Present and Future of Internal Auditing in GRC – Governance, Risk Management, and Compliance

Submitted by:
Wanyin Yan
University at Buffalo
March 1, 2017

Essay Topic:
• 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 audit evolving further to keep with this trend and continuing to effectively communicate to stakeholders?

Submitted to:
The Institute of Internal Auditors Research Foundation
Table of Contents

Acknowledgements.......................................................................................................................... ii
About the Author ............................................................................................................................ ii
Executive Summary ........................................................................................................................ iii
Introduction ....................................................................................................................................... 1
Function of Internal Auditing in GRC ............................................................................................. 1
  Internal Auditing in GRC - Governance ....................................................................................... 2
  Internal Auditing in GRC - Risk Management ............................................................................ 2
  Internal Auditing in GRC - Compliance ...................................................................................... 3
Future Evolvement of Internal Auditing in GRC .......................................................................... 4
  Keep up with emerging technology ............................................................................................ 4
  Establish and maintain good relationships with several different entities ............................... 4
  Lessons learned from failures ...................................................................................................... 5
Effective Communication with Stakeholders .................................................................................. 5
  Communicate in a timely manner ............................................................................................... 6
  Communicate comprehensive information ............................................................................... 6
  Communicate through appropriate methods .............................................................................. 6
Conclusion ........................................................................................................................................ 7
List of Figures ................................................................................................................................... 8
References ......................................................................................................................................... 9
Acknowledgements
The author would like to thank The Institute of Internal Auditors Research Foundation (The IIARF) for the opportunity to participate in this research award competition. I am grateful for the significant knowledge and insights that I was able to obtain during the process of completion of this IIA research essay.

The author also sincerely thanks Alex B. Ampadu, CPA, CMA, CIA, CFE, FCPA, CEE, CGMA, and other faculty in the Accounting and Law Department within University at Buffalo for their teaching and instructions over the past several years. During the time period to complete this research essay, Professor Ampadu provided his generous support and encouragement to the author, which greatly inspired the author to generate and innovate ideas about the research topic. This paper would not exist without his support.

About the Author
Wanyin Yan was born and raised in Guangzhou, China and has come to the United State to study for accounting for both her Bachelor and Master of Science (BS/MS) degree. As an accounting graduate student in the accounting program at University at Buffalo, she previously served as an intermediate course assistance for junior students in the accounting program.

Wanyin had been very involved in organizations within the School of Management at University at Buffalo during her undergraduate time. She was an active member of Beta Alpha Psi, an accounting and finance honor society, and Delta Sigma Pi, an internal professional fraternity. Through her involvements in this two clubs, she greatly developed her knowledge in profession in accounting and various soft skills that could be applied in her future career. In this year, Wanyin will obtain her MS in Accounting degree with a specialization in Internal Auditing, and she will devote her best efforts to pass the Certified Public Accountant exams.
Executive Summary

Jose Tabuena, a former compliance officer of both On Lok Senior Health Services and Texas Health Resources, and a current principal consultant for PrincipledEdge, stated:

“When effectively deployed, GRC can help ensure controls are appropriate, operate effectively, address risks as intended, and use resources efficiently. Importantly, an integrated review of GRC processes by IA can help provide assurance to the board and senior management that the entire system of governance, risk, and compliance is effective and high performing.”

The idea of “GRC” – Governance, Risk Management, and Compliance was brought to our attention more than ten years ago, but it has not been quite noticed until these recent years. The Institute of Internal Auditors (IIA) believes that internal auditing could play important roles in an organization in adapting GRC.

The fundamental rule for GRC to work is that Governance, Risk Management, and Compliance within an organization have close relationships or interconnections with each other. Organizations should not manage these three elements separately, or there would likely be duplicate controls, systems, or even conflicts of instructions within these three elements. Internal auditors should realize their role in each of the element, and they should use resources that can be shared among GRC and put values that are created in one element to the other two elements.

In this paper, I describe internal audit function in Governance, Risk Management, and Compliance, respectively. I also provide some examples of how internal audit function can impact all three elements at the same time, which align with the rule of interrelationships between GRC.

I also introduce the ways of how internal auditing will evolve further in GRC. In the further future, internal auditors will need to adapt to the constant changings of technology; establish and maintain good relationships with the Board of Directors (the Board), the audit committee, the governing body, and senior management; learn lessons from internal failures and some real life examples of failures of GRC in other firms.

At the last part of the paper, I suggest how internal auditing should continue or even improve effectiveness of communications with its stakeholders. To do so, internal auditors should report to the stakeholders in a timely manner; provide comprehensive information of internal audit work they perform; and communicate with the stakeholders using their preferable methods.

