Modern Risk-Based Internal Auditing

Norman Marks explains how a modern approach can improve internal audit performance
You’re successful, respected, and committed. What does it take to get to the next level?

The QIAL identifies, assesses, and develops core skills linked to audit leadership success. It caters to CIAs and CAEs who are already strong performers and have the potential for greater leadership.

Registration is now open. Start your leadership journey TODAY at globaliia.org/QIAL.

www.globaliia.org/QIAL
Dear Readers,

Globally, the IIA held its 2015 Global Council in Beijing, China in April 2015. A few interesting statistics from the Global Council include: a) There are now over 5,000 members of the IIA in the Middle East region which has experienced the largest growth over the past year in terms of membership. b) There are over 130,000 internal auditors with the Certified Internal Auditor (CIA) designation but less than 100 who hold the elite Qualification in Internal Audit Leadership (QIAL).

Further, the IIA will be holding its annual international conferences in Vancouver, Canada from 5 – 8 July 2015. During the conference, the IIA will unveil the new improvements that have been made to the International Professional Practices Framework. There, the IIA will also release the first of many research reports that have been produced as a result of the 2015 global internal audit survey (part of the Common Body of Knowledge – CBOK) which was completed by over 14,000 internal audit professionals around the world, including over 800 from the GCC region. The UAE-IAA plans on teaming up with other institutes in the region to produce original research to be released in 2016.

In addition, we celebrated the International Internal Audit Awareness Month in May 2015. Colleagues from around the world worked to build awareness in their workplace and local community and shared the motto “Proud to be an Internal Auditor”. In the UAE, we conducted joint events with Emirates Transport, the Dubai Directorate of Residency and Foreigners Affairs, the Sharjah Chamber of Commerce and for the first time ever, we conducted a joint training session with ISACA, the Institute of Chartered Accountants of India and the Association of Certified Fraud Examiners.

On a final note, in this issue we are delighted and honored to have an insightful cover story from Norman Marks, a world renowned author and thought leader in the internal auditing profession. You can learn more about Norman by visiting https://iaonline.theiia.org/blogs/marks

Our strategic partners and volunteers will continue to support our magazine and ensure that we maintain its quality. We extend our appreciation and gratitude to them. If you wish to write an article for the magazine or provide any feedback, please feel free to email editor@internalauditor.me

We hope you all enjoy reading this issue and we wish you a pleasant summer ahead.

Sincerely,

Abdulqader Obaid Ali
President
To achieve new heights, finding the right balance of audit tools is essential. Only TeamMate offers an integrated set of solutions that include the industry’s leading audit management system, an innovative controls management system and powerful data analytics.

TeamMate AM | TeamMate CM | TeamMate Analytics

Learn more at: TeamMateSolutions.com
FEATURES

16 COVER STORY: Modern Risk-Based Internal Auditing  The “audit universe” is a thing of the past. Internal auditors need to focus on the risks that matter in order to be more effective.
BY NORMAN MARKS

20 Managing the Risks Facing the Internal Audit Department  Internal Audit departments also need to manage their own risks.
BY CHRISTIAN THUROW

22 The Increasing Relevance of Continuous Auditing  Internal auditors need to change their approach to keep up with a fast-paced business environment.
BY PORUS PAVRI

26 Auditing Ethics  It is not easy and internal audit standards require it.
BY ALSHAREEF MARWAN ALKHOULI

DEPARTMENTS

4 Reader Feedback

5 Knowledge Update  PwC’s Risk Survey; Internal Audit Capabilities; Pulse of Internal Audit; Financial Crime; Governance, Risk & Compliance.
BY VISHAL THAKKAR

8 UAE-IAA Events

10 Risk Management  The true value of risk management can only be realized through an integrated approach.
BY EHAB SAIF

12 Conversations with Colleagues  Salem Sultan Al Dhaheri advises internal auditors on how to meet the expectations of the audit committee.
BY FARAH ARAJ

28 Governance Perspectives  Family businesses have specific governance systems which need to be in place to ensure their continuity.
BY ARIF ZAMAN

31 Fostering Fundamentals  How to effectively control retail store risks.
BY MOHAMMED KHALIL AL JALLAD
Marketing Internal Audit

I really enjoyed reading Ala’ Abu Naba’a’s article titled “Marketing Internal Audit Services” (March 2015). Indeed as internal auditors we need marketing skills in order to convince our stakeholders of our added value to the organization. I have read a lot of articles about the communication gap between internal auditors and various groups of stakeholders such as the audit committee and executive management.

Marketing internal audit is a very good way to close this gap.

In addition to what was included in the article, I think improving our writing skills and shortening our audit reports are also good marketing tools. The quality of our audit reports does not depend on the length of the report, it depend on the value we create for the report’s readers.

I strongly suggest that your respected magazine concentrate more on providing articles on how to close the communication gap between internal auditors and their stakeholders. There is plenty of good advice that can be shared with internal auditors in our region.

Sent anonymously by a Chief Audit Executive in Kuwait.

Positive About the COSO Framework

The article “COSO’s Internal Control – Integrated Framework” (March 2015) is a very good and informative article for all internal auditors and businesses. It clearly highlights the importance of the COSO Framework where in 100% of US stock exchange listed companies subject to Section 404 have chosen COSO as their internal control framework. The article is very well written and provides a good starting point for companies who want to start adopting the framework and provides good references. Further it highlights that the top tier companies in GCC have already implemented COSO Framework which gives the starting point to other companies to learn and implement the COSO Framework in their respective organization to add value and ensure compliance to best practices.

It would have helped if there was also a paragraph on lessons learnt in first time implementation or time/ cost involved. Moreover, I recommend to include a second article on COSO framework where it should highlight the benefits achieved by companies after the implementation of COSO Framework, real time examples would be great.

Ahmed Godil
Internal Audit Manager
Abu Dhabi, UAE
STREAMLINE YOUR INTERNAL AUDIT PROCESSES FOR MORE EFFICIENCY

ACCELUS AUDIT MANAGER

Internal audit is being asked to evolve beyond the “third line of defense” or ticking regulatory boxes. Boards and senior management now value the insight and analysis that a strong audit function can deliver.

Accelus Audit Manager can help:

- Liberate audit teams from manual tasks
- Enrich your dialogue with the business
- Drive enhancement of audit quality
- Deepen engagement with your board audit committee
- Contribute to business operational excellence
- Improve identification of emerging risks

For more information on Accelus Audit Manager please visit: http://accelus.thomsonreuters.com

CONNECT | SIMPLIFY | PERFORM
PwC’s 2015 ‘Risk in Review’ Survey

An analysis of PwC’s Risk in Review survey, which was carried out during this year, shows that an approach of having proactive risk management prevents costly misjudgments, drives efficiency and generates higher profit margin growth. However, the significant majority of companies have not developed the processes and structures that can bring these benefits into effect. A proactive, risk-enabled approach is specifically important as technology is rapidly evolving. The quick and incremental growth of digital platforms has opened an unknown world of sophisticated cybercrime and privacy threats. This has caused established industries to encounter technology risks with which they are not very familiar with when developing new products, operating in new markets or regulatory jurisdictions. Even, new regulations are compelling new compliance needs and there is a growth in third party risks as companies engage in innovative but relatively less-established outsourcing vendors, contractors and sub-contractors. Accordingly, without a risk-enabled approach to growth, companies are not geared to take full advantage of the impending growth climate without exposing themselves to significant threats.

Over the past three years, 55% of risk management leaders recorded increased profit margins compared with only 43% of non-leaders. Further, 41% of leaders achieved an annual profit margin of more than 10% whilst only 31% of non-leaders achieved such margins.

Where risk leaders get it right – The following are 4 leading practices that distinguish the best of the best:

1. Risk leaders understand that risks are interconnected
2. Risk leaders align risk management to the business
3. Risk leaders strive to be proactive, not reactive - they bring the right tools to the job
4. Risk leaders know their risk appetite and are willing to take chances


2015 Internal Audit Capabilities and Needs Survey by Protiviti

All organizations, however big or small, and operating in different industries, are experiencing an alarming number of cybersecurity issues. IT departments have major responsibilities in addressing these areas. Internal auditors also play a key role in securing the organization by closely interacting with executive management and functional leaders to ensure that cybersecurity is incorporated in the flow of business operations and processes.

