Emerging Issues and Challenges

Lesson 9

KEY CONCEPTS

■ Financial Accounting Risk ■ Funding Risk ■ Conflict of Interest

Learning Objectives

To understand:

- What is Financial Accounting & the risks involved in Financial Accounting?
- How Financial Accounting Risks can be avoided?
- What is Funding Risks? How it can be avoided?
- Why funding risk to be considered in internal audit?
- Various business related challenges while conducting internal audit
- Prons and Cons of In-house Internal Audit function
- Prons and Cons of Outsourcing of Internal Audit function
- Prons and Cons of Co-sourcing of audit assignment
- Various emerging areas to be looked in Internal Audit

Lesson Outline

- Financial Accounting and Funding Risks
- Business Related Challenges
- In-house vs Outsourcing Audit Assignments
- Emerging Issues
- Emerging areas getting into focus in Internal Audit
- Lesson Round-Up
- Test Yourself
- List of Further Readings

FINANCIAL ACCOUNTING AND FUNDING RISKS

Many businesses have to take risks when it comes to their finances. Whether it's investing in new projects or increasing production, there is always the potential for failure. But with the proper financial accounting and funding risk management techniques, one can minimise their risk and ensure the success of business.

Financial accounting and funding risk are two different topics, but they go hand in hand. Financial accounting is the process of recording and summarising financial information, while funding risk is the potential for losses due to inadequate or inappropriate funding. How financial accounts are managed can significantly influence the level of funding risk a company faces.

Poorly managed accounts can lead to insufficient funds, which in turn, can lead to cash flow problems and other financial issues. On the other hand, well-managed accounts enable companies to utilise their resources efficiently and effectively, minimising their exposure to funding risks. Let's explore different ways to manage financial accounting and funding risks. We will also look at how financial accounting and funding risk are related and how organisations should manage their finances to reduce risk exposure.

What is Financial Accounting?

Financial accounting is the process of recording, classifying, and summarising financial transactions to provide useful information in making business decisions. The three primary financial statements are the balance sheet, income statement, and cash flow statement. Financial accounting also includes preparing reports for taxation, regulatory compliance, and management decision-making.

The purpose of financial accounting is to provide information that is useful in making business decisions. The information provided by financial accounting can be used to make an investment, financing, and operational decisions. Financial accounting information is also used by government agencies to make policy decisions.

Financial accounting aims to create transparent and accurate financial statements that conform to generally accepted accounting principles (GAAP). Financial statements should be free from material misstatements and provide a true and fair view of a company's financial position and performance.

What are the risks of Financial Accounting?

There are several risks associated with financial accounting, which can be broadly categorised into two main types:

1. Financial risks; and
2. Funding risks.

Financial risks include the risk of errors or omissions in financial statements, the risk of fraud or misappropriation of assets, and the risk of non-compliance with laws and regulations.

Funding risks include the risk that sufficient funds will not be available to meet obligations when they fall due, the risk of losing access to funding sources, and the risk of incurring additional costs in order to raise additional funds.

Both types of risks can significantly impact an organisation's ability to continue operating and achieving its strategic objectives. Therefore, effective management of these risks is essential to ensure the long-term success of any organisation.

How can you avoid Financial Accounting Risks?

There are a few key ways through which one can avoid financial accounting risks:

1. **Understand the financial statements:** Review income statement, balance sheet, and cash flow

statement on a regular basis. This will help to identify any potential red flags or areas of concern on timely basis.

2. **Maintain strong internal controls:** Having strong internal controls in place will help to ensure that financial information is accurate and reliable. Testing and review of internal controls and identifying the gaps allows to have better and thorough understanding of the standard operating procedures. It also gives the insight on creating better strategies to protect organisation's reputation and financial risk.
3. **Work with a reputed accountant or financial advisor:** Getting expert advice can help to navigate through complex financial issues and make sound decisions for business.

What is Funding Risk?

When it comes to financial accounting, funding risk is the potential risk that an organisation may face when it comes to its ability to obtain funding from lenders or investors. This type of risk can arise due to several factors, including the overall health of the economy, interest rates, and the specific financial situation of the organisation in question.

For organisations that are dependent on external financing, funding risk can be a major concern. If an organisation is unable to obtain the necessary funding to keep operating, it could quickly find itself in financial trouble. As such, it's crucial for organisations to monitor their funding risk and take steps to mitigate it where possible.

There are a few different ways that organisations can manage their funding risk. One common approach is known as "risk hedging." This involves taking out loans or lines of credit from multiple lenders to diversify the sources of funding and reduce reliance on any one particular lender. Another approach is maintaining strong relationships with existing lenders and investors and keeping them updated on organisation's financial situation. Doing so will make more likely to have their continued support in times of need.

Funding risk is an essential consideration for any company that relies on external financing. By taking steps to hedge against this risk and maintaining strong relationships with lenders and investors, can help to protect business from financial difficulties down the road.

Why should funding risk be considered in an internal audit?

