IIA Malaysia e-techline
April 2020 Issue 2/20

CURRENT ISSUE

SIX TIPS FOR INTERNAL AUDIT TO REMAIN RESILIENT IN THE FACE OF THE CORONAVIRUS PANDEMIC

As the situation regarding coronavirus ("COVID-19") continues to deteriorate, businesses becoming stretched and challenged on multiple fronts. From the massive impact on supply chains, to staff availability, to a plunge in demand for products and services in hospitality, transportation, energy and many other industries, the pandemic is proving to be a real test for businesses and their disaster recovery and continuity plans.

Undoubtedly, the coronavirus has caused massive disruption to internal audit activities and lead to internal audit resources become stretched thin.

Below is a list of activities that internal audit teams can undertake to ensure they remain resilient in the face of the coronavirus outbreak.

1. Ensure Technical Capabilities are Performing Properly

Simple tasks such as ensuring team members have the ability to work remotely, VPN access is working and documents are placed in the cloud (such as OneDrive or Google Drive). Ensuring working papers are maintained on the cloud can help avoid disruption should audit team members need to work remotely.

2. Review the Annual Audit Plan

Review the plan to see what audits can be performed remotely or which ones can be deferred. As internal audit may draw into COVID-19 discussions more frequently, it may be worthwhile to defer less critical audits and free up available resources to assist the organisation with its business continuity planning. At this critical period, chief audit executives will want to ensure that their teams are still focused on the right risks and providing assurance where it is most needed.

3. Review Your Audit Team Structures

If there is a large number of audit team members, it may be worthwhile to reduce the number of auditors on a particular audit, extend the audit time frames, work remotely and ensure there is enough separation, so that an entire team does not become compromised.

It is also important to remind internal audit team members to stay home if they are not feeling well or think they may have been exposed to someone who has the coronavirus.

4. Review Your Audit Approach

Whilst most teams are likely already using Skype or Teams to have remote meetings, this can also be seen as an opportunity for internal auditors to try new techniques and approaches. Where possible, audit teams may wish to undertake more in-depth and detailed analytics rather than placing reliance on traditional walkthroughs and controls. Encourage a "safe to fail" environment and allow audit teams to try new things or investigate a workaround where traditional face-to-face meetings are not available.

It may also be a good time to encourage internal audit team members to undergo online training to increase capabilities while working remotely.

5. Bring in Guest Auditors

Where audit teams are geographically separated, it may be worthwhile to share resources across teams within your current office. For instance, if your Information Technology ("IT") audit team is located in another office and cannot travel, consider using IT team members based locally to assist with your audit processes.

For audit teams, it provides an opportunity for auditors to learn new skills, but to also educate others on the audit approach; For business areas, it can help them to better understand the role and purpose of audit. It can also help embed an audit mindset within business units.

6. Maintain Good and Regular Communication

As priorities change and resources move, it is important that to keep both management and auditees up to date on that activities of internal audit. Where an audit needs to be deferred or time frames revised, it is important that we communicate this to relevant stakeholders.

What CAE should do?

CAE to consider the above all as it is important that audit teams remain agile and flexible during these challenging times and it is likely that team members will need to be moved and priorities changed at short notice.

Reference:
https://internalaudit360.com/six-tips-for-internal-audit-to-remain-resilient-in-the-face-of-the-coronavirus-pandemic/

EHS PLANNING FOR COVID-19 AND BEYOND

Internal audit's role in crisis preparation and response.

As the threat of COVID-19 evolves by the day, people and organisations are evaluating what it means to them. At the extreme ends of the spectrum are those who see it as just another news story and those who proclaim it as the end of the global marketplace as we know it. Whatever the perspective, the worst time to plan for a crisis is in the middle of it. The prudent approach is to have a plan and implement it now.

Here are some essential steps in developing or modifying a crisis management plan for COVID-19:

- Determine the potential impact on organisational finances and work-related domestic and international travel.
- Find up-to-date, reliable pandemic information from community public health, emergency management, and other organisations. Create sustainable links to these resources so they are ready to access.
- Establish emergency communications protocols:
  - ❖ Back up key contacts,
  - ❖ Create a chain of communication (including suppliers and customers),
  - ❖ Develop processes for tracking and communicating the status of facilities and employees,
  - ❖ Test these systems to assure they are ready when needed.
- Implement an exercise/drill programme to test and, as necessary, revise the plan. This can be part of an overall emergency preparedness programme, using the 2016 National Preparedness for Response Exercise Programme (PREP) Guidelines as a guide.