Based on the findings of this year’s ‘2015 Internal Audit Capabilities and Needs Survey’, as expected, cybersecurity represents a major focus for internal audit programs, but it is not the only pressing issue on internal audit’s agenda. Following are the important matters that came out from the survey:

- Engagement of the board and the audit plan represent keys to effective cybersecurity
- Priority list of internal audit continues to grow
- Rise in technology-enabled auditing
- Internal audit is focusing more on marketing and collaboration


Risk Management & Internal Audit in the UAE

77% of companies have a comprehensive risk management program or certain processes in place

25% of companies conduct a quarterly risk assessment

Source: Risk Management Practices and the Role of Internal Audit
Navigating an Increasingly Volatile Risk Environment – Pulse of Internal Audit Survey

According to The Institute of Internal Auditors’ North American Pulse of Internal Audit 2015 survey, internal auditors generally are aware of many of the challenges, however, following areas needs closer attention:

- Nearly 7 in 10 respondents of the survey (which was conducted in October 2014) viewed cyber attacks and other security threats as a high or critical priority. However, respondents as a whole did not express major concern about significant geopolitical developments, global health threats or the impact of social media. This could be due to failure to see how such factors could impact organizations.

- More than half of the Chief Audit Executives (CAEs) and directors that responded to the survey consider emerging risks identification as their biggest challenge. In spite of this, only about one-third expressed a greater degree of confidence in their ability to identify emerging risks.

- 4 in 10 respondents put a high priority on attracting and retaining talent and 54% of respondents referred to competition for a limited pool of skilled auditors as a reason for skill gaps on their audit teams.

- 45% of the respondents consider the sustainability of the organization and its business partners, supply chain, revenue change and product development to be a high (36%) or critical (9%) priority. These indicate that they care strongly about these issues.

https://na.theiia.org/services/Pages/Pulse-of-the-Profession-Study.aspx

2015 Governance, Risk & Compliance Survey by Grant Thornton

Chief Audit Executives (CAEs) and Audit Committee members were surveyed to know the priorities of both these groups. The survey pointed to clear indications of a disconnect between these two groups of respondents. The responses suggest that priorities of internal audit are different for CAEs and audit committee members. When asked to rank their focus on four types of risks, audit committee members cited their priorities as: financial, compliance, operational and strategic risks and CAE’s ranked their risk focus as: compliance, operational, financial and strategic risks.

Upon inquiring about the top three areas where they want internal audit to deliver value, audit committee members ranked “mitigating risk” first, followed by “stronger financial controls compliance” and “identifying improvement opportunities as against CAEs ranked “identifying improvement opportunities” first, “mitigating risk” in the second position and “increased efficiency” in third position.


Financial Crime in the Middle East and North Africa Region

Thompson Reuters’ 2015 survey of financial crime programs in the MENA region is the first of its kind and can be used by regulated firms to help with benchmarking, planning and resourcing such programs in the future.

Based on the analysis of the results, following themes were noted:

- Compliance departments are juggling competing priorities

Survey results show that compliance officers in the region are experiencing a certain amount of pressure. This was due to the tide of regulatory change is not expected to turn in the medium term which combined with constraints over budgetary and resources, the ongoing pressure to balance business objectives with regulatory requirements.

The UAE-IAA held its 16th Annual Regional Audit Conference on 9 and 10 March 2015 at the Abu Dhabi National Exhibition Center (ADNEC). The 2 day conference was preceded by workshops held on 8 March 2015. The theme of the conference was “Innovate Your Future Now”

The conference had more than 50 international and regional speakers including the keynote speaker H.E. Mohamed Alabbar, Chairman of Emaar Properties, who inaugurated the conference and shared with Abdulqader Obaid Ali, President of the UAE-IAA, in presenting tokens of appreciation to the strategic partners and sponsors.

The conference was attended by over 600 internal audit professionals from the UAE and the region. The conference also featured 8 concurrent tracks, out of which 2 tracks were in Arabic.

Further and as is the tradition each year, the UAE-IAA selects 2 professionals (one from the UAE and one from outside the UAE) to be presented with the “Life-Time Achievement Award” as recognition for their contribution and added value to the internal auditing profession. This year the awards were given to following:

- **From the UAE:** Mr. Salem Sultan Al Dhaheri, Deputy Director of Internal Audit at the Abu Dhabi Investment Authority.
- **From outside the UAE:** Dr. Khalid Al-Faddagh, Executive Director – Internal Auditing, at Saudi Aramco.

Keeping up with the concept of having smart conferences, this year a new technology called Poken, which is an Near Field Communication (NFC) device, was used by the attendees to gather presentations, contacts and materials all on a USB stick by using touch interaction with other devices.
Joint Hospitality & Fraud Subgroup Event

The UAE Internal Audit Association Hospitality & Fraud subgroups collaborated to hold their first meeting for the year 2015 at the Novotel Al Barsha, in Dubai on 17 March 2015. The event was hosted by Aldrin Sequeira, Chief Internal Audit Officer for the Jumeirah Group & Chairman of the Hospitality Subgroup.

The event was attended by various internal audit professionals and had 3 keynote presentations:

- The session began by a presentation from Hisham Slim, Chief Audit Executive at Abdul Latif Jamal Company LTD, where he talked about the “IIA Standards Related to Fraud”.
- The second session was conducted by Nabil Al Ouf, who is Head of Internal Audit at Dragon Oil, who presented on the topic of “Fraud Risk Assessments”.
- The third and final presentation was from Kamal Bhatia, the Managing Director at Wide Computers Systems, who gave an interesting presentation on “Data Integrity and Mystery Shopping”.

Event participants were awarded 2 Continuing Professional Education credits.

Joint Event with the Securities and Commodities Authority

Both government and private institutions have come to realize the vital importance of internal auditing and internal control in the fight against corruption.

Being aware of this and realising the need to support the internal audit profession with an appropriate governance & legal framework, the UAE Internal Audit Association along with the UAE Securities and Commodities Authority (SCA) held a joint event in the Dubai offices of the SCA on 27 April 2015. The event aimed at increasing cooperation between the two institutions and at promoting the development of specialized standards in the field of internal audit to elevate the profession.

The event was opened by H.E. Mohammed Khalifa Al-Hadhari, Deputy CEO of SCA, who spoke about the importance of the internal audit and the importance of holding such seminars in creating awareness of internal audit. This was followed by an introduction by with Abdulqader Obaid Ali, President of the UAE-IAA, who gave an overview of the UAE-IAA and the services that it provides. In particular he emphasised the translation to Arabic of many important pieces of internal audit related guidance such as the “Certified Internal Auditor” exam and materials, the “Sawyer Guide for Internal Audit” and the COSO Internal Control Framework. Mr. Abdulqader then emphasised the importance of internal audit in various institutions and the support of His Highness Sheikh Mohammed bin Rashid who issued a Federal Internal Audit Charter to require to establish internal audit departments in the federal government.

Then Mr. Nagesh Suryanarayana, Internal Audit and Risk Advisory Director at Protiviti Middle East gave a lecture on the “Effectiveness of Audit Committees”. This was followed by a presentation by Mr. Peter Chambers, Lead Partner of BDO in Abu Dhabi, on “Rules of Ethics on Governance”.

The event was attended by various internal audit professionals and had 3 keynote presentations:

- The session began by a presentation from Hisham Slim, Chief Audit Executive at Abdul Latif Jamal Company LTD, where he talked about the “IIA Standards Related to Fraud”.
- The second session was conducted by Nabil Al Ouf, who is Head of Internal Audit at Dragon Oil, who presented on the topic of “Fraud Risk Assessments”.
- The third and final presentation was from Kamal Bhatia, the Managing Director at Wide Computers Systems, who gave an interesting presentation on “Data Integrity and Mystery Shopping”.

Event participants were awarded 2 Continuing Professional Education credits.
Increasing the Perceived Value of Risk Management

The integration of enterprise risk management and operational risk management roles is bound to lead to more effective risk management.

Based on my experience in the Middle East region, the ERM concept is relatively new and many business owners have difficulties in understanding the role of the ERM function. I recently noted a perceived gap between the “Head of Enterprise Risk Management (ERM)” and the “Operational Risk Manager” roles. In many cases, this leads to a performance expectation gap. In my view, these roles should be integrated to ensure a smooth implementation of ERM.

