IIA Malaysia e-techline
January 2019 Issue 01/19

AN EARLY LOOK INTO AT INTERNAL AUDIT PRIORITIES FOR 2019

It may be useful to take an early look at the priorities your peers are planning to address in the year ahead. Risk is what shapes our audit plans, directs our stakeholders, and determines our success or failure. That is why we spend so much time and effort helping our organisations identify, understand, and mitigate or leverage risks. Understanding the unique mix of risks our organisations face, and the risk appetites of our stakeholders, is crucial to internal audit adding value.

The challenge is to identify or anticipate unexpected, emerging, or atypical risks that may mature in the coming weeks or months, in hopes of preparing to gird against them or use them to benefit the organisation.

Two recently published reports, one from Gartner Inc. and the other from the European Confederation of Institutes of Internal Auditing (ECIIA), identify a familiar foe as the top risk for 2019: cybersecurity. Over the years, this challenge to organisations has consistently climbed up the risk hierarchy in annual reports. It also has opened our eyes to other risk categories, as our understanding of cyber becomes more sophisticated and our approaches to managing it mature.

Indeed, the focus on cybersecurity has helped us to understand that technology and data are inexorably intertwined, and it has increased our awareness of risk related to data governance and data privacy. It has driven us to be more cognisant of risks related to third-party relationships, IT governance, and culture.

For example, four of the top five risks in the Gartner report arguably stem from our focus on cybersecurity – cybersecurity preparedness, data privacy, data governance, and third-party risk. *Risk in Focus 2019,* the report developed and produced by the ECIIA, groups cybersecurity, IT governance, and third-party risks into one category. Data and technology also are central to risk discussions on digitalisation, automation, and artificial intelligence. These discussions neatly demonstrate the challenge of balancing risk and opportunity.

The Gartner report, which surveyed 144 CAEs, found two-thirds of respondents said they had experienced either a third-party-related disruption in the past two years or lacked sufficient knowledge of third-party activities to identify a disruption. What is known is that third-party risks are growing more complex as digitalisation, data sharing, and weak oversight of third-party relationships threaten to expose organisations to reputational harm.

It is easy to fixate on data- and technology-driven risks, but others certainly exist, as the two risk reports agree. Gartner identifies ethics and integrity as a risk that has evolved from culture risks identified in its 2018 report. The ECIIA report also identifies workplace culture as a risk. The Cambridge Analytica scandal provides another example. Facebook and its iconic founder, Mark Zuckerberg, suffered significant reputational damage for allowing the British company to mine personal information of millions of the service's users. It also raised awareness of the ethical responsibilities associated with data protection and privacy that now is viewed as a significant risk in both the Gartner and ECIIA reports.

As we look toward 2019, the risk landscape will likely focus on cybersecurity, data governance and privacy, third-party risk, and the evolving hazards associated with technology's impact on organisational ethics, culture, and integrity. As you prepare your internal audit plans for the coming year, you should ensure that you have considered all of the risks facing by your organisation and discuss them with your audit committees and executive management. The list is by no means comprehensive or necessarily applicable to all organisations. However, it does provide a useful benchmark as you contemplate what may lie ahead in 2019.

What CAE should do?

CAE should understand the unique mix of risks our organisations face, and the risk appetites of our stakeholders, is crucial to internal audit adding value. It is important to embrace the challenge in identifying or anticipating unexpected, emerging, or atypical risks

that may mature in the coming weeks or months, in hopes of preparing to gird against them or use them to benefit our organisations.

Reference:
https://iaonline.theiia.org/blogs/chambers/2018/Pages/An-Early-Look-at-Internal-Audit-Priorities-for-2019.aspx

TONE AT THE TOP - BUDGETING THE INTERNAL AUDIT FUNCTION: HOW MUCH IS ENOUGH?

Chief audit executives (CAEs) must ensure that internal audit resources are "appropriate, sufficient, and effectively deployed to achieve the approved plan," according to The IIA's International Standards for the Professional Practice of Internal Auditing. Board and audit committee members are similarly responsible for approving the right level of resources.