Plan for impact on employees and customers Planning for COVID-19 must contemplate the effects on employees and customers.

The following are considerations for any organisation:

- Forecast and allow for employee absences due to factors such as personal illness, family member illness, community containment measures and quarantines, school and/or business closures, and public transportation closures.
- Implement guidelines to modify the frequency and type of face-to-face contact among employees and between employees and customers.
- Encourage and track annual influenza vaccinations for employees and evaluate access to and availability of healthcare.
- Identify employees and key customers with special needs and incorporate their requirements into the preparedness plan.

... 2

1. Establish Policies in Advance

The worst time to develop policies is during a crisis. Take the time to establish reasoned policies that are not created in the heat of the crisis. Policies should be considered for the following areas:

- Employee compensation and sick leave. Considerations for potentially prolonged absences unique to a pandemic (e.g., non-punitive, liberal leave) should include clear direction on when a previously ill person is no longer infectious and can return to work.
- Face-to-face employee interaction. Consider flexible worksite (e.g., telecommuting) and flexible work hours (e.g., staggered shifts).
- Suspected or confirmed exposure. Consider infection control protocols for employees who may have been exposed, are suspected to be ill, or become ill at the worksite (e.g., immediate mandatory sick leave, disinfecting work areas, establishing and monitoring potential exposure of co-workers).
- Implementing emergency protocols. Set up authorities, triggers and procedures for activating and terminating the company's response plan, altering business operations (e.g., shutting down operations in affected areas), and transferring business knowledge to key employees.

2. Protect Employees and Customers

Act now to assure resources are available to handle differences in demand during a pandemic. Take steps to assure that you can provide sufficient and accessible infection control supplies (e.g., hand-hygiene products, tissues and receptacles for their disposal) at all business locations. Supplies needed during a pandemic will be stretched, so identify alternate suppliers.

3. Educate Employees

Communication is always critical, and even more when facing a crisis. Anticipate employee fear and anxiety, rumours and misinformation, and plan your communication accordingly. Employees and customers need information to counteract panic and protect themselves, their families, and the company.

- Develop and disseminate programmes and materials covering pandemic fundamentals (e.g., signs and symptoms of influenza, modes of transmission), personal and family protection, and response strategies (e.g., hand hygiene, coughing/sneezing etiquette, contingency plans).
- Ensure that communications are culturally and linguistically appropriate.
- Share pandemic preparedness and response plans.
- Provide information to support at-home care of ill employees and family members. It is essential to develop platforms (e.g., hotlines, dedicated websites) for communicating pandemic status and actions to employees, vendors, suppliers, and customers inside and outside the worksite in a consistent and timely way, including redundancies in the emergency contact system.

Coordinate with external organisations and help your community Finally, it is important to realise that organisations do not operate in a vacuum. Make plans to leverage and support the community.

- Collaborate with major healthcare facilities and federal, state, and local public health agencies and/or emergency responders.
- Understand the capabilities and plans of federal, state, and local public health agencies and emergency responders.
- Share the organisation's crisis management plans.
- Share best practices with other organisations, chambers of commerce, and associates to improve community response efforts. While a single organisation cannot prevent a pandemic, many resources are available to plan for and manage its effects should they happen.

What CAE should do?

From an internal audit perspective, The IIA's International Standards for the Professional Practice of

... 3

Internal Auditing (Standards), on Due Professional Care (1220.A3) states, "Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources."

Standard 2010 requires chief audit executives to establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organisation's goals.

The related interpretation states: To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organisation's strategies, key business objectives, associated risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programmes, systems and controls.

Reference:
https://global.theiia.org/member-resources/Global%20Documents/EHS-Planning-for-COVID-19-and-Beyond.pdf

GLOBAL KNOWLEDGE BRIEF: REMOTE AUDITING FOR COVID-19 AND BEYOND

Most of the internal auditors begin to focus on conducting remote auditing in the current situation, due to the emergence of COVID-19 and its related worldwide travel restrictions.

This article will enable auditors to understand the following:

1) Reason for implementing remote auditing.
2) Pros and cons of remote auditing.
3) Strategies for implementing remote auditing, in each part of the audit engagement process (planning, document review, fieldwork, interviews and closing meetings).
4) The best practices from other organisations that have used remote auditing in their COVID-19 response.