As part of the implementation of a comprehensive ERM program, a considerable amount of time is required to develop an ERM framework, spread risk awareness, execute entity-wide risk assessments and embed Risk Management in each business unit. This lengthy timeframe can lead to a less responsive and inflexible Risk Management model, given the dynamic nature of businesses and frequent changes in business risks. Bringing a focus onto operational risk management helps achieve quick wins and keeps the risk profile under management attention.

Resilient Risk Management Function

In order to have an effective and resilient Risk Management model, the Risk Management function should work as an operational risk advisor to management by dynamically reviewing business decisions, investments, processes and other risk exposures. In parallel and simultaneously the Risk Management function should also implement a robust ERM program that ensures high level Risk Management assurance and the creation of a risk-aware culture.

While some organizations recruit industry-specialized technical risk managers for operational levels and/or Enterprise Risk Managers to implement the ERM framework, very few organizations have a Risk Management department that combines both the strategic and operational levels of risk management.

Internal Audit vs. ERM

In most cases, an ERM function focuses only on risk identification and prioritization, without being an integral part of the decision making process and actively advising management on dynamic and emerging risks. This can result in Risk Management being perceived and classified by senior management as part of the internal audit function; which can create unnecessary barriers, decreasing the added value of having a Risk Management function.

Independence

Based on my experience, the majority of ERM functions in the Middle East (excluding the financial sector) are still working under the umbrella of internal audit departments, reporting directly to a Chief Audit Executive (CAE) and up through to the Audit Committee. This is also the case in the UAE whereby a recent study has shown that in 35% of the cases, the Chief Audit Executive took the lead role for ERM compared to 25% for the Chief Risk Officer. This model dilutes the effectiveness of the Risk Management activities and increases the limits on Risk Management involvement in decision making process.

In order to achieve its initial objectives, the Risk Management department could report directly to the CEO and/or Risk / Audit Committee; being independent from the Internal Audit Department. This may result in greater cooperation with management and a common perception of the Risk Management function as a trusted business advisor. For example, if Risk Managers are responsible for identifying contractual risks after an organization had signed a contract; who is responsible for proactively advising management on contractual risks prior to entering into any liability with third parties? Moreover, having a combined Internal Audit and Risk Management function will impair the assurance role of Internal Audit over the adopted Risk
Management framework.

Independence from Internal Audit will further allow the Risk Management function to explore areas that are not commonly considered, such as the dilemma of “who audits the auditors” and risks associated with Internal Audit as a function, such as:

- The sufficiency of resources to ensure audit coverage of high risk areas and ensuring maximum value from auditing activities;
- The competency of subject matter experts whom add value through audit recommendations; and
- The management of outsourced internal audit service providers from a quality and value-adding perspective.

The diagram below illustrates the optimal Risk Management Governance Model in any organization:

**Risk Management Standards**

International Risk Management Standards (e.g. ISO 31000:2009, COSO ERM Framework) focus on having a function which is responsible for the establishment of a robust Risk Management framework that facilitates and coordinates the risk assessment and ensures the promotion of risk awareness within the organization.

Although Risk Management standards emphasize the importance of frequent communication and consultation with stakeholders throughout the implementation of the ERM program, they do not provide sufficient attention to the dynamic role of the Risk Manager as an operational risk advisor whom adds value to the company through his or her industry knowledge.

**The Way Forward**

The structure and mandate of the Risk Management function is still under global debate with no clear consensus. On one hand, it is important to emphasize the differentiation between Risk Management and Internal Audit; however, on the other hand, it is also important to focus on merging operational risk and ERM responsibilities under the same umbrella.

Although we should emphasize that Risk Management cannot guarantee mistakes will not happen, I do not agree with the idea that Risk Management should be prevented from making decisions for the organization. The reason for this is due to the fact that it is difficult to justify the existence of another “all cares no responsibility” function that has similar roles to the internal audit department in the perception of senior management. If both Internal Audit and Risk Management are seen as an independent assurance functions, then it is justifiable for business owners to merge both functions under one department, in an effort to cut costs.

My alternative recommended model for a Risk Management function is to evolve and justify its existence through having direct involvement in operations and focusing on its risk advisory role by having subject matter knowledge, which has true value to the organization, in addition to its role as a coordinator and facilitator of a comprehensive ERM program.

**Characteristics of Risk Managers**

Finding a suitable candidate to lead a Risk Management function that has operational risk and ERM responsibilities is not a simple task. In order to gain Senior Management confidence and to be perceived as a trusted business advisor, an effective Risk Manager should possess deep industry-specific experience, in addition to having ERM program implementation experience, coupled with outstanding communication, presentation and interviewing skills.

The Risk Manager should also accept part of the responsibility over his business advisory role, which at the same time, should be part of his key performance indicators.

**References:**


**Ehab R. Saif, CMA, CIA, CFE** is an Internal Audit Manager at a private holding company in Abu Dhabi.
In an exclusive interview, Internal Auditor - Middle East spoke to Salem Sultan Al Dhaheri, CPA, who is the Deputy Director of Internal Audit at the Abu Dhabi Investment Authority (ADIA). Salem has 21 years of experience in auditing investments, leading internal audit departments and serving as a board member for several public and private companies.
How do audit committees ensure that internal audit is responding to the “risks that matter”?
This is done through a review of the risks identified in the risk assessment for internal audit planning. Internal audit’s role is to ensure that priority is directed to high-risk areas. Further, Audit Committee members should also, when required, dive into the details of the residual risks identified and ensure that there is a plan to address risks which fall outside the company’s risk appetite. This can only be done if the risk assessment carried out by the internal audit department is thorough and leads to the identification of the top 10 risks facing the company. Also, internal audit will need to periodically interview management to identify changes in the company’s risk profile and emerging risks. Only then can the audit committee determine whether internal audit is focusing on the right risks. The traditional risk assessment which involves the annual ranking the audit universe is not sufficient. CAEs need to transform and move away from their comfort zone.

What kinds of reports/communication do you expect from the CAE?
The internal audit report is, in reality, the only deliverable from the internal audit department and therefore it should be a high quality deliverable. If there is one thing that I like, it is to see how the company changes as a result of internal audit reports. A good audit report is one which is accepted by management and creates positive change in the company. Further, I appreciate seeing a big picture analysis of an entity or process. This would show the overall progress and performance including positive observations. The audit committee should not get into the details of each observation unless it is very significant. It is management’s responsibility to address the individual observations raised in the internal audit report. The audit committee will assess the quality of the recommendations and see what action management is taking to mitigate those risks.

I am aware of situations where CAE has copied the audit committee on all reports issued to management! The committee should be copied only if there is a major problem; even then the whole report is too much. Quality and conciseness of the IA reports is more important than quantity.

In terms of quarterly presentations to the audit committee, the same principles mentioned above should apply. We need to see the consolidated view of findings: how many overdue action items are there, how many observations have been raised/closed, what is high/medium/low priority, what activities are internal audit carrying out etc.

A recent survey by the UAE-IAA, emphasised the need for internal audit to take the lead in risk management where such a process/function does not exist. What are your thoughts on this?
I support this. Internal audit is best placed to facilitate the establishment of a risk management process (with appropriate safeguards). A good internal audit team has knowledge of both the organization and its risks. This is one way for internal audit to move towards being a trusted advisor. However, at a later stage, when the risk management process matures, and if the organization has grown sufficiently,
Interview

What are your thoughts on internal audit quality assurance reviews or reviews by regulators?

Compliance with the IIA’s Standards and carrying out a quality assurance review by an external assessor are fundamental to assuring the audit committee of the quality of the internal audit department. However, a checklist approach against a set of standards is not enough. The assessor should meet with a variety of stakeholders and determine whether the internal audit department is adding value and meeting expectations. It is also important to see the internal audit department’s processes mapped against a maturity framework to allow the audit committee to better understand the current state of the internal audit department.

Have audit committees in the UAE been pushing for the concept of the 3 lines of defense and combined assurance?

Not many are giving attention to this concept. This is an area which we should be focusing on where multiple assurance providers exist and where there is sufficient maturity in risk management processes. The Audit Committee should make sure that each assurance function is playing its part and that there is no overlap in assurance or missing assurance. Helping build such a framework is a very good way for internal audit to add value to the business.

Are CAE’s keeping audit committees up-to-date with developments in the internal audit profession?