While there is no simple formula for determining an internal audit budget, there is a process that audit committees, executive management, and the audit department can use to determine whether the internal audit budget is appropriate for the organisation. By following these steps, all can be assured that the internal audit budget will likely be a good fit every time.

1. Define the Audit Universe.
Start the process by defining the audit universe, which is made of distinct "auditable entities" that, taken together, include every part of your organisation — all departments, divisions, systems, processes, subsidiaries, programs, activities, and even accounts. If it can be audited, it should be included in the audit universe as an auditable entity, even if there is no plan to perform an audit of that area in the coming year. The idea is to ensure nothing is overlooked.

2. Assess the Risks.
Working with key personnel throughout the organisation, internal audit will evaluate the likelihood of significant risks in each auditable entity. It will also estimate the probable impact of each type of risk to decide which risks are most important. Often auditors consider the velocity of risks, or the speed at which risks are likely to develop. Internal audit must consider everything that could impact the achievement of the company's objectives — not only negative impacts, but also the risks of missed opportunities.

The CAE generally will consult with management, the audit committee, and assurance providers such as external auditors, compliance officers, internal controls specialists, and risk management specialists. Internal auditors will also review the results of previous audits. The list of auditable entities is ordered from highest to lowest perceived risk, and brief descriptions are provided to explain why the area or process is considered high, medium, or low risk. Specific audits required by legislation or regulation are automatically moved to the top of the list. The list may be adjusted for factors such as length of time since the last audit.

3. Develop the Audit Plan.
To ensure that the schedule is flexible enough to address new and emerging risks, resources also should be allocated for unplanned "quick response" audits. The draft audit plan must also strike an appropriate balance between traditional assurance engagements and consulting work. Cost is a factor, but the coverage must be adequate to protect the company against the risks it can't afford to take. The secret is to balance what your organisation requires in terms of internal audit's services against specific identified risks. Because the appropriate level of internal audit resources can be subjective, many audit committees periodically review the top five risks that internal audit will not be able to address with current resources. If the audit committee is not comfortable with the level of risk in the areas that are not included in the proposed audit schedule, it's time to consider whether the budget should increase so additional audits can be performed.

4. Determine Training, Co-sourcing, and Administrative Expenses.
Budgets and schedules must also allow for time-off, as well as time spent on administrative tasks, training, and activities such as quality assurance and audit follow-up. It is important to consider training needs

... 2

carefully — not just training budget, but also the impact training might have on the number of audits that can be performed during the year. The CAE must ensure that internal audit resources will be appropriate, sufficient, and effectively deployed to achieve the approved plan with the breadth, depth, and timeliness expected by senior management and the board.

5. Review and Approve: Independence Matters.
It's important to review the operating budget periodically to ensure that it remains realistic and accurate, identifying and reporting any variances promptly. In most organisations, the CAE prepares the budget and senior management reviews it, but final review and approval are left to the audit committee or board of directors. One factor that makes a significant difference in internal audit budgets is the audit committee independence.

What CAE must do?

CAE must ensure that the internal audit resources will be appropriate, sufficient, and effectively deployed to achieve the approved plan with the breadth, depth, and timeliness expected by the senior management and the board. The approval of the plan and resources to obtained from the audit committee.

Reference:
https://dl.theiia.org/AECPublic/Tone-at-the-Top-December-2018.pdf

ADDING VALUE IN REVENUE & RECEIVABLE AUDITS

Internal auditors can focus on specific areas of revenue and receivables audits to ensure alignment with organisational objectives. External auditors and in-house Sarbanes-Oxley auditors perform test procedures to validate various assertions related to revenue transactions, receivables balances, and their presentation and disclosures in the financial statements. Internal auditors can work with management to ensure that the revenue and receivables processes are set up and controlled effectively to achieve the organisation's goals. There are several areas on which internal audit can focus to help achieve this objective.

1. Pricing Strategy.
Internal auditors should interview senior management to get insight into the assumptions, historical sales growth analysis, customers' feedback and forecasts, and other resources tapped to gain the pulse of the market. This insight will help internal auditors assess if the pricing strategy is moving in the right direction to help the organisation achieve its goals. If not, internal audit should discuss with management how to improve the analysis and pricing strategy.