On top of that, internal auditors can also rely on information technology in facilitating the remote auditing.

What Internal Auditor should do?

Auditors to refer to the article to have a greater understanding of what is remote auditing and how it can provide assurance to the management during this critical time.

Reference:
https://na.theiia.org/periodicals/Member%20Documents/EHSKB-Remote-Auditing-for-COVID-19-and-Beyond.pdf

GOVERNANCE

GLOBAL KNOWLEDGE BRIEF: DATA ETHICS

Where does internal audit fit?

Data are facts collected for reference. In the modern age, we often think of data in terms of electronic data, but on a basic level, data is simply raw information that has been observed and recorded. Modern technology allows us to record and store data on a scale never imagined. Data ethics looks at how data is collected, stored and used, whether it is for marketing, medical research, law enforcement or other purposes, and how the privacy of those whose data is collected is protected.

... 4

ELEMENTS OF DATA GOVERNANCE

1. Data Protection

Data protection is a central component of sound data governance and defines the ways an organisation stores, secures, moves, and disposes of data. Although data protection strategies vary from organisation to organisation, they retain a few core elements. For example, a sound data protection strategy should involve data mapping, which maps how data is moved from one system to another. This is essential to discovering potential privacy risks. However, data mapping is not possible without first creating a data asset inventory that accounts for all the data and information in the company.

Data protection strategy involves accounting for data lineage, which is the path that data takes through different platforms and environments. It records not only movement and data origin, but also how it relates to other data, who uses it, and what language was used in the applications pertaining to it. Today, artificial intelligence ("AI") can use techniques to track data lineage including sophisticated natural language processing, neural networking that allows the AI to learn data patterns and behaviors, and machine learning that uses those same networks to teach machines how to learn and gain insights. This allows AI to catch instances of misuse at any stage of the data handling process, from acquisition to disposal.

2. Internal Auditing and Data Ethics

Internal auditors' function as the final line of defense in an effective data governance strategy. Through their engagements, they could assess the effectiveness of data protection policies and if they are being properly executed. The internal auditors should perform the following:

- To evaluate data ethics when applicable as part of their engagements.
- To be aware of industry-specific regulations and any data privacy requirements.
- To research and understand emerging and evolving risks regarding data as applicable.
- To consult with subject matter experts when necessary.

3. Consumer Notification Procedures

In the event of a data breach, regulations often state that organisations must inform their customers and authorities of the incident. This varies by region and specific regulation.

4. Codes of Conduct

A well-thought-out and enforced employee code of conduct can help to prevent regulatory issues, such as the privacy and data handling violations, that are central to data ethics discussions. Though different industries and even individual organisations have specific requirements for their codes, certain core fundamentals exist. For example, a code of conduct should always outline the responsibilities and restrictions regarding data use for employees, as well as actions and consequences if data is misused. Additionally, training should be provided for new employees with updates on a periodic basis, as well as regular refresher training for all current employees. This helps to reinforce the importance of data privacy and proper handling.

What CAE should do?

To provide value to their organisation through incorporating internal control activities relating to data protection and data ethics into risk assessments and regular engagements as internal auditors can understand how their organisations obtain and handle all types of data, and if they do so in an ethical way.

Reference:

https://global.theiia.org/member-resources/Global%20Documents/GKB-Data-Ethics.pdf

TONE AT THE TOP

What Directors Need to Know Now

Director responsibilities are constantly evolving, but occasionally, there is a dramatic shift: a time when the rules of sound governance are fundamentally transformed. It happened shortly after the fall of Enron Corporation, for example, when waves of governance failures led to the enactment of legislation such as the Sarbanes-Oxley Act. Almost overnight, director responsibilities changed significantly. Board agendas expanded to previously unimagined complexity, and meeting schedules multiplied.

Date Governance Questions for Directors

1. What data are we concerned with?

Effective data governance starts by knowing what data is being collected, where it resides, and how it is being used throughout the organisation. In many cases, mapping the flow of data can enhance understanding and strengthen data governance.

2. Is our data being used properly?

The data governance system should help assure that data is available when needed for legitimate business reasons, but it must also protect sensitive information and assure that data is used ethically. Directors need to know whether the company has created adequate policies and procedures on data usage, and they need to ensure that there are controls to monitor and enforce the policies.