When it comes to financial accounting, organisations must take into account funding risk in the decision-making process. This type of risk can come from a variety of sources, including changes in interest rates, regulatory changes, and economic conditions. While funding risk is often out of an organisation's control, there are still ways to manage and mitigate it. Internal audit can play a vital role in identifying and evaluating funding risks, as well as in providing recommendations on how to best manage them. By considering funding risk in internal audit, organisations can make more informed decisions that can help protect their bottom line.

When it comes to financial accounting, there is always the potential for funding risk. This is because organisations rely on outside sources of funding, such as loans, lines of credit, and investors. If these funding sources dry up, it can significantly impact a company's ability to continue operating.

Internal audit teams should also consider funding risk when evaluating a company's financial statements. They should look at things like cash flow and liquidity to see if there are any red flags that could indicate a problem with funding in the future. If there are concerns, the internal audit team can work with management to develop a plan to mitigate the risk.

Funding risk is just one of many risks that internal audit teams need to be aware of. By considering all risks, they can provide valuable insights that help organisations make better decisions and avoid financial problems down the road.

How can avoid Funding Risks?

There are a number of ways to avoid funding risks when it comes to financial accounting. First, be sure to have a clear understanding of organisation's financial situation and goals. This will help to make informed decisions about how to allocate funds and where to invest. One way is to choose investment vehicles carefully. Make sure to understand the risks associated with each type of investment before commit any money.

Another way to avoid funding risks is to diversify investments. Don't put all of eggs in one basket, so to speak. By spreading money around, can minimise the risk of losing everything if one particular investment goes sour. Diversifying will help protect from market fluctuations and other risks.

Finally, stay informed about the latest developments in the world of finance and investing. The more you know, the better equipped you'll be to make smart decisions about where to put your money. And always be prepared for the worst-case scenario. Have a contingency plan in place in case something goes wrong. By being proactive and prepared, can help minimise the impact of potential risks.

Let's discuss the practical examples from the past:

Example 1:

The fall of the energy trading corporation Enron Corporation in 2001 is a relevant example of financial accounting and funding risk. Enron was once one of the world's largest energy companies and was highly regarded for its innovative and sophisticated accounting practices. However, in the late 1990s, Enron began to face financial difficulties due to its heavy investments in speculative energy trading and its risky use of off-balance-sheet financing.

Enron's financial statements during this period were highly complex and difficult to understand, making it difficult for investors and analysts to fully assess the company's financial health. In addition, Enron engaged in aggressive accounting practices that allowed it to book revenue from deals that had not yet been completed, leading to inflated earnings reports and a false sense of financial stability.

Enron's funding risks became apparent in 2001 when the company's credit rating was downgraded, and lenders began to demand more collateral for its debt. This triggered a downward spiral for Enron, as the company's stock price plummeted, and it was unable to secure new funding. In December 2001, Enron filed for bankruptcy, causing significant financial losses for its shareholders, employees, and creditors.

The collapse of Enron resulted in widespread public outcry and led to increased scrutiny of accounting practices and financial regulation. The incident also highlighted the importance of transparent and accurate financial reporting, as well as the risks associated with complex financing structures and off-balance-sheet transactions.

Example 2:

The bankruptcy of the German payment processing business Wirecard AG in 2020 is another illustration of financial accounting and funding risk.

Wirecard was once considered a rising star in the financial technology industry, providing electronic payment and risk management services to businesses worldwide. However, in 2019, a series of investigative reports by the Financial Times alleged that Wirecard had inflated its revenue and profits through fraudulent accounting practices.

Wirecard initially denied the allegations and launched an internal investigation, but in June 2020, the company admitted that €1.9 billion ($2.2 billion) was missing from its accounts. The revelation triggered a sharp decline in Wirecard's stock price and led to its eventual collapse.

The Wirecard scandal has raised questions about the reliability of financial reporting and auditing, as well as the effectiveness of regulatory oversight. It has also led to a broader discussion about the risks associated with investing in high-growth technology companies and the need for greater transparency and accountability in the financial sector.