Once satisfied with the pricing strategy, internal auditors should then evaluate transformation of this strategy into the actual pricing structure, assess whether the framework provided to the sales team for negotiating with customers aligns with the pricing strategy, and ensure that the approvals for pricing structure and negotiations include exceptions to the pricing strategy.

2. Having the Right Customers.
In a business-to-business model, working with profitable and creditworthy customers is a sign of sustainability and consistent growth year over year. When reviewing the customer selection process, internal audit should:

- Ensure adherence to these policies.
- Assess the adequacy and reliability of resources used to check customers' credit rating (good credit provides reasonable assurance over revenue collection).
- Evaluate profitability at a customer level and question management on loss-making deals (profitability analysis provides visibility over profitable deals).

3. Having the Right Customers.
This area is more applicable to organisations that provide a complex bundle of services. Such sales need a well-drafted contract detailing all performance obligations. Internal auditors should check for the existence of control where contracts are reviewed by legal experts, an accounting policy team, and an operations team, and are approved by the appropriate

management level to protect the company from unwanted obligations and commitments. If a contract template with standard clauses is already developed, the auditor's job is to focus on any non-standard terms agreed upon by customers and assess their reasonability and approval process effectiveness. Internal audit should risk-rank the contracts based on their contribution to the organisation's objectives and then develop a testing strategy to review the reasonableness of key non-standard terms. The higher the number of non-standard terms, the greater the challenge for internal auditors.

4. Conversion of Orders to Invoices.
Internal auditors should confirm that a process exists to capture the goods or services provided to customers and to invoice them for these goods or services. Prices for goods and services sold by the organisation should be updated in the price database, and the revenue system must capture all goods and services sold to customers for accurate invoicing. Internal auditors should pick up on clues about process gaps, control weaknesses, and system.

These areas could reveal missing management oversight and potential revenue leakages, constraints through process map reviews, data analytics, rework queues, pain points, and process improvement ideas communicated by management.

5. Tracking Receivables and Collection Efforts.
The receivables aging report is a good source to determine tracking process efficiency. Internal auditors should analyse write-off data to identify outliers, such as the same employee writing off certain customers' dues frequently or the same customers' dues getting written off often. The root causes of these outliers will help reveal the process control issues.

6. Recording Cash Receipts.
Cash receipts include electronic fund transfers, checks, credit cards, and physical cash receipts. Internal auditors can focus on the timeliness of recording the collection of cash in addition to the adequacy of segregation of duties and sufficient oversight in receiving, depositing, and recording cash funds.

7. Performance Metrics.
Internal audit should review the accuracy of key metrics to ensure that the data used for metrics calculations are correct and current. Internal auditors also can suggest additional metrics that will be useful to management.

What Internal Auditors should do?

Internal auditors should perform all 7 points highlighted in order to add value in Revenue and Receivable audits.

Reference:
https://iaonline.theiia.org/2018/Pages/Adding-Value-in-R-and-R-Audits.aspx

THE UNSCRUPULOUS ADVISOR

Internal auditors at investment firms should look out for schemes to overbill clients — even when they originate at the top of the organisation. A federal grand jury has indicted the CEO of an investment management firm on 23 counts of fraud, the *Idaho State Journal* reports. Federal prosecutors say David Hansen, majority owner of Yellowstone Partners LLC, headquartered in Idaho Falls, Idaho, overbilled client accounts by submitting false billing requests to a brokerage firm. Last year, former Yellowstone Partners employees told the *Post Register* newspaper they had found "significant irregularities" in some customer accounts in 2016. Prosecutors estimate Hansen's alleged scheme defrauded clients of more than $9 million. The indictment also charges Hansen with aiding in preparing false corporate and personal income tax returns that underreported the company's revenue and his own income in 2012 and 2013.

The CEO of the investment management firm in this story allegedly has run afoul of the U.S. Securities and Exchange Commission (SEC) and more particularly Section 206 of the Investment Advisers Act of 1940 (the "Advisers Act"). In part, Section 206:

"prohibits misstatements or misleading omissions of material facts and other fraudulent acts and practices " in connection with the conduct of an investment advisory business. As a fiduciary, an investment adviser owes its clients undivided loyalty, and may not engage

... 4

in activity that conflicts with a client's interest without the client's consent."