3. Have we defined specific goals for our data governance programme?

Every company is different, so there is no standard one-size-fits-all approach to data governance. If the data governance programme is relatively new, for example, it might be a considerable undertaking merely to determine where all of the organisation's critical or sensitive data resides.

Later, the focus might shift to minimising risks, increasing the value of data, improving the flow of information, or other priorities. Therefore, data governance goals and priorities should be reassessed regularly.

4. How have we evaluated the risks?

Every company must deal with risks such as data loss or corruption, data breaches, or compliance lapses. It is impossible to eliminate all risk, but it is important that the board receives timely information about significant data risks and evaluates whether the level of risk exposure is appropriate for the company's risk appetite.

5. When significant issues are identified, how do we assure that they are handled appropriately?

The board needs to understand the processes for communicating and addressing significant data governance issues. They also need to ensure that when problems are identified, they are addressed appropriately.

6. What about data governance frameworks?

A data governance framework provides guidelines for using data, managing it, and resolving data issues. It identifies the people and departments that should control and manage different types of data. Organisationally, the framework might include a data governance office that helps run the programme, along with a data governance committee or council that prioritises data governance projects; approves data usage policies, processes, and procedures; and identifies data stewards and stakeholders. If your company has not yet agreed upon a data governance framework that assigns specific responsibilities, it may be time to ask why not.

What CAE should do?

To advice their board on relevant data governance questions they need to know to fulfill their duty of oversight.

... 6

Reference:
https://dl.theiia.org/AECPublic/Tone-at-the-Top-February-2020.pdf

INTERNAL AUDIT

SHOULD INTERNAL AUDIT REPORTS INCLUDE RATINGS WITH FINDINGS?

Many internal audit shops include a rating or grade at the end of an audit report intended to summarise the findings and bring attention to the most important conclusions of the report.

Ratings may be scored with a number—from one to five, for example; a colour—often red, yellow, and green; with an adjective such as "satisfactory," "needs improvement," or "unsatisfactory"; with a letter grade from "A" down to "F"; or with other mechanisms.

1. Growing in Popularity

The practice of including rating in audit reports appears to grow in popularity. A survey by the IIA found that about two-thirds of internal auditor respondents said their organisations include some type of rating in their audit reports.

2. Creating Battleground

Despite their benefits, ratings can provoke disagreements. Few managers, not surprisingly, want to see their areas earn an unsatisfactory rating.

That is especially true when the ratings will be seen by upper management and could impact their performance reviews or compensation. Disagreements about ratings can consume time and energy that would be better spent identifying ways to remediate control weaknesses.

3. Using Ratings Effectively

Internal auditors can take steps to leverage the benefits of ratings while minimising their shortcomings. Before implementing a rating system, the organisation should have a fairly mature governance and risk management structure.

4. Be Objective

Another starting point is making the audit criteria as objective and as clear as possible. Just as students need to know how they will be graded, managers should understand the methodologies used by internal auditors evaluating their departments. The ratings—high, moderate, low—are not included in audit reports, but are in an audit issue log that's presented semi-annually to senior management and the finance and audit committee of the board.

5. Rating Alternatives

While the popularity of ratings shows no sign of decline, not all organisations use them. Some organisations identify issues as reportable or not reportable. While simpler than a rating structure, this still requires some judgment by the auditor. Typically, organisations looking to focus on the substance of their overall control environment are less likely to use ratings. They want a holistic conversation around risk.

What CAE should do?

Allowing management to provide input at the initial stages of developing new audit methodologies criteria helps in fostering understanding. As a result of this effort, management has a better understanding of and appreciation for the justification for assigning a particular rating.

Reference:
https://misti.com/internal-audit-insights/should-audit-reports-include-ratings-within-findings

PRACTICE GUIDE: IT CHANGE MANAGEMENT: CRITICAL FOR ORGANISATION SUCCESS (3rd EDITION)

Change management is defined as the systematic set of processes that are executed within an organisation's IT function to manage enhancements, updates, installations, implementations, incremental fixes and patches to production systems.

In order to ensure an effective change management control of IT in place, the control to include management of patch updates, enable management to address new development projects, regulations and system changes effectively and efficiently while appropriately utilising resources.

