerabilities, that the Internal Audit Function must focus on moving forward if it is to continue to effectively provide value to stakeholders throughout the organization.
Understanding the GRC Framework

In its *Maturity Model for an Integrated GRC*, the Open Compliance and Ethics Group (OCEG) formally defines the GRC Framework as a holistic system of people, processes, and technology that enable an organization to:¹

- Understand and prioritize stakeholder expectations.
- Set business objectives that are congruent with the organization’s values and risks.
- Optimize their risk profile and protect values.
- Operate within relevant legal, contractual, internal, social, and ethical boundaries.
- Provide relevant, reliable, and timely information to appropriate stakeholders.

As organizations become more forward-thinking, the GRC Framework serves as a well-coordinated approach to maintaining all of the functions and capabilities necessary to support optimal organizational performance. Carole Switzer, President of the OCEG, supports this notion and states that the integrated GRC Framework “has the potential to provide organizations with a uniform view of information so as to align risk management with objectives in order to reduce complexity and harness technology for optimal performance.”² Figure 1 depicts the GRC Framework illustrated by *Strategic Finance* magazine.³

---


Establishing the GRC Framework begins when an organization’s Board of Directors and Senior Management Team implement the firm’s Enterprise Risk Policy and Appetite. This policy, approved by the Board of Directors, represents the organization’s strategic approach to managing risk, in part, by determining the appropriate risk appetite of the firm. The Enterprise Risk Policy also establishes the role of each Governance, Risk, and Compliance Function across the organization, represented by the vertical columns in Figure 1. In addition to establishing each function’s role, an organization’s Enterprise Risk Policy defines the overall goal of value creation as well as the expectations for the working relationships and sharing of knowledge amongst employees across the organization. While each function serves a unique role to the organization, the GRC Framework calls to combine these functions with the shared goal of managing risks through integration. The horizontal rows depicted at the bottom of the framework represent the common elements that are intended to be leveraged across each function in order to improve the overall efficiency and effectiveness of the organization’s governance, risk, compliance efforts. Those elements include the sharing of risk assessments, the identification of emerging risks facing the organization, and the monitoring of key risk indicators (KRIs).
With no GRC Framework in place many organizations face the threat of becoming fragmented, vulnerable, and silo’d. When an organization becomes silo’d, "groups or departments within that organization operate inside a vacuum with little functional access to other groups, or little communication with them."4 The leads to delays in the communication of important issues and decisions facing the organization. As a result, many functions can only react to situations as they occur rather than anticipate these issues proactively. This can stagnate the organization, hinder its growth, and eviscerate its value creation. Figure 2 illustrates in greater detail the issues an organization encounters when departments are silo’d and the GRC Framework is absent. As shown, withholding from an integrated GRC approach leads organizations into pitfalls that harm the stakeholder's value and prohibits the organization from achieving its optimal performance.5

However, if adopted and appropriately aligned with the organization the GRC Framework can help ensure controls operate effectively, resources are used efficiently, and risks are addressed as intended. Figure 3 illustrates this by depicting an organization with the GRC Framework in place. This organization experiences streamlined processes, integrated data-sharing, and a common dialogue throughout the entire enterprise. As a result of these benefits, the organization as a whole experiences

---


lower cost associated with the management of their controls. Most importantly, however, is the assurance provided to the board and senior management that the entire system of internal control is effective and high-performing.

Internal Audit’s Role in the GRC Framework

As a primary component of the GRC Framework, the Internal Audit Function is uniquely positioned to support an integrated, proactive organizational environment that strives to achieve optimal performance. In this position it is easy to recognize the immense responsibilities of the Internal Audit Function in each individual field of Governance, Risk Management, and Compliance. Yet in order understand the Internal Audit Function’s position in guiding and supporting the GRC Framework, the role of the Internal Audit Function must first be acknowledged. The Institute of Internal Auditor’s International Professional Practices Framework (IPPF) defines Internal Auditing as:
An independent, objective assurance and consulting activity designed to add value and improve an organization’s operations.  

As an independent and objective function of the organization, two essential ways in which the Internal Audit Function provides value to an enterprise is by (1) providing objective assurance that major business risks are being managed appropriately and (2) assuring that the enterprise-wide risk management and internal control framework is operating effectively. The Institute of Internal Auditors (IIA) view the Internal Audit Function in these roles as “helping an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.” Given the proper support, the Internal Audit function can also aim to analyze and interpret information to help management identify the major business challenges facing the firm. Further responsibilities of Internal Audit Function within the GRC Framework include the following.