(Laughs) I rarely get any professional or industry updates from CAEs! I usually get it from outsourced service providers. When the audit committee is informed and given executive education, it will be in a better position to understand the issues and risks raised by internal audit. I think the CAE should make an effort to summarize new reports or research from the IIA or other sources at the quarterly audit committee meeting. He can take 5-10 minutes to deliver an overview. Also, if planned properly the CAE can deliver a training session on a particular topic to ensure that the audit committee is kept up to date. To do this the CAE must participate in professional associations such as the IIA and regularly attend workshops and conferences.

Any final advice to Chief Audit Executives?

As mentioned earlier, the CAE needs to work to become a trusted advisor. Internal audit by design is an assurance provider. It is when internal audit goes beyond this traditional role that it is able to add value to the business. Internal audit needs to build knowledge & skills and understand the business in order to be a trusted advisor. This includes getting specialized certifications (E.g. CFA if you work in investments), having staff members work in the business, building skills such as IT, cybersecurity, data analytics, forensics, Six Sigma, industry specific skills etc. Leading CAEs have implement a talent acquisition plan (using internal or external resources) to meet stakeholder expectations. The CAE needs to get to a point where stakeholders are asking him for additional help. Only then will the CAE know that the internal audit department is doing a good job.

internal audit will need to hand over the role to a dedicated risk function; a second line of defense. Internal audit will then elevate itself to auditing the risk management process.

What are your thoughts on internal audit quality assurance reviews or reviews by regulators?

Compliance with the IIA’s Standards and carrying out a quality assurance review by an external assessor are fundamental to assuring the audit committee of the quality of the internal audit department. However, a checklist approach against a set of standards is not enough. The assessor should meet with a variety of stakeholders and determine whether the internal audit department is adding value and meeting expectations. It is also important to see the internal audit department’s processes mapped against a maturity framework to allow the audit committee to better understand the current state of the internal audit department.

Internal Auditors - Middle East
RAISE THE RED FLAG
An Internal Auditor’s Guide to Detect and Prevent Fraud
Lynn Fountain, CGMA, CRMA

Help Your Organization Identify the Risk of Fraud Before It’s Too Late!

Get your copy today!
Visit www.theiia.org/bookstore
Item No. : 1191
Norman Marks, one of the most highly regarded thought leaders in the global profession of internal auditing, explains how companies in the Middle East can add more value to their stakeholders by applying a modern risk-based approach to internal audit planning.

I remember talking to an internal audit leader for whom I have great regard. I was stunned to hear him say that you do two risk assessments: one when you develop the audit plan to identify the processes, locations, and business units to audit, and a second when you start each audit so you can identify the risks to assess in each area. That is the way I learned to build the audit plan more than 20 years ago!

I had a few discussions with some internal audit colleagues at an event last year and I learned that some companies in the Middle East develop their internal audit plans in the same way. I moved away from this process in the early 1990’s because I didn’t believe it was helping me address the areas of significance to the board, top management, and the company. If internal audit is to be “relevant” (a term increasingly being used to question whether internal audit is delivering what the organization needs most), it is important to ensure that the engagements it will perform focus on the risks that matter to the organization today.

What does “risk-based” mean?
The concept of risk-based planning comes from The International Standards for the Professional Practice of Internal Auditing (Standards) issued by the Institute of Internal
Instead of starting with an assessment of the audit universe, I start with understanding the risks to the enterprise as a whole. The more significant risks might include: our implementation of a new enterprise resource planning (ERP) system; the start up of a new factory in Jordan; the expansion of the business into Iraq; compliance with health & safety regulations; reliance on single source vendors for critical components; and the timeliness and accuracy of monthly management reporting to the executive committee.

My goal is to provide assurance on how well management’s processes are able to manage the more significant risks. My audit plan includes projects to identify and assess the controls that management is relying upon to manage the ERP implementation, to comply with health & safety rules, sourcing of critical components, and to ensure the integrity of monthly management reports.

For example, one might rate the following as higher risk areas: The factories in Saudi Arabia and Qatar; the Corporate Shared Services Center in Dubai; and, the general controls over the IT Data Center in Oman. The scope of the Saudi Arabia audit would be based on a risk assessment of the factory’s processes, assets, etc. The audit might include the higher risk areas of inventory management, quality control, and code of conduct training. The scope of the Qatar factory audit would be different, as the risks in that location are not the same: payroll, procurement, and accounting for inventory. A similar local risk assessment would be performed for the other audits.

While this approach was “risk”-based, it was not talking about risks to the objectives of the organization as a whole. “Risk” was about the potential for any deficiencies in internal control to have an impact (in monetary terms) of some size to one location. The difference may be subtle, but it is important. I want to focus my audits on ensuring the organization has the ability to achieve or surpass its objectives.

Modern Risk-Based Audit Planning

My approach today — my definition of modern risk-based auditing — is different.

Auditors (IIA). They require the chief audit executive to “establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals” (Standard 2010). This concept has also been included in governance-related thought leadership. Principle 7.2 of The King Report on Corporate Governance for South Africa states that “Internal audit should pursue a risk-based approach to planning as opposed to a compliance approach that is limited to evaluation of adherence to procedures”.

While IIA Standards and other guidance, from internal audit thought leaders and the consulting firms, advocate a “risk-based” approach to internal auditing, they generally don’t provide a great deal of guidance on what that means and how to accomplish it. However, there is one thing in common with all the guidance and approaches; they all need to begin with an assessment of risk.

Traditional Risk-Based Audit Planning

This approach was all about building a “risk”-ranked audit universe. The first step was to identify all the potential areas for audit, including business processes, locations, data centers, etc. A frequent question among auditors was “how large is your audit universe?” You then considered various factors such as:

- Revenue generated or accounted for at that location, by that process.
- Asset size.
- Time since last audit.
- The significance of any findings in the prior audit.
- The level of change in systems, process, and personnel.
- Management and board input on risk.

The audit plan included engagements at these locations or of these processes.

So instead of using risk assessment to determine which “audit universe” elements I will include in the audit plan, I moved to an approach where I identified the top risks to the achievement of the company’s objectives (a “risk universe”), and then identified the engagements I could perform to identify and assess the controls that management is relying upon to manage the ERP implementation, to comply with health & safety rules, sourcing of critical components, and to ensure the integrity of monthly management reports.

The concept of “audit universe” is outdated.

Traditional

<table>
<thead>
<tr>
<th>Location/Process 1</th>
<th>Location/Process 2</th>
<th>Location/Process 3</th>
<th>Location/Process 4</th>
<th>Location/Process 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact on Audit</td>
<td>Selected for Audit</td>
<td>Execution of Audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1st Risk Assessment</td>
<td>2nd Risk Assessment &amp; Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1st Risk Assessment</td>
<td>2nd Risk Assessment &amp; Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1st Risk Assessment</td>
<td>2nd Risk Assessment &amp; Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1st Risk Assessment</td>
<td>2nd Risk Assessment &amp; Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1st Risk Assessment</td>
<td>2nd Risk Assessment &amp; Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

The audit plan has to be designed to address the major risks to the enterprise. The traditional audit planning process must die a quick death (assessing risk levels based on an audit universe, and then performing audits of the controls designed to address risks to the achievement of objectives for those areas, locations, business units, etc.) A modern risk-based approach will take its stead. Here the more significant risks to the enterprise are identified and targeted in audit engagements. Rather than focus on risks to objectives at a process, department, or location, audits will focus on risks to the objectives of the organization.

Building the audit plan based on an audit universe instead of the top risks to the organization is likely to result in auditing risks that are not significant. Chief Audit Executives need to have the confidence to build a risk-based audit plan that is agile and designed to address the risks that matter to the organization. When internal auditors provide assurance and insight on the risks that matter, their work matters to the board and top management. Instead of finding problems and being perceived as an overhead activity that adds to management’s task list, they are helping the board and management deliver value to stakeholders.

References


NORMAN MARKS, CPA, CRMA was a chief audit executive and chief risk officer at major global corporations for 20 years.
Building relationships, creating value.

Whenever there is business to be done, you will find PwC providing insight, perspective and solution to many of the world’s most successful companies.

Through our global network of firms we can bring the power of more than 195,000 professionals in 157 countries. We believe that the best outcomes are achieved through close collaboration with our clients and the many stakeholder communities we serve.

Our people will listen to you and tailor solutions that will help you meet the challenges and opportunities of doing business and beyond.