Finally, in my conclusion of the paper, I restate the purpose of GRC for an organization and the importance of internal audit function to support and implementation of the GRC approach because internal auditing has more comprehensive knowledge and insights about the governance, risk management, and compliance perspectives within an organization.
Introduction

What exactly is “GRC”? There is no a clear definition of the term. The Open Compliance and Ethics Group (OCEG) provides the following definition: “GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives while addressing uncertainty and acting with integrity – this is the outcome that we call Principled Performance.”\(^2\) Governance, risk management, and compliance seemed to be three separate elements for organizations to successfully achieve their business objectives, but “GRC” is more than just an abbreviation of them – it is more like a strategic tool which emphases to enhance interrelationships between these elements and manage them on a more collaborative basis so that organizations can better and more quickly achieve their business objectives.

Traditionally, internal auditing is considered to be a role to provide reasonable assurance of operation effectiveness and quality of an organization’s governance, risk management, internal controls to mitigate risks, and compliance. However, with increased notice of internal auditing and the added-values that it can bring to an organization, many organizations have started to put more reliance on internal auditing, and even start requesting internal auditing to play a role in strategic transactions.

GRC approach will not be possible to function effectively without collaborations between many departments, such as Compliance and Legal Department, Risk Department, and HR Department, the Board and senior management, and of course, the Internal Audit Department.\(^3\)

It is time for us to think: what roles can internal auditing play in GRC and in what ways that internal auditing supports GRC efforts?

Function of Internal Auditing in GRC

As mentioned above, the foundation for integrated GRC to work is to discover and enhance the interrelationships between Governance, Risk Management, and Compliance. Below are some common relationships between these three elements:

- For governance, senior management will need to set the risk appetite for the organization and then determine business objectives that align with the risk appetite, which set the benchmark to be considered in risk management while assessing and controlling the risks;
- Risk Management involves management of internal and external risks. External risks include legal and regulatory compliance risks - other than business failure, organizations probably are mostly concerned about compliance risks because every single operation within the business can involve rules, regulations, and other legal issues;
- An organization must acknowledge about the compliance requirements to develop a comprehensive governance structure.

In fact, in the processes of handing these three elements, organizations will often use some same resources, such as people, technologies, and information. Furthermore, one element may create information or resources for the other two elements. Based on these two simple point of perspectives, we can know that if an organization manage these three activities separately, it would very likely to waste many unnecessary resources or result in unpleasant outcomes.
Thus, to help implement the integrated GRC approach within the organization, internal auditing should play a cross-functional role within the organization.

**Internal Auditing in GRC - Governance**

Governance is an overall management approach used by the Board senior executives to guide the entire organization by ensuring critical decisions and strategies are delivered to and executed by managers. Without appropriate and effective governance, organizations could easily lose their track to succeed and develop their business. At the entity level, the Board and senior management should create a governance structure to oversee the implementation of GRC framework by setting up goals, policies, and other high-level strategies related to GRC. In addition, organizations should identify the relationships between their business objectives and GRC. For example, to ensure its legitimate operations of online sales, Amazon needs to recognize important legal requirements and regulatory guidelines that regulate online retail sales; creates company policy and procedures to ensure the compliance with such requirements; provides instructions for risk management about such compliance risks. Similar to what it does in Risk Management, internal auditing should play a role of evaluating the design and operation effectiveness of the governance structure; and providing suggestions and guidance for the organization to improve its governance structure.4

Here are some highlights of key activities of internal audit in assisting its board and audit committee for their responsibilities in governance (Florea)5:

Insert Figure 1 here

*Figure 1 – Internal audit assisting activities in governance (figure created based on source from Florea)*

These activates above show that internal auditing has cross-functions among GRC, which emphasizes its critical role for the effective and efficient implementation of GRC.

**Internal Auditing in GRC - Risk Management**

Risk management requires management personnel to identify, assesses, and manage to mitigate the risks that could interfere the achievement of business objectives. Familiarly with accounting professions, the Enterprise Risk Management (ERM) framework is a valuable tool that enables organizations to do so. Generally, internal auditing plays a core role in regard to ERM in five areas: giving assurance on the risk management processes, giving assurance that risks are correctly evaluated, evaluating the reporting of key risks, and reviewing the management of key risks; it also play safeguard role in some other areas, such as coordinating ERM activities and coaching management in responding to risks (see figure 1). In summary, internal auditing plays roles as a reviewer, monitor, evaluator and counselor in Risk Management.
Below is a figure of internal auditing’s role in Enterprise Risk Management.

Insert Figure 2 here

Figure 2 – Internal auditing’s role in ERM

Using the GRC approach, while evaluating the adequacy of the design of internal controls and effectiveness of the controls, internal auditing should consider overlaps areas in risk management that can support the organization governance structure. For example, internal auditors find out that there are several managers who does not authorize business transactions in accordance to the organization’s policy, internal auditors could communicate to the Board about the issues. The Board may realize the lack of oversight of the management personnel and they would adjust the organization policies about management and host more frequent management meetings to address the issues.