- Assisting in the development of an enterprise-wide risk management (ERM) strategy.
- Making recommendations on systems and processes.
- Offering best practice advice and implementation assistance.

The Internal Audit Function should also look to quantify potential areas of cost savings for the organization and balance the goal of establishing adequate organizational controls with the goal of creating efficient and effective operations. Recognizing and understanding these responsibilities prove the Internal Audit Function serves as a key component in the continuous effort to bridge the gaps between an organization’s Governance, Risk Management, and Compliance Functions.

### Governance and the Internal Audit Function

Sir Adrian Cadbury, contributing author to the 1992 *Commission Report on Corporate Governance*, once stated that governance is “concerned with holding the balance between economic and social goals and between individual and communal goals.” Governance, therefore, is not only set up to encourage the efficient use of resources but also necessitates accountability for the stewardship of those resources.

---


As Sir Cadbury explained, “The aim is to align as nearly as possible the interests of all individuals, corporations, and society.” Establishing and maintaining a culture of sound governance should be a top priority for all Board of Directors, especially when considering the potential harm an organization can experience for failing to do so. In fact, when surveyed on this matter, nine in ten business leaders stated that they believe culture to be important to a robust and actionable governance framework. Failing to establish a culture of effective governance is a serious threat that can bring down seemingly even the most prominent of institutions. As an example, consider the origination of the 2008 Financial Crisis. In wake of the global recession, there remains a justifiable and persuasive argument that the economic failures of major U.S. financial institutions brewed from shortfalls in corporate governance. Jefferson Wells’ position paper titled “Internal Audit: From Corporate Policeman to Strategic Partner in GRC Success” suggests that at a simplistic level, management deployed overly complex financial products that hindered effective supervisory and governance controls. In addition to the dubious and unethical practice of approving loans with a high probability of default, this lead the United States to experience its worst economic downturn since the Great Depression.

To effectively govern an organization, Board of Directors should be held to three legal standards: Duty of Care, Duty of Loyalty, and Duty of Obedience. According to The Bridgespan Group, Duty of Care describes the level of competence that is expected of a board member. It is expressed as the care that a reasonably prudent person would exercise in the same position and under similar circumstances. Duty of Loyalty is the Board of Director’s standard of faithfulness. It asserts that a board member should never use information obtained from his or her position in the organization for personal gain. Instead, the board member must act in the best interest of the organization. Finally, Duty of Obedience requires that board members be faithful to an organization’s mission. By doing so, they are not permitted to act in a way that is inconsistent with the central goals of the organization.

To reduce the possibility of infringing upon the duties owed to an organization’s stakeholders, the Board of Directors should work with Senior Management and the Internal Audit Function to: (1) establish ethical codes and policies, (2) decrease vulnerability to fraud and misconduct, (3) create sound

---

9 Sir Adrian Cadbury, UK, Commission Report: Corporate Governance 1992
upward feedback channels, (4) regularly communicate cultural values and behaviors to every member of the organization, and (5) demonstrate integrity and advocate corporate responsibility.

Oftentimes, Senior Management and the Board of Directors will call upon the Internal Audit Function to help provide assurance that risks are appropriately identified and monitored and organizational processes are effectively controlled. The IIA’s Performance Standard 2110 expands on this role and states that the Internal Audit Function must assess and make appropriate recommendations for improving the governance process of an organization in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Effectively communicating risk and control information to appropriate areas of the organization.
- Coordinating and communicating information among the board, internal and external auditors, and management.

More recently, governance has expanded to also include management’s crucial role in setting the “tone at the top”, or rather, the organization’s commitment towards openness, honesty, integrity, and ethical behavior. This expansion requires that the Internal Audit Function be mindful of potential conflict with management when assessing the effectiveness of the organization’s governance processes while simultaneously reporting to the Audit Committee of the Board of Directors regarding the “tone at the top”. To adhere to this responsibility, the Internal Audit Function should, at least annually, carry out an assessment regarding the overall effectiveness of the GRC Framework in the organization. Upon completion, the results of this assessment should be communicated directly to the organization’s board. The Internal Audit Function should also work to ensure the organization’s internal control framework is operating effectively by assessing, evaluating, and reporting on the enterprise’s:

- Board composition regarding skills, experience, independence, etc.
- Audit committee activity and involvement in risk oversight
- Legislative and Regulatory requirement compliance
- Business conduct and ethics

---

12 Practice Advisory 2110: Governance Definition, Institute of Internal Auditors
Risk Management and the Internal Audit Function

Although an organization’s Board of Directors has ultimate responsibility for ensuring that risks are managed appropriately, in practice, this responsibility is often delegated to the senior management team. One popular framework seen across organizations today is the Committee of Sponsoring Organization’s (COSO) Enterprise-wide Risk Management (ERM) Framework. Defined as “a structured, consistent, and continuous process across the organization,” ERM is utilized in “identifying, assessing, and deciding on responses to opportunities and threats that affect the achievement of organizational objectives.”

Following the release of the ERM Framework, many audit professionals debated the role the Internal Audit Function should assume in the risk management process. COSO’s ERM Framework directed the Internal Audit Function to “assist management and the board of directors by examining, evaluating, and reporting on the adequacy and effectiveness of the organization’s enterprise risk management” (COSO 2004). According to John Hall, recipient of the IIA’s 2007 Esther R. Sawyer Research Award, this shift of internal audit from a traditional monitoring and assurance role to one of consulting and general oversight of the entire risk management process, was not wholeheartedly embraced nor was it fully understood.

Some organizations instructed internal audit departments to assume ownership over business risks while others restrained the Internal Audit Function to a strict monitoring role.

In response to this incertitude, the IIA released the position paper “The Role of Internal Auditing in Enterprise-wide Risk Management.” This position paper suggested particular ways for internal auditors to maintain the objectivity and independence required by the IIA’s professional standards while providing assurance and consulting services (IIA 2004). More importantly, this paper clarified which roles the Internal Audit Function should and should not be involved in throughout the ERM Process. The IIA divided these roles into three key areas: (1) core internal audit roles in regard to ERM, (2) legitimate internal audit roles with safeguards, and (3) roles internal audit should not undertake due to independence impairment.

---

The IIA organized this information into a graphic, shown below, which is commonly referred to as the “ERM Fan”.

**Figure 4: The ERM Fan**

Within the ERM Framework, the core role of the Internal Audit Function is to provide objective assurance to the board relating to the effectiveness of risk management (IIA 2004). By doing so, the Internal Audit Function, in both its assurance and consulting roles, can prove to be a valuable contributor in the management of an organization’s risks. It is important to note the key factors to take into account when determining internal audit’s role in ERM are (1) whether the activity raises any threats to the audit function’s independence and objectivity and (2) whether it is likely to improve the organization’s GRC processes (IIA 2004). From Figure 4, the activities on the left side of the ERM Fan are assurance activities that internal audit, operating in accordance with the *International Standards for the Professional Practice of Internal Auditing*, can and should perform. These activities include, among other responsibilities, providing assurance that risks are correctly evaluated and reviewed. The middle section of the ERM Fan represents the legitimate consulting roles that the Internal Audit Function may assume in ERM with safeguards in place. Some of these consulting roles include but are not limited to (IIA 2004):

- Championing the establishment of ERM in the organization.
- Making available to management the tools and techniques used by internal audit to analyze risk and controls.
• Promoting the development of a common language and understanding throughout the organization.

Activities listed in this section of the ERM Fan typically require enhanced safeguards to be in place when the Internal Audit Function is engaged so that objectivity and independence can be maintained. Notwithstanding, it is unlikely that the Internal Audit Function will be prepared to engage in the consulting activities listed in the middle section of the ERM Fan unless the risk-based assurance functions to the left of the ERM Fan are put in place first (IIA 2004). To the far right of the ERM Fan are the roles which the Internal Audit Function should not undertake. If assumed, these roles can severely compromise the independence and objectivity requirements set forth in the IIA’s Professional Standards (IIA 2004).

Compliance and the Internal Audit Function

The International Compliance Association (ICA) describes ‘compliance’ as the ability to act according to an order, set of rules, or request. More specifically, it is the means by which an organization proactively ensures that regulatory and business requirements are met. The ICA asserts an organization’s compliance function typically operates at two varying levels:

• Level 1 – Ensuring compliance with external rules that are imposed upon the organization as a whole (i.e. Regulatory requirements)
• Level 2 – Ensuring compliance with the internal systems of control that are imposed to achieve compliance with Level 1

To understand Internal Audit’s role in support of the Compliance Function, it is important to recognize that these functions serve distinct organizational roles. Internal Audit’s objective is fundamentally assurance – looking at the past and present to provide assurance that all activities are being carried out according to written policies and procedures. On the other hand, the Compliance Function’s objective is fundamentally operational. This function is concerned with ensuring that all activities carried out by the organization are in compliance with the prevailing regulatory requirements. Therefore, as a component of management, the Compliance Function is positioned to serve as a valid contributor in the effort to achieve optimal organizational performance.