For more formation on how we can help you address your business needs, please visit our website: www.pwc.com/me

© 2015 PwC. All right reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.
Most articles written about internal audit and risk management focus on internal audit’s role in ensuring the effective management of risk within the first and second lines of defense. Little attention is given to managing risk within the third line itself.

People Risk

Ask any Chief Audit Executive (CAE) for the Risk Register of his Internal Audit function and there is a fair chance he or she will show you the risks relating to the audit universe. That’s all good except for the fact that Internal Audit is not part of that universe. Management is expected to define a set of controls to ensure that the business operates as planned. Regular Control Self Assessments or similar techniques are implemented to monitor the ongoing effectiveness of these controls. In a nutshell, that’s what Internal Audit expects to see when auditing a business unit. But does Internal Audit live up to the same standards? Practice Advisory 2120-2: Managing the Risk of the Internal Audit Activity states that “the internal audit activity is not immune to risks. It needs to take the necessary steps to ensure that it is managing its own risks”. So where is the Risk Register for the Internal Audit Department, including gross risk assessments, controls and residual risks? Where are the regular Control Self Assessments for the Internal Audit department? Is there an established Risk Management process within the Internal Audit function? Typically such a process, like any risk management process, should include the following stages:

- **Risk Identification:** What are the risks Internal Audit is facing?
- **Risk Assessment:** How severe are those risks? Often assessed by applying an impact / likelihood matrix.
- **Risk Mitigation:** Accept, mitigate or transfer of risks depending on their severity.
- **Risk Monitoring:** Look out for new risks, changes to the risk assessment for existing risks and effectiveness of mitigation actions put in place.

Take the example of People Risk, a subset of Operational Risk. When asked about People Risk, CAEs might think of staffing, lack of skills etc. All those risks that might impact the timely execution of the audit plan. But that is only one side of People Risk. The other side is the risk the Internal Audit staff is facing or causing while performing their job. The following scenarios, most based on incidents that appeared in the news, help to raise the awareness for that type of People Risk.

**Medical Assistance**

An Internal Auditor is sent from the United States to audit a subsidiary in rural China. On the evening of his arrival, his appendix ruptures and he needs urgent medical treatment. Think of:

- Who will bring the auditor to the hospital and help with translation?
- Who will inform the company?
- Who will secure the personal belongings and the company assets (Laptop, Smartphone) from the hotel room?
- Who will authorize any payments if the hospital wants to see cash?
The Standards advise chief audit executives to address risks related to internal audit department and its objectives and specify 3 categories of risks:

1. Audit Failure: This refers to the inability or “failure” of the internal audit department to identify or make recommendations to prevent control failures. The question asked is usually “Where were the internal auditors?”. Reasons for Audit Failure include poor risk assessments, improperly designed audit procedures, auditors who are not skilled in the area they are auditing, etc.

2. False Assurance: This occurs when the management believes that the internal auditors is covering a particular area or risk when in fact it is not. It is important to make sure that the risks being audited are clear and that internal audit’s involvement in projects is clearly defined.

3. Reputation Risk: While chief audit executives worry about having a reputation of being a policeman, there can be far worse labels which result from various control failures in the organization, the quality of internal audit staff, the attitude of auditors, etc.

Local laws and regulation
An Internal Auditor is sent from the Europe to audit a subsidiary in Singapore. While waiting for a taxi he spits out his chewing gum and is fined SGD 1000 (USD 800) by a nearby Police Officer. Think of:

• Do Internal Auditors travelling abroad receive briefings on local laws and regulations?
• Is there an agreement about who has to carry the costs for fines for misconduct that is not a criminal act in one’s home country?

Emergency procedures
A UK Internal Auditor is conducting an audit at an oil drilling site in Russia. While he is there, a fire breaks out. All emergency signs are in Cyrillic. Think of:

• Do Internal Auditors receive a briefing on local emergency procedures while working in a different location?
• Is there a general procedure how Internal Auditors should react in case of a disaster?

Threats
An audit team is investigating a suspicion of fraud at a branch. After returning from lunch they find a letter in their room telling them to leave immediately or they will be killed. Think of:

• Who needs to be informed within the company?
• Should the police be informed?
• Should the audit team be evacuated or stay on site and finish their investigation?

Fraud
An Internal Auditor who is travelling a lot is fiddling with his expense claims. Think of:

• Internal Auditors are in a position of trust. Are there ways how they could abuse this? Are there controls in place?
• Does Internal Audit receive the same level of scrutiny like other members of the workforce when submitting claims etc.?

The internal audit department faces more than just People Risk. The CAE needs to document and identify these risks and how to respond to them. Also, depending on the size of the department & complexity of operations, he could:

1) provide a gross risk assessment, map existing controls to the identified risks and analyze root causes, and 2) put controls in place to bring risks within the stated Risk Appetite, and 3) Implement ongoing Control Self Assessments to ensure control effectiveness.

Conclusion
Evaluating the effectiveness of risk management and first line of defense is an important part of Internal Audit’s work. But it is equally important that Internal Audit apply the same standards of Risk Management that it expects to see during an audit to itself. Every CAE should have a departmental Risk Register for the Internal Audit function that shows all risks Internal Audit is facing and the steps required to manage these risks.

“The internal audit department is not free from risks”

Data Protection
A German Internal Auditor attends an IIA Conference in the US. He takes his business laptop with him. During his last audit assignment in Germany he audited the HR function of his company including the payroll process. A lot of the payroll information is stored on his laptop. By taking the laptop to the US he is physically taking this information out of the European Union. That might be a violation of European Data Protection law and can lead to Reputational Risk. Think of:

• What information is stored on Laptops or Smartphones?
• How is that information protected?
• Are there any restrictions for moving the information to other countries?

The internal audit department faces more than just People Risk. The CAE needs to document and identify these risks and how to respond to them. Also, depending on the size of the department & complexity of operations, he could:

1) provide a gross risk assessment, map existing controls to the identified risks and analyze root causes, and 2) put controls in place to bring risks within the stated Risk Appetite, and 3) Implement ongoing Control Self Assessments to ensure control effectiveness.

Conclusion
Evaluating the effectiveness of risk management and first line of defense is an important part of Internal Audit’s work. But it is equally important that Internal Audit apply the same standards of Risk Management that it expects to see during an audit to itself. Every CAE should have a departmental Risk Register for the Internal Audit function that shows all risks Internal Audit is facing and the steps required to manage these risks.

“The internal audit department is not free from risks”

References:
1. IIA Practice Advisory 2120-2: Managing the Risk of the Internal Audit Activity (April 2009)

CHRISTIAN THUROW, CFSA is a lead auditor at a major European bank based in the United Kingdom.

INTERNAL AUDITOR - MIDDLE EAST  21
For several years now, management experts have been emphasizing the need to strengthen Corporate Governance and enhance Corporate Performance through changes in culture, structures and processes. The foundations of both Corporate Performance and Corporate Governance are built on the following FOUR PILLARS:

- Measuring and Managing Information Integrity Risk
- Achieving Operational Efficiency
- Striving for Business Process Optimization
- Leveraging Business Intelligence for Strategic Decision Making

If it is true that organizations today, whether proactively or reactively, are looking to strengthen the four pillars supporting Corporate Performance and Corporate Governance, it means Internal Audit departments need to evolve in order to achieve their core mission. The Core mission of any Internal Audit department, large or small (as explained by the IIA) is - the provision of independent, objective assurance and consulting services that (a) add value (b) improve operations and (c) help the organization achieve its objectives, by bringing a systematic, disciplined approach to evaluating the adequacy and improving the effectiveness of its governance, risk management and control (GRC) processes.

Stated differently, the aim of IA is NOT to audit GRC processes for their own sake, but to audit them to help the organization achieve its objectives!
In order to achieve this core mission, it is obvious that an audit framework that is reactive, backward-looking, based substantially on labor-intensive, manual verification of a small, statistically correct, representative sample of records will not help internal audit departments much in adding value to the organizations of the (near?) future, nor help those organizations achieve their objectives. Instead, what Internal Audit departments need is a risk-based audit framework that, while forming part of an overall risk-based Internal Audit plan, provides a complete, consistent and continuous method, wherever possible, of providing assurance to the board of directors or equivalent.

According to Norman Marks, prolific thought leader and an authority on Internal Audit, in these days of rapidly changing risks, when businesses are moving faster and faster, IA needs to be able to “audit at the Speed of Business”!