Notably, there are risks associated with GRC if departments involved do not function effectively as they should be. In such case, GRC activities can result in problems, for examples, requiring higher expenditures, failure to address third party risks, and more negative surprising outcomes. For example, risk management would be optimal if it can identify the critical risks and put appropriate controls (both quantity and quality) to mitigate such risks. However, if management does not realize the risk appetite of an organization, which is a discrepancy of governance and risk management, management may overly spend resources to mitigate an immaterial risk or have any forms of aggressive and excessive risk management.

Thus, internal auditing should work closely with the departments involved in GRC to help ensure that governance, risk management, and compliance are working hand-in-hand. Putting it into simple words, internal auditing should help governance, risk management, and compliance function “on the same page” within an organization.

Internal Auditing in GRC - Compliance

Compliance, at the organizational level, can be simply described as complying with established guidelines and requirements. One key role of internal auditing in compliance is to monitor whether or not the organization is operating in compliance with rules and regulations. Another key role it has is to provide assistance for the organization to adapt new regulations. For example, for the change of requirements in revenue recognition, internal auditors should get familiar with the changes and act as a consultant while the organization is working in adapting the new requirements. Moreover, internal auditing can also be a “reporter” of the changes of regulations that affect their organization. By communicating such changes or requirements with the Board and senior management, internal auditing helps the enhancement of governance of compliance in the organization.
Keep up with emerging technology

There are two views of the significance of such requirement for internal auditors. First, the dramatic increased necessity for an organization to control and mitigate technology risks. In the generation of explosion of technology, businesses gain incredible benefits from it. Nevertheless, on the other hand, the inherent risks associated with technology are also incredibly increased. In 2015, The World Economic Forum (WEF) released an annual report named “Global Risks 2015”. In the Global Risks Landscape 2015 graph, the risk of critical information infrastructure breakdown and the risk data fraud or theft were placed in the middle-high risk area, while the risk cyber-attacks was placed in the high risk area. Due to the unavoidable trend of growth in technology, internal auditors should be very open to technology changes and be willing to consistently learn about or acknowledge of new technology - at the minimum level, the new technology related to the business of the organization for which they work. Because of the widespread use of computer systems in organizations, Information Technology (IT) Internal Auditor has been introduced. This is a strong proof of the need for specialized internal auditors for tremendous information and technology risks. Second, internal auditors will be able to use the updated technology to increase efficiency and quality of their work. Emerging technology provides internal auditors more possibilities to analyze great amount of data and information within a short time period. Some of my accounting professors and some accounting professionals that I met before told me twenty years ago, how they used to need to use pens to document evidences during an audit; used an amortization table to re-compute the correct amortization for bonds payable premium or discount by hand; how many pieces of paper they needed to use during one audit. Could you imagine us doing everything by hand anymore?

Establish and maintain good relationships with several different entities

According to the Three Lines of Defense model in a PowerPoint from IIA (see figure 2), there are several different entities that internal auditors are accountable for, including the Board, the audit committee, the governing body and senior management. Internal auditors of organizations should establish and maintain good relationships with these entities to accelerate and improve the adoption of GRC within organizations. For example, when a good and solid relationship is established, it is more likely that senior management would consult internal auditors before making a decision, which could help optimize the decision made regarding governance, risk management, or compliance area. Moreover, internal auditors can gain more easiness to ask for assistance from the management or the Board while performing internal audit work. The Board and senior management make most of the strategic decisions for the organization, and they perform the overall governance of the organization, so as to better support the GRC strategic approach, internal auditors should maintain good relationships with them. Below is a figure of the Three Lines of Defense model.

Insert Figure 3 here

Figure 3 - The Three Lines of Defense model
Importantly, a good relationship between the audit committee and internal auditors could bring significant values to the organization. Internal auditors report their work and any findings in their work to the audit committee of the organization. The audit committee is responsible to discuss any reported issues with the Board and then address issues to management to solve them. If internal auditors routinely report to and communicate with the audit committee, the organization could be able to address and solve internal issues in a timelier manner. Furthermore, although, generally, the audit committee oversees the work of internal auditors, internal auditors could in fact provide their insights of the internal audit function of the organization to the audit committee. With insights and reflections from internal audit, the audit committee may work with the Board and senior manager to improve the governance of internal auditing.

**Lessons learned from failures**

I believe that it will be a very meaningful and useful way for internal auditors to learn lessons from previous internal failures or real-life examples regarding governance, risk management, and compliance issues.

Internally, if there were previous issues happened within the organization, for example, an employee sold customer information to a competitor of the organization, internal auditors should review the case to identify whether there was no internal control put into place or the controls were not effectively operated. Then, internal auditors could provide their opinions to management so that the management could make implementation of some controls or improvement of controls that have been put in place.