What Internal Auditors should do?

Internal auditors should consider measures to help their organisation prevent and detect the kind of fraud represented in this story.

Reference:
https://iaonline.theiia.org/2018/Pages/The-Unscrupulous-Advisor.aspx

"WE ARE HERE TO HELP YOU": MANAGING RELATIONSHIP WHEN MANAGEMENT IS SKEPTICAL

Is Internal Auditor (IA) viewed as nitpickers, time-wasters or even a bearer of bad news?

It is always good to take a hard look at how IA is viewed and how IA can change mistaken perceptions about IA in the minds of skeptical clients. Richard Chambers has offered some tips to win over the skeptical or adversarial clients.

1. Manage Expectation.
Good relationships start with keeping our promises, and we can help audit clients avoid future disappointments simply by not promising results that we are not sure we can deliver. If you're not certain when an audit report will be approved, for example, don't promise the report for "next month." If you are not sure how long the audit will continue. If you promise to limit the on-site presence of your audit team to a specific time frame, you should make every effort to meet that deadline. Of course, if your team discovers significant problems or potential fraud, all bets are off.

2. Practice the Fine Art of Appreciation.
Thanking clients for their time at the beginning and end of an audit is obligatory. But if you are not showing appreciation to your clients throughout the audit, you are missing opportunities to turn audit adversaries into supporters. It is particularly important to show your appreciation when you are not in the agreement. If a client questions findings or criticises your audit, for example, try starting by saying, "Thank you so much for sharing your perspectives. How would you recommend we word that instead?"

3. Don't Dwell on the Past.
Clients can't undo the past, so it helps to keep conversations forward-looking. The easiest way? Limit phrases like "should have" and "failed" in your client meetings and audit reports. Instead, substitute "from now on" or "in the future." The change is subtle, but you are repositioning internal audit from being perceived as a fault-finder focused on past mistakes, to being forward-looking and focused on future improvement.

4. Practice the Art of Listening.
We all know that listening is an important component of communication, but auditors too often forget that, just because you understand your client's point of view, it does not mean that the client is finished talking about it. Internal audits often surface troublesome issues, and when clients push back, it can well mean they feel they have not been heard or that you don't understand their point of view.

5. Try to Conclude Every Conversation with a Consensus.
The best way to transform the skeptical client is to consistently strive for a consensus. In only a few seconds, simple words such as, "Let's see if we can't find some common ground" can diffuse a confrontational discussion and demonstrate your collaborative attitude. If, after extensive discussion, your audit client still vehemently disagrees with your conclusions, you should probably offer to reevaluate your conclusions to allow a cooling-off period. As the old saying goes, you may eventually "agree to disagree." However, clients almost always appreciate your efforts to reach consensus on audit results.

What Internal Auditors should do?

With the above tips, internal auditors should be able to forge a client relationship built on sustainable trust which ultimately can serve the organisation well into the future.

Reference:
https://iaonline.theiia.org/blogs/chambers/2018/Pages/We-Are-Here-to-Help-You-Managing-Relationships-When-Management-Is-Skeptical.aspx#disqus_thread

ASSURANCE IN THE PRIVACY REGULATORY AGE

Public outcry about the growing severity of data breaches has led to enhanced regulations around the world to protect consumers' personal information. The most prominent of these data privacy regulations is the European Union's (EU's) General Data Protection Regulation (GDPR). These data privacy laws can increase compliance risk for organisations and disrupt business operations.

Additionally, data privacy regulations prescribe requirements such as having written information security programmes, policies and procedures, and compliance with a security programme. New regulations also could impact organisations' long-term planning by forcing them to change current or future business approaches. Opportunities abound for internal audit to add value to ensure the organisation complies with data privacy regulations.