Nevertheless, as a major part of the internal control environment, the Compliance Function should be subjected to independent audits along with the Governance and Risk Management Functions of an organization. To ensure the activities of the Compliance Function are subjected to an independent
review, the Basel Committee on Banking Supervision specifically mandates the Compliance and Internal Audit functions be separated.\textsuperscript{19} Thus for effective coordination of activities between these two functions to occur, it is essential the Internal Audit and Compliance Functions leverage a common language of risk and control. This will allow the functions to adequately provide transparency in their reporting to management and the board. Since both functions are focused on helping the organization achieve effective corporate governance and management of risks, best practices should be adopted, shared, and implemented.

One best practice shared between both functions is reporting functionally to the organization’s Board of Directors. The Internal Audit Function accomplishes this role in its relationship with the Audit committee of the Board of Directors, while the Compliance Function reports, respectively, to an established compliance committee. This reporting relationship provides each function with the necessary authority to effectively address their responsibilities. Both functions should also be granted access to the entire organization, provided the board’s permission. In order to ensure unbiased reporting results, compliance and audit professionals must have open access to all records and personnel of the organization. This role is traditionally established in the board-approved charter. The ability and authority to conduct independent investigations is yet another example of the shared responsibilities between each function. In many cases, compliance and internal 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 of an organization (e.g.: human resources, legal, informational technology, etc.). One of the most important roles of each function, however, is the undertaking of risk assessments. These assessments involve the application of a methodical process for identifying key risks that organization faces. As each function works to assess the level of an organization’s governance, risk management, and overall control, conducting risk assessments will help each function prioritize the resources needed to effectively address the most important issues. For sake of clarity, risk assessments conducted by the Compliance Function are primarily focused on regulatory matters. On the other hand, risk assessments managed by the Internal Audit Function are traditionally focused around internal control matters. Due to the natural overlap experienced in these assessments, coordination of planning efforts should greatly improve risk assessment results, thereby benefiting both functions and the organization.
Moving Forward: Areas of Focus in the Future of Internal Auditing

In any organization, there are numerous areas where the Internal Audit Function’s objectivity, perspective, and skills can provide value to stakeholders. With roles and responsibilities spanning throughout an organization’s Governance, Risk Management, and Compliance Functions, it is clear to see the Internal Audit Function has the potential to profoundly impact the efforts to achieve organization’s objectives. Nevertheless, firms are continuously innovating and growing, resulting in constant change and new ventures for the Internal Audit Function to recognize. To avoid becoming irrelevant internal audit must evolve into a more future-oriented and dynamic function. This belief stems from a study conducted by Deloitte Touche Tohmatsu Limited, which surveyed more than 1,200 Chief Audit Executives in 29 countries across eight industries.16 In the study Terry Hatherell, Global Internal Audit Leader for Deloitte, states “In less than a generation, the business world has been transformed in terms of methods, markets, technologies, regulations, and risk. The results of the survey indicate internal audit must evolve in specific ways in order to meet those needs.” Moving forward this raises the question, “Where can Internal Audit have the most impact and influence?” While the specific course of action largely depends on each Internal Audit Function’s particular circumstance, impact and influence typically increases when Internal Audit attends to the areas of greatest risk, importance, and concern to key organizational stakeholders. With this in mind, two areas of focus for the Internal Audit Function to consider on its path forward include: (1) the use of analytics in conducting audits and (2) the assessment of an organization’s cybersecurity vulnerabilities.