Externally, internal auditors can learn lessons by reviewing discovered real-life fraud cases. By doing so, internal auditors would be able to identify the internal control weaknesses that are in those cases. Thus, internal auditors could check if their organization has such controls or could reevaluate the design and operation effectiveness of the controls.

For example, in 2013, Target’s credit-card breach raised significant attention from the public about the credit card risk and information security. This accident brought quite a large amount of monetary losses to Target, but more crucially, the damage of its reputation and image among the public. In a case study of the Target credit-card breach, the author listed twelve attack vectors related to the breach, with the Critical Controls listed next to each of the attack vector (a full list of 20 Critical Controls have been introduced by the SANS Institute, a cooperative research and education organization that specializes in information security, to help prevent and detect known attacks effectively). Through study of cases like this case, internal auditors, especially the ones in technology-related company, could more easily assess and evaluate the controls within the organization.

**Effective Communication with Stakeholders**

Other than entities within the organization, internal auditors are also accountable for the stakeholders of the organization. More effective communications between internal auditors and stakeholders is demanded due to increase in expectations from the stakeholders in internal auditing - it will be expected to provide more trusted advisory services to both the organizations and the stakeholders. According to an internal audit profession study report issued by PricewaterhouseCoopers (PWC), “…a number of stakeholders are expecting more from internal audit functions: Overall, 62% of
stakeholders expect more value from internal audit, including almost half of those already receiving significant value.”

Effectiveness in communication with stakeholders includes the time manner, content, and the communication methods:

Communicate in a timely manner
Stakeholders will expect to obtain information and opinions from internal auditors in a timely manner because the information can greatly impact their decision about the investments in the organization. Internal audit report should be communicated with the stakeholders in a monthly or quarterly basis, or any time period based on the needs of the stakeholders.

Communicate comprehensive information
In fact, internal auditing communicates with its stakeholders through an intermediary, the audit committee of the organization. To ensure internal audit information is effectively delivered by the audit committee to the stakeholders, it is important that internal auditors provide comprehensive information to the audit committee.

First, internal auditors should report to the audit committee every area on which they perform internal audit work within the organization, including the organization’s governance, risk management, and compliance activities. Second, both the quality and outcomes of the internal audit work should be communicated to the audit committee. For example, internal auditors can report to the audit committee in what extent they perform the internal audit work and what findings they discover, and moreover, probably some opinions from the internal auditors about the issues. Third, internal auditors should also update any decisions, plans, or changes they make in the Internal Auditing Department with the audit committee. The audit committee will then inform such information to the stakeholders, which helps maintain stakeholders’ knowledge about the internal audit function of the organization, increase transparency of the Internal Auditing Department, and obtain more reliance and trust from the stakeholders.

Communicate through appropriate methods
It would be more effective if the stakeholders are communicated through the methods they prefer. For example, some stakeholders prefer to receive information through emails while others prefer to attend a stakeholder meeting. If the organization does not have a general system to do so, it should at least provide relevant information on the company’s website on a regular basis.
Conclusion

GRC - Governance, Risk Management, and Compliance is an integrated approach for an organization to better achieve its business objectives. Internal auditing should identify and enhance the interconnections between these three elements because the fact the internal auditing evaluate all three elements and often have insights of each of the element.

Nowadays, internal auditing is more involved in the strategic work for an organization. The nature of internal audit function enables it to add more values to organizations, so the organization should give more reliance to the internal audit function in regard to GRC. For the future of internal auditing in GRC, internal auditors should gain knowledge and be more familiar with technology tools to help perform their work, establish and maintain good relationships with several different entities, and learn lessons from failures of GRC from internal issues and outside real-life cases.

Investments from stakeholders are crucial for the success for an organization, internal auditing should act as an advisor to stakeholders and communicate internal reports to stakeholders through the audit committee to gain more reliance and trust from them.

Ultimately, the integrated GRC should be one framework for everyone within the entire organization to follow to reduce miscommunications and duplications of work and increase overall operation effectiveness.
List of Figures

Figure 1 - Internal audit assisting activities in governance ................................................................. 2
Figure 2 - Internal auditing’s role in ERM ............................................................................................... 3
Figure 3 - The Three Lines of Defense model ........................................................................................ 4
References


3 Ibid., Page 1.

4 Tabuena, op. cit., Page 2.


7 The Open Compliance and Ethics Group, op. cit., Page 3.


Figure 1 – Internal audit assisting activities in governance

- A review of the organization’s control culture, especially the "tone at the top"
- An objective evaluation of the existing risk and internal control framework
- A source of information on major frauds and irregularities
- Reviews of the compliance framework and specific compliance issues
- Feedback on adherence to the organization’s values and code of conduct/code of ethics

(Graphic created based on information obtained from Florea)
Figure 2 – Internal auditing’s role in ERM
Figure 3 - The Three Lines of Defense model