Internal audit can help ensure the organisation complies with the new wave of privacy regulations:

1. **Breach Management.**
With only 72 hours to notify victims after a data breach is discovered, organisations subject to GDPR need an established and tested incident response plan to ensure notifications occur succinctly and timely. The plan should ensure all third-party contractual data breach notifications are aligned.

2. **Choice of Consent.**
GDPR allows EU residents to choose whether and how organisations can use their personal data. The organisation's legal team should provide guidance about when consents must occur. This requires the organisation to document and maintain consents.

3. **Limitations.**
The organisation's retention policies should document the time period in which it retains customer data and complies with respective data privacy regulations. Compare data retention policy requirements to the tracking system to ensure data was removed as stipulated.

4. **Third-Party Vendor Management.**
GDPR requires organisations to gather third-party guarantees for compliance along with proof of compliance. These guarantees usually are included in contractual provisions along with provisions for overall vendor monitoring and oversight processes.

5. **Privacy Policy.**
An organisation's online privacy policy should note customers' rights and align with associated privacy regulations. Examples include the customers' rights to know how their data is used, request removal, and correct their data. Additionally, the privacy policy may include types of security practices the organisation may use such as encryption. Overall, internal audit's assurance activities should align with the respective online data privacy policies.

6. **Cross-Border Data Transfers.**
The regulations may prohibit data transfers or require specific data protections. Many governments are implementing cooperative agreements to permit data transfer while still appropriately protecting individual privacy.

Organisations should remain abreast of current developments to ensure compliance with data transfer requirements. Internal audit must understand the requirements of these intergovernmental agreements and ensure compliance with each requirement.

7. **Policy and Procedure Management.**
Internal audit assurance activities should focus on ensuring compliance with these policies and procedures and determining whether there are appropriate processes to maintain them.

8. **Data Management.**
Organisations usually have a data policy that categorises types of data and provides guidance on the manner in which each type of data should be secured. They should

formally define a data management program to ensure they maintain a data inventory and comply with existing policies and procedures.

What Internal Auditors should do?

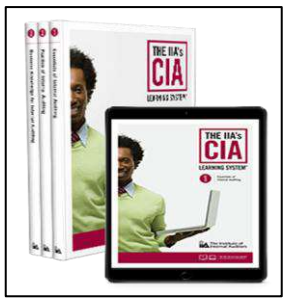
Internal auditors should remain abreast of current data privacy requirements that affect the organisation. This includes serving as consultants for management to implement appropriate compliance measures and posting audit assurance activities.

The annual audit planning efforts should include audits that will allow validation of current data privacy compliance. This is especially necessary with organisations facing the risk of increased fines and penalties as well as a heightened potential for lawsuits by victims of data breaches. In this environment, internal audit can help ensure the organisation has sound and prudent security practices.

Reference:
https://iaonline.theiia.org/2018/Pages/Assurance-in-the-Privacy-Regulatory-Age.aspx

BOOK'S REVIEW

The IIA's CIA Learning System Version 6.0



Format: Paperback + Online access
Year of Publication: 2018

The IIA's CIA Learning System Version 6.0 teaches and reinforces the entire updated global CIA exam syllabus in a flexible, online format, with optional printed books to ensure you're prepared to pass the CIA exam and armed with critical tools and knowledge to excel in your internal audit career.

New for Version 6.0!

- Aligned with updated CIA Exam Syllabi, testing January 1, 2019 and beyond
- 500 new test questions
- Download books to your e-reader, read online, or choose printed books (optional add-on)
- Link seamlessly from online quiz questions directly to pertinent sections of the online reading materials for convenient topic review
- Includes most recent IPPF enhancements
- Video tutorials providing an overview of the IPPF components

Gleim CIA Review Test Bank 2019 edition

Format: Paperback + Online access
Year of Publication: 2018

The Gleim CIA Book and Test Prep set allow candidates to study review materials written by professional educators and apply knowledge with the most realistic, exam-emulating multiple choice questions on the market. Our bank of multiple choice questions is refined collection of sample problems that provides candidates with a comprehensive review of questions as found on the CIA exam. Our test bank emulates the exam environment and provides detailed answer explanations for both correct and incorrect answer choices.

Reference:
https://www.iiam.com.my/book-list-catalogue/