Throughout the next decade, the value of the controls-focused approach that has dominated internal audit is expected to diminish. Internal audit will provide its customers - the board of directors and executive management - with ongoing assurance that those risks which impact the achievement of its objectives, are subject to appropriate and effective governance, risk management and control processes. This ongoing assurance will be enabled primarily through continuous risk and controls assurance, with a much reduced set of traditional audit projects and more reliance on continuous auditing methods.

Continuous Auditing or Continuous Assurance – let’s call it CA, is defined very simply by the IIA as “any method used by auditors to perform audit-related activities on a more continuous or continual basis”.

While there is a specific, detailed methodology for planning and executing CA, the objective of the remainder of this article is not to detail the methodology, but to explain the core concepts of CA, the key business benefits, and some key implementation perspectives.

**CA comprises the following two broad components:**

a) **Continuous Risk Assurance** (let’s call it CRA) – which provides ongoing assurance that the organization is addressing all its current and emerging key risks, including Fraud Risks, and their risk levels.

b) **Continuous Controls Assurance** (let’s call it CCA) - which provides ongoing assurance that all controls that respond to current and emerging key risks (“key controls”), including controls that respond to Fraud Risks, are suitably designed, established and operating as intended.

One of the key terms in these definitions is “ongoing” – which does not mean 24 x 7 x 365, but rather a more continual process for identifying and assessing key risks to the achievement of objectives, monitoring changes in their levels, a more frequent testing of key controls that respond to those risks, and just as importantly, more continual reporting of findings. Another key term is “current and emerging”: What is the use of monitoring risks that no longer impact the achievement of the enterprise’s objectives, but are listed in a legacy Risk Register? And, what is the use of testing controls that are listed in a legacy Controls matrix, but which do not address an existing or emerging risk to an enterprise objective?

A concept related to Continuous Risk and Controls Assurance is the review / monitoring of (i) data that acts as an indicator of the level of risk i.e. risk drivers, and (ii) transactions that have already been subjected to a control. Ongoing review or monitoring of data relating to key risk drivers is the means by which Internal Audit provides Continuous Risk Assurance. And ongoing review or monitoring of transactions that have been subjected to a key control(s), is an additional line of defense, which not only provides a more comprehensive level of Continuous Controls Assurance, but also significantly increases the probability that if any out of control processes or fraudulent transactions did slip through the “control net”, they will be detected on a timely basis.

Technology may or may not be used in Continuous Assurance – in fact it would be a mistake to think that Continuous Assurance can be provided only through the use of technology. For instance, monthly physical attendance by Internal Audit at a stock count to ensure that it is performed in accordance with predefined company policies and procedures, is an equally valid example of Continuous Assurance. Technology is a great enabler of Continuous Assurance, no doubt, and should be used as such – i.e. as a means to an end, and not as an end in itself, by purchasing, for instance, an off-the-shelf GRC software just because it seems the in-thing nowadays, or because a competitor bought it! So, follow the methodology, understand if and where IT (i.e. CA software) would add most value, check for availability of in-house solutions, and then go out into the market to check what IT solution, if any, best fits your enterprise’s specific IT environment and CA requirements.

**Let’s consider a couple of examples of CA….**

A global company sells its products to, among others, customers in a country currently experiencing turmoil owing to international sanctions and a plunging currency, thus exposing the company to reputational and credit risk. One of the
“drivers” of that risk will be the pipeline of sales orders to customers in that country. As that pipeline grows, so does the risk. Technology is used by the Internal Audit function to continuously review and monitor the level of sales orders by country and send an alert to the pre-defined recipients/decision makers if sales to that country exceed a predefined level.

Another example....In order to test the quality of authorization controls over Corporate Credit Card expenditures in a more efficient and effective manner, internal auditors develop a series of continuous, data analytic tests to identify corporate credit card policy violations, such as personal expenses (travel, jewelry, alcohol, clothes, home furniture, etc.), use by unauthorized cardholders, split purchases to avoid authorization limits, transactions involving prohibited merchants, etc. The above data analysis tests are turned over to the Corporate Credit card manager who runs them on a monthly basis, as a control over credit card usage. Internal Audit verifies on a monthly basis that the manager has run this control (i.e. these analytic tests).

The Business Case for CA is built around several benefits, the most important among them being:

i) More effective and efficient risk assurance, focusing on key risks, both current and emerging, for business operations, reporting and compliance

ii) Comprehensive validation of the efficiency and effectiveness of the current internal control system, with prompt notification of control breakdowns, process deficiencies, data errors, missed SLAs with clients, IT security violations, Segregation of Duties violations, non-compliance with internal policies & procedures – which allows management to respond promptly with corrective action that prevents or minimizes losses.

iii) Prompt identification of non-compliance with external laws & regulations across diverse systems, geographies, summarizing them into an enterprise view of regulatory compliance, and enabling the organization to reduce the costs of compliance (penalties, etc), over time

iv) Deterrent against fraud owing to real-time, or near real-time audit activity

v) Greater risk & controls coverage by Internal Audit within budget constraints

Finally, a few key implementation perspectives, Do’s and Don’ts….

• Whether you are monitoring a risk or testing a control, and whether

you do it sitting at your computer, or by physically visiting a location, it must be remembered that under CA, you are providing a much deeper level of assurance, since the monitoring, testing and reporting is ongoing / repeated as per a pre-defined schedule, throughout the audit cycle. As a result of this ongoing / repeated testing, it is vital within a CA framework, to diligently follow the pre-defined continuous audit plan, to validate all potential findings with process owners, to summarize repeat audit findings into common trends, and to perform root cause analysis for each finding.

• It should also be noted that there are certain types of controls that are suitable for continuous controls testing – for instance, controls over high volume transaction processing, and certain others that are not suitable for continuous testing – for instance authorization controls over judgmental areas.

• Get Board sponsorship - this is not an IT project – it is a Business Improvement Program – position it, and treat it as such

• The Head of Internal Audit / CAE provides the vision, and a “CA Champion” is needed to provide the push and the glue that keeps different stakeholders moving towards the common goal of program success

• Start small, with “low-hanging fruit”, build confidence, then gradually expand areas covered by CA

Internal auditors should aim to provide continuous assurance on the risks to the organization’s objectives.

• When CA is first implemented, you will likely find a lot of exceptions. The exceptions were there yesterday, but no-one knew. Encourage recognition of the fact that you have moved the inspection ‘microscope’ from 1x to 1000x magnification

• Report continually - No surprises

CA is the way forward, and while it may be at the “cutting-edge” of developments in the internal audit profession today, it is soon expected to become one of THE MOST IMPORTANT ways in which the Internal Audit profession remains relevant to organizations of the future!
Hawkamah provides advisory services on various aspects of corporate governance for companies across the MENA region.

We develop tailor-made corporate governance frameworks for listed companies, banks and Islamic financial institutions, family-owned businesses, SMEs, state-owned enterprises, group companies, and private equity backed companies.

Hawkamah through our Mudara Institute of Director provides professional development courses and workshops for Board of Directors.

Our services include:
- Governance Assessments
- Development of Governance Codes and framework
- Customized Training and Workshops
- Board briefings
- Director Development Program (DDP)
- Company Secretary Workshop
Auditing Ethics

Introduction
Ethics is all about behavior, choices and doing what is right.

Internationally there have been developments around ethics and how organizations handle this. Many multinational companies have, over the past few years, appointed a senior executive with the responsibility for promoting ethical behavior throughout the company. While such appointments are more common in the United States than the rest of the world, this does not mean that ethics is not one of the priorities of a company. The ‘Tone at the Top’ is all about the board, chief executive officer and senior executives demonstrating their personal commitment to ethical behavior.

Ethics is the basis of good governance and ultimately the basis for the success of an organization. The lack of ethics can be safely described as the reason for many high profile corporate fraud cases.

Most organizations have a code of ethics for their workforce which prescribes expectations of the behavior expected of employees. In some cases, the code of ethics extends to consultants, contractors and suppliers. However, a robust ethics program is more than just a code of conduct; it also includes policies, regular communication, response protocols for ethical violations, etc. Regardless of who is responsible for the ethics program, the effectiveness is not always assessed. Therefore an audit of ethics becomes important to provide an independent view on the state of the organization’s ethics program.