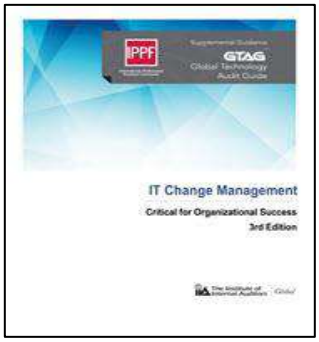
This guide will aid the internal auditors in evaluating processes and controls which subsequently provide assurance and advice that helps the organisation enhance its change management process.

This guide will enable internal auditors to:

1) Have a working knowledge of the change management process.
2) Distinguish between effective and ineffective change management process.
3) Recognise indications of potential control issues related to change management in IT environments.
4) Understand that effective change management hinges on implementing preventive, detective and corrective controls, including the appropriate segregation of duties and adequate management supervision.
5) Recommend the best practices for addressing these issues, both for assurance that controls mitigate risks and for increasing effectiveness and efficiency to the management.

You may also find the appendixes in this guide which provides tools to help internal auditors obtain and evaluate evidence to support assessments, such as the validation of control design and operational effectiveness, performance, efficiency and the accuracy of management's assertions.

You may also find the appendixes in this guide which provides tools to help internal auditors obtain and evaluate evidence to support assessments, such as the validation of control design and operational effectiveness, performance, efficiency and the accuracy of management's assertions.



Reference:
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Global-Technology-Audit-Guide-IT-Change-Management-Critical-for-Organizational-Success.aspx

PRACTICE GUIDE: AUDITING CREDIT RISK MANAGEMENT

Credit risk is one of the essential risk categories of the financial services sector. Regulators across the globe are focused on financial services organisations' credit risk management activities. Moreover, regulators and supervisors consider managing the credit risk one of the pillars required to maintain a robust and solvent financial sector, which in turn encourages a steady economic condition.

Given the complexity and importance of managing credit risk within a financial services organisation, this guidance will focus on credit risk arising from a financial services firm's lending practices. Further guidance will address more complex topics such as derivatives, hybrid investment portfolios, options and other structured securities.

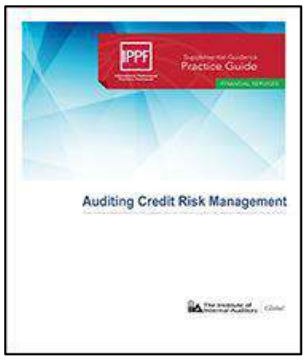
The purpose of this guidance is to provide internal auditors with a baseline skillset that allows them to test and evaluate the effectiveness of their organisation's credit risk management framework and processes.

This guidance will enable internal auditors to:

1) Understand the importance of credit risk in a financial services context.
2) Understand the regulatory environment and requirements related to credit risk.
3) Understand the risk governance and risk management processes surrounding credit risk.
4) Describe the nature and basis of measurement of the probability of default.
5) Design an audit engagement that assesses the appropriateness and effectiveness of the credit risk management framework and the adequacy of the institution's credit profile.
6) Apply IPPF and risk-based internal audit techniques to assess and audit credit risk in their organisation.

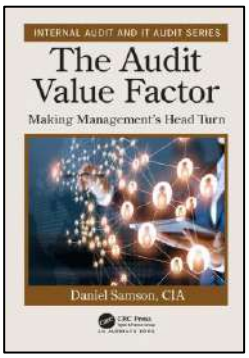
What Internal Auditor should do?

- The role of an internal auditor is to independently assess the adequacy and effectiveness of the policies, procedures, and processes applied by the organisation to manage credit risk.
- The internal audit activity provides assurance on whether the outcomes achieved by management affected by credit risk align with the mission, strategies, and risk appetite of the organisation, in addition to stated policies and procedures and regulatory requirements.
- Internal auditor verifies the correctness of the accounting criteria and the adequacy of the Loan Loss Reserve.



Reference:
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Auditing-Credit-Risk-Management-Practice-Guide.aspx

NEW RELEASES



The Audit Value Factor
By: Daniel Samson
Format: Paperback
Publication Year: 2019

Understanding and Auditing Corporate Culture: A Maturity Model Approach (*Coming soon)*
By: Angelina K. Y. Chin, CIA, CRMA, CPA
Format: Paperback
Publication Year: 2020

Reference:
https://www.iiam.com.my/wp-content/uploads/2017/11/Book-Order-Form.pdf