Analytics

Analytics hold serious power and potential to transform the Internal Audit Function and the value it provides to an organization. Key examples of areas where analytics can be applied include information technology cost containment and execution risks related to capital projects and organizational transformations.17 Despite obstacles to implementation, such as shortage of skilled talent, data quality, and date availability issues, the cost and complexity of analytical tools have drastically fallen while their value to the Internal Audit Function has skyrocketed. Analytics also provides the opportunity to boost

---


efficiency and effectiveness in a range of audit activities. This enables the Internal Audit Function to provide foresight into risks and areas of interest for stakeholders. Leading audit functions have only begun to use data visualization tools such as heat maps, bubble charts, and interactive graphics to report on audit results as well as to derive insights from analytics. Alternatively, predictive analytics, an increasingly popular form of advanced analytics, enable the Internal Audit Function to provide a forward-looking analysis of possible control breakdowns an organization can face. According to Deloitte’s 2017 Internal Audit Insights: High Impact Areas of Focus, organizations should attempt to “home-grow” their analytical talent, but co-sourcing may help to get enterprise beyond basic analysis to more advanced analytic techniques. Nonetheless, if utilized correctly, the power of analytics can provide great value to both the organization and the Internal Audit Function.

**Cybersecurity Vulnerabilities**

Assessing cybersecurity vulnerabilities are an additional area of emphasis for internal audit functions moving forward. The rise of the sophisticated cyber-criminal has become one of the fastest growing security threats facing organizations to date. Consider, for example, the recent cyber-security breaches of large corporations such as Sony, Target, Yahoo, Home Depot, and Ebay. These breaches have put millions of people in harm’s way. The landscape of today’s cyber-crimes feature “malware exploits” than can routinely evade traditional security controls.18 With this understanding, it is clear to see that responding reactively to these threats are no longer sufficient to deal effectively with this level of ingenuity. As a result, boards have begun to seek out the Internal Audit Function’s independent, objective, and comprehensive assessment of cybersecurity risks facing the organization. Legislative and Regulatory Agencies are also seen driving this trend. The Cyber-Security Systems and Risks Reporting Act, proposed to the U.S. Congress on April 26th, 2016, could expand SOX reporting requirements to include cybersecurity systems and risks. Proposals such as this reflect the widespread recognition that cybersecurity protection is critical to organizational performance and value.

To support this evolving trend, the Internal Audit Function should work to strengthen their plans and capabilities accordingly. Given the shortfall of cyber auditing skills in the marketplace, audit functions should look to co-source respective responsibilities to help maintain effective cyber-security capabilities. Due to the high impact and varied level of risks associated with cybersecurity (including

---

18 Internal Audit Insights: High-Impact areas of focus (pp. 6-8, Rep.). (2016). Deloitte.
brand, relationship, and reputational risks), the Internal Audit Function should begin to conduct independent and objective reviews of their cybersecurity functions in the near-term. Internal Audit must also define a cyber-auditing approach that meets the needs of both the industry and organizational standards. Finally, the audit plan should prioritize the processes and capabilities to be audited and define methods of related internal audits. Only then can the Internal Audit Function gather the appropriate resources (i.e. people, skills, tools, etc.) needed to effectively execute on those plans.

**Conclusion**

In the absence of an integrated GRC Framework— one that provides transparent and accurate information on which to base risk-intelligent decisions – organizations can be significantly constrained. As an independent and objective function of the organization, Internal Audit offers the most value when it identifies risks and provides objective assurance that those risks are being managed appropriately. To provide this value the Internal Audit Function should be independent of, but closely aligned with, an organization’s Governance, Risk Management, and Compliance Functions. In support of the Governance Function, Internal Audit should work to ensure that an organization’s ethical codes and cultural values are appropriately communicated to all stakeholders. Management’s commitment to ethical behavior (i.e. “Tone at the Top”) should also be assessed and reported on, at least annually. Within the Risk Management Function, Internal Audit should aim to align itself as closely as possible with the roles established by the IIA and depicted in ERM Fan. In doing so, the Internal Audit Function can remain independent and objective while providing value-enhancing service to the organization. To ensure consent with applicable rules and regulations, it is imperative that Internal Audit establish a common language with the Compliance Function. Establishing this language allows both functions the opportunity to identify risks facing an organization, report on the effective of controls that are in place, and advise the business on appropriate action when necessary. If an organization chooses to adopt the GRC Framework in response to the complex business environment, stakeholders can rest assured that the enterprise’s functions are integrated and high-performing. Only then does an immense opportunity exist for the Internal Audit Function to improve an organization’s risk coverage, business operations, and competitive advantage. Moving forward the Internal Audit Function should begin to focus more time, energy, and resources on identifying emerging trends, such as cybersecurity vulnerabilities, that could represent areas ripe for risk assessment. Finally, with the power and proper use of data analytics, the
Internal Audit Function can drastically strengthen its value to the organization by providing guidance in foresight of risks.