The Role of Internal Audit
Internal auditors have often avoided the challenge of auditing ethics because it is difficult. Far easier to do a simple compliance or financial audit where hard controls are easier to audit than soft controls. However, the International Standards for the Professional Practice of Internal Auditing (The Standards) issued by the Institute of Internal Auditor (IIA) state that (Standard 2110.A1):
“The internal audit activity must evaluate the design, implementation, and effectiveness of the organization’s ethics-related objectives, programs, and activities.”

In 2011, as part of a global IIA survey, a research report showed that ethics audits were one of the top five topics for internal auditors to focus on over next five years. These results were fairly consistent across the type of organization (private, publically listed or government) and its location.

The Scope of an Ethics Audit
The IIA Practice Guide ‘Auditing Ethics-Related Programs and Activities’ states that the four pillars of organizational governance are the board, management, internal audit, and external audit, and that ethics is an integral part of this organizational governance structure. This means that any assurance provided around governance needs to take into account ethics. Internal audit needs to audit ethics in order to provide an opinion to the audit committee and senior management on its effectiveness.

An audit of ethics should at least cover the following:

- **Tone at the top** – commitment of the board and top management to ethics.
- **Ethical principles** – how well these are adhered to by all levels of the organization, including stakeholders and suppliers.
- **Risk management** – recognition of the need for risk management and effective implementation of risk management throughout the organization.
- **Information** – availability of such as a documented ethical program, awareness activities, and breaches of

Ethics is the foundation of any successful organization and internal audit has a key role to play by auditing the organization’s ethical program.
ethics guidelines.

- **Sharing** – active sharing of information relating to the ethical program and its results.
- **Alignment** – risk management alignment with the organization’s ethical culture.

### Key Considerations to Auditing Ethics

There may be several approaches to take when carrying out an ethics audit such as reviewing ethics policies and procedures, reviewing the work of the ethics or compliance department or surveys/interviews with employees. Regardless of the approach taken, there are several considerations that should be taken into account:

1. **The audit committee should identify specific ethics-related issues on which to focus.** In some settings, the committee may decide to conduct a comprehensive ethics audit. In other organizations, the committee may focus on specific ethical issues that are especially important in those settings.

2. **An audit of ethics needs to be risk-based and based on a risk assessment.** The internal auditor must establish the key risks to the organization’s ethics program which will help to focus the audit objectives.

3. **Realistic audit objectives need to be set,** which are likely to include such things as whether:
   - There is compliance with laws, regulations, and policies.
   - The organization has a documented ethics program and adequate means of measuring its effectiveness.
   - There has been effective implementation of the ethics program.
   - Breaches of the ethics program have been properly investigated and adequate sanctions imposed on offenders.
   - Lapses in ethical behavior have an impact on the efficiency, effectiveness and, if so, what is the impact on the organization.

   - **Assets are properly safeguarded from unethical conduct.**
   - **Opportunity for fraud and corruption is minimized.**

4. **Determine how to audit controls around ethics:**

   **“Internal auditors should help a company improve its ethical culture”**

   - **Tone at the top from the board, chief executive officer and senior executives.**
   - **Employee awareness.**
   - **Assurance regimes to identify unethical conduct and its impact on the organization.**
   - **Code of conduct and treatment of breaches.**
   - **Reporting arrangements for alleged unethical conduct.**
   - **Investigation protocols and if these are independent.**
   - **Effectiveness of whistleblower mechanisms and treatment of whistleblowers.**

5. **Report the audit results without fear or favor to the audit committee and senior management.**

6. **Monitor and follow-up to ensure recommendations are effectively implemented and meaningful change occurs in a timely way.**

The IIA’s Practice Guide provides more guidance on how to audit ethics and to evaluate the maturity of an ethics program.

### Conclusion

Conducting an ethics audit requires a team effort as well as a clear definition of ethical behavior. Auditing ethics is not only required by the IIA’s Standards but it is essential for the overall health of the organization. Even though there is no “one size fits all” approach to auditing ethics, the internal audit department should still take steps to audit the ethics program. Just because it is a difficult audit to do is no reason to ignore it especially when the risk of not carrying out an ethics audit can be severe.

### References:

1. **What's Next for Internal Auditing?** The Institute of Internal Auditors Research Foundation (2011)
2. **The Institute of Internal Auditors’ Practice Guide: Evaluating Ethics-Related Programs and Activities** (June 2012)

---

Al Shareef Marwan Al Khouli, CPA, MBA, CFE, CPM, CRA, CRP, CFC is General Manager - Head of Internal Audit Group at Oman Arab Bank.
A family business refers to a company where the voting majority is in the hands of the controlling family. Several studies have shown that family owned companies outperform their non-family counterparts in terms of sales, profits and other growth measures. Some of their strengths include commitment from family as business owners, willingness to pass knowledge and experience, willingness to work harder and reinvest in the business, family name and pride associated with the business.

It is also a fact that most family businesses have a very short life span beyond their founder’s stage and that 95% of the family businesses do not survive the third generation of ownership. Main reason for this being complexity, informality due to absence of articulated practices and procedures and lack of discipline.

The evolution of family business can be projected into three stages; the founder stage, the sibling partnership stage and the cousin confederation stage. In the founder stage, the business is entirely owned and managed by the founder. In the sibling partnership stage, management and ownership is transferred to the children of the founder. In the cousin confederation stage, the business governance becomes more complex as more family members are directly or indirectly involved in the business, including children of the siblings, cousins, and in laws.

Each stage brings with it unique governance challenges. The following table summarizes the key family governance issues faced by family businesses during their development cycle:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Issues</th>
</tr>
</thead>
</table>
| The founder stage             | Leadership transition  
Succession  
Estate planning                |
| The sibling partnership       | Maintaining team work and harmony  
Sustaining family ownership  
Succession                     |
| The cousin confederation      | Allocation of corporate capital; dividends, debt and profit levels  
Shareholder liquidity  
Family conflict resolution  
Family participation and role  
Family vision and mission  
Family linkage with the business |

Six steps that can help family businesses to attain business continuity are:

**Step 1: Establishment of Family Constitution**

The family constitution is a statement of the principles that outline its commitment to core values, vision and mission of the business. It’s a living document that evolves as the family and its business continue to grow. A typical family constitution will cover the following elements:
- Family values, mission statement and vision
- Family institutions such as family assembly, family council, education committee and family office
- Authority, responsibility and relationship among the family, the board and the senior management etc.

**Step 2: Forming Family Governance Institutions**

Family governance institutions help strengthen the family harmony and relationship with its business. Deciding what type of institution to establish will depend on the size of the business, the family’s stage of development, the number of existing family members and the degree of involvement of family members in their business.

- **Family Assembly**: It is a formal forum, which meets 1 or 2 times in a year, to discuss business and family issues. Family assembly is open to all family members, with some restriction such as minimum age, participation of in-laws and voting rights. Its role is to approve family vision, values, family related policies, election of committee’s member etc.
- **Family Council**: It is the governance body for the assembly. Family council comprises of 5 to 9 members elected by the family assembly and meets 2 to 6 times in a year. Its role is to act as bridge between family, the board and senior management, suggest name for board candidate and formulate family polices etc.
- **Family Office**: It is an investment and administrative center that is organized and
overseen by the family council. It looks after family member’s personal investment, taxes, insurance coverage, estate planning, career counseling and other areas of interest to individual family members. This is managed by professionals.

- **Other Family Institutions;** Depending on size, the family business can have education, share redemption, career planning, family reunion and recreation committees.

**Step 3: Establishment of Advisory Board and Board of Directors**

As the family business gets more complex, it becomes necessary to establish two boards, the Advisory Board and the Board of Directors. This allows the family business to become more organized and well-focused.

- **Advisory Board;** the advisory board is a group of experienced and respected individuals outside the family. The members of the advisory board are usually experts in the family business industry and market or in other areas such as finance, marketing and international markets. Over a period of time and once the family sees the added value of the advisory board, some of its members are often invited to join the Company’s BoDs.

- **Board of Directors;** in family business, BoD constitutes of family members and company senior managers. The BoD look in to the matters of strategy, succession planning, finances, internal controls, risk management and reporting to the owners and other interested parties. The presence of independent directors in the Board can play a vital role in the board meetings. Independent directors can bring an outside perspective on strategy and control.

**Step 4: Developing Family Member Employment Policy**

Many family businesses that didn’t set up clear employment policies for their members end up with more employees from the family than the company needs. As the family business reaches the sibling partnership stage of growth, it becomes necessary to formalize the family members’ employment policies. This would require setting up clear rules about the conditions of entry, staying, and exit from the business. The policy should also cover the treatment of family member employees in comparison with non-family employees.

**Step 5: Succession Planning**

Many family businesses put off the succession planning of their senior managers until the last minute, which leads to crisis. This could indeed be one of the reasons most family businesses disappear before they reach their third generation. Effective succession plan should allow for the selection of the most competent person, whether it is a family member or not. In addition, it is crucial to involve all family members, the board, key senior managers and other important external stakeholders in the selection process and make sure they agree on the next choice.

**Step 6: Exit Strategy of Family Member**

There should be clarity over the mechanisms that allow family members to sell their shares if they prefer to exit from the family business. Preparing an exit strategy well in advance helps avoid many conflicts and increases chances of business continuity. Some family businesses establish a “Shares Redemption Fund” in order to buy back any shares that family members would like to liquidate. The Fund is usually financed by contributing a small percentage of profits to it every year.

**Conclusion**

These initiatives are not exhaustive but are some of the fundamental factors crucial for business sustainability. Studies suggest that family businesses that demonstrate good corporate governance not only enjoy greater longevity, but improve efficiency, effective risk management and greater rewards for all stakeholders.

**References**


Bringing Powerful Insights and Proven Delivery to organizations in the areas of:

Internal Audit Services - IT Consulting - Business Consulting - Governance, Risk & Compliance
Financial Risk Management - Fraud, Investigations & Forensic Services
Human Capital Consulting - Transaction Services - Finance & Accounting Excellence

Contact Us:

ABU DHABI
Tel: +971 2 658 4640
Email: abudhabi@protivitiglobal.me

BAHRAIN
Tel: +973 1710 0050
Email: bahrain@protivitiglobal.me

DUBAI
Tel: +971 4 438 0660
Email: dubai@protivitiglobal.me

QATAR
Tel: +974 4421 5300
Email: qatar@protivitiglobal.me

SAUDI ARABIA
Tel: +966 11 293 0021
Email: saudiarabia@protivitiglobal.me

KUWAIT
Tel: +965 2242 6444
Email: kuwait@protivitiglobal.me

OMAN
Tel: +968 2469 9403
Email: oman@protivitiglobal.me

www.protiviti.com
The 2014 Global Retail Development Index1, issued by A.T. Kearney, indicated that gross domestic product of the Middle East will continue growing, which will bolster consumer confidence. Further, upcoming monumental events, such as Expo2020 in Dubai and Football World Cup 2022 in Qatar, will have a positive impact on the retail sector. There are other factors which will boost the growth of the retail sector, such as the construction boom in the region supported by significant national investments in infrastructure. The expansion in retail stores operating under international or local trademarks will increase the potential business risks and force companies to draw up policies and action plans to curb such risks. Furthermore, the role of the internal auditor has become pivotal to evaluating the effectiveness of policies and procedures; and informing senior management of any improvements that may assist in achieving the objectives of the company.

The proper management of business risks at retail stores boosts competitiveness. The senior management team should view risk management a means to assist in making decisions concerning the company’s investments and its sustainability thereof. Accordingly, we have to review the most critical risks faced by retail stores, the auditor’s role, and the sufficiency of internal controls to address such risks.

1 A Decline in Consumer Spending
The decline in consumer spending is the greatest danger facing retail stores, as it has a material impact on cash flows, which in turn affects the day-to-day operations relating to purchases from suppliers and meeting the daily obligations of the company. Consumer spending is affected by a host of factors that the company cannot easily control, such as local and international economic factors and the price of oil.

The role of the internal auditor should be to ensure that the company:
- Takes proper procedures to monitor and consider the impact of the changes in economic indicators such as government spending, oil prices, and unemployment;
- Monitors a consumer confidence index designed to measure consumer optimism on market conditions, and constitutes a tool for predicting consumer behavior;
- Adopts a proper strategy to increase consumer spending; and
- Monitors daily sales and considers the consequences of any decrease in these sales.

2 Reputation Risks
The retail sector is characterized by direct contact with consumers and the worse problems for retail stores if when customers stop buying from these stores or view them negatively. Further, reputation risks have increased due to social media and the internet. Accordingly, any shortcomings in consumer satisfaction may quickly impact a store’s reputation and hence its revenue.

The role of the internal auditor should be to ensure that the company:
- Conducts periodic consumers satisfaction surveys and formulates surveys to predict customer needs and expectations;
- Adopts a consumer relation management system to deal with any complaints and reply to any inquiries;
- Analyzes mystery shopper results to measure the quality of the rendered services as well as the quality of the employee-consumer relation;
- Provides proper training to employees; and
- Draws up a policy for dealing with social media with swift replies to any negative comments affecting the stores or products.

3 Intense Competition
Retail business is known for intense competition due to limited barriers to entry. An increase in competition may hinder revenue growth. Competition through product price reduction is a major factor in consumer purchasing decisions.

The role of the internal auditor should be to ensure that the company:
- Determines its competitors and periodically monitors product prices in the market;
- Uses the concept of loyalty cards which helps in consumer analysis as well as predicting the products that satisfy consumer expectations;
- Adopts a product pricing strategy by understanding consumer behavior and the manner by which they make purchasing decisions; and
The role of the internal auditor should be to

- Works out a plan for sales increase by taking advantage of sporting events, beginning of the school year, and holidays.

4 Supply Chain Failure

Lack of goods to display is a sensitive issue for day-to-day operations and can result from a failure in the supply chain. The role of the internal auditor should be to ensure that the company:

- Qualifies more than one supplier without depending on a specific supplier;
- Uses proper forecasting of sales;
- Adopts stock management policy;
- Controls the stock periodically and maintains reasonable levels. This ensures smooth store operation without facing any product shortage; and
- Adopts an automated system to review the level of available stock in the stores to meet any increase in the sales of a specific product as well as securing direct supply to the stores.

5 Online Shopping

Online shopping is one of the emerging risks that may increase due technological developments. A recent study issued by PricewaterhouseCoopers2 in early 2015 showed that online shopping is expanding at the expense of traditional retail stores. The study indicated that smart phones play a pivotal role in the online shopping boom, as 17% of the respondents shop weekly online whilst 28% prefer traditional retail stores.

The role of the internal auditor should be to ensure that the company:

- Adopts procedures for identifying and complying with any changes made to laws and legislations;
- Adopts procedures for following up on the terms of agreements and licenses; and
- Fixes a time period for initiating the action required for renewing agreements and licenses prior to expiry.

7 Fraud and Theft

Fraud risk arises when customers pay using counterfeit money or credit cards, and employees manipulate discounts granted to them to sell goods at a cheaper price. Further, direct thefts from retail stores either by customers (stealing goods) or by store employees (stealing goods or money) occurs very often.

The role of the internal auditor should be to ensure that the company:

- Uses money counting equipment and counterfeit detectors;
- Controls credit card transactions on a daily basis.
- Develops a clear policy on employee discounts, including a maximum amount of the discount granted to each employee, and develops a periodic report on the same;
- Hires security employees at stores containing high value goods, and insures goods against theft; and
- Secures goods against fire and maintains a valid insurance policy.

8 Improper Storage of Goods

Goods are sometimes stored in an improper manner. They may be stacked without any consideration of the safety factors inside the stores. Thus, it becomes very difficult to deal with any fire or emergency. It is also necessary to comply with the requirements of goods storage to avoid any damage thereto in the same manner adopted for handling medicine and foodstuffs requiring storage in an environment at a specific temperature. The role of the internal auditor should be to ensure that the company:

- Develops procedures for storing goods in compliance with the safety conditions;
- Periodically reviews storage conditions for each type of good; and
- Secures goods against fire and maintains a valid insurance policy.

Conclusion

The retail store business is vulnerable to several risks that should addressed in order to avoid potential losses. The importance of the internal auditor’s role is to ensure the sufficiency and effectiveness of policies and procedures established to mitigate such risks. The development of a risk based audit plan helps the internal auditor to cover the high risks affecting retail stores, and evaluate the established controls to adequately address such risks.

References:

MOHAMMED KHALIL AL JALLAD, CIDA, CFC is an audit and accounting professional who works at a leading institution in Kuwait.