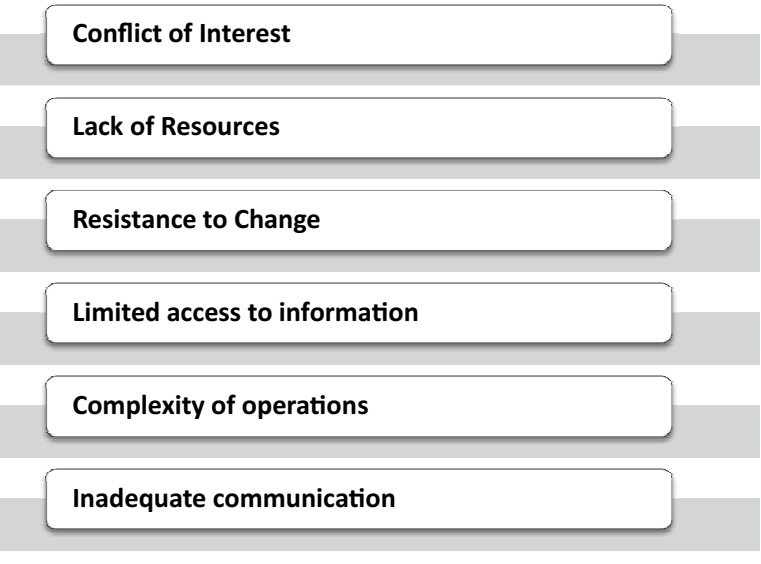
Conclusion

To summarise the discussion one can say, financial accounting and funding risk are two sides of the same coin. Poorly managed accounts can lead to insufficient funds, which in turn can lead to cash flow problems and other financial issues. On the other hand, well-managed financial statements help companies utilise their resources efficiently and effectively, minimising their exposure to risks.

Understanding the potential risks and taking steps to manage them properly can help ensure that business is financially successful. The use of financial accounting and funding risk can be complex and difficult to master, but the rewards for doing so are well worth it. Companies that understand the key concepts involved in these aspects of their business will have a much better chance of success than those that do not. Financial savvy is essential for businesses looking to survive in today's competitive economic environment, and having a firm understanding of financial accounting and funding risk can help give company that edge over the competition.

BUSINESS RELATED CHALLENGES

Conducting an internal audit of business can be a challenging task, and some of the common business-related challenges that may arise during the process include:



1. **Conflict of Interest:** One of the significant challenges of internal audit is managing the conflict of interest. In large business houses, Internal auditors are employees of the company, and they are expected to report on the operations of the business objectively. However, auditors may be hesitant to report negative findings if it could jeopardise their job security or relationship with their colleagues.

   For example, an auditor may face a conflict of interest if asked to audit the department where they worked before being appointed as an auditor. As a result, they may hesitate to report negative findings that could jeopardise their relationship with their former colleagues or impact their career prospects within the company.

Organisations can take the following precautions to avoid conflicts of interest in internal audit:

(i) **Develop and communicate clear policies:** Organisations should establish clear policies and procedures to identify and address potential conflicts of interest. These policies should outline the steps to be taken when conflicts arise, including recusal, disclosure, or seeking a second opinion.

(ii) **Ensure auditor independence:** Organisations should ensure that internal auditors have the necessary independence to conduct the audit objectively. This can be achieved by appointing auditors who are free from any conflicts of interest and establishing clear lines of reporting and accountability for auditors.

(iii) **Rotate auditors:** One way to reduce conflicts of interest is to rotate auditors between different departments or functions. This can help to reduce the risk of auditors becoming too close to the business units they are auditing and enhance the objectivity of the audit process.

(iv) **Encourage open communication:** Organisations should encourage open communication between auditors and management. This can help to ensure that any potential conflicts of interest are identified and addressed promptly.

(v) **Foster a culture of transparency:** A culture of transparency can help to reduce conflicts of interest by promoting openness and accountability. Organisations should establish clear channels for reporting conflicts of interest and provide support to auditors who raise concerns.

2. **Lack of resources:** Conducting an effective internal audit requires adequate resources, including skilled staff, technology, and time. However, many organisations may not allocate enough resources to an internal audit, resulting in suboptimal performance.

Lack of resources is a common challenge that organisations face when conducting internal audits. The lack of resources can compromise the quality and effectiveness of the audit process, leading to incomplete or inaccurate findings and recommendations.

To address the issue of lack of resources in internal audits, organisations can take the following steps:

(i) **Allocate sufficient resources:** Organisations should allocate adequate resources, including personnel, budget, and technology, to ensure that the internal audit team has the necessary support to conduct a thorough and effective audit.

(ii) **Prioritise audit activities:** Organisations should prioritise audit activities based on their impact and risk level. This can help to ensure that resources are allocated to the most critical areas, reducing the risk of overlooking critical issues.

(iii) **Adopt risk-based approach:** Adopting a risk-based approach to internal audit can help to focus the audit process on areas of highest risk. This approach can help to ensure that limited resources are used effectively and the audit team can provide more value to the business.

(iv) **Leverage technology:** Technology can help to enhance the efficiency and effectiveness of internal audits. Organisations should consider investing in technology tools, such as data analytics software, to help the audit team identify risks, analyse data, and automate manual processes.

(v) **Partner with external audit firms:** Organisations can also consider partnering with external audit firms to supplement their internal audit function. This can help to bring additional resources, expertise, and perspectives to the audit process, enhancing its effectiveness.

(vi) **Continuously review and adjust resource allocation:** Organisations should continuously review and adjust resource allocation to ensure that the audit function is adequately supported. Regular reviews can help to identify areas where additional resources are needed, and adjustments can help to ensure that the audit process remains effective and efficient.

3. **Resistance to change:** Internal audit may require changes in the business processes, systems, or culture. However, resistance to change may arise, making it difficult for the internal audit team to implement recommendations that could improve business operations.

   Resistance to change is a common challenge that organisations face when implementing new policies, procedures, or initiatives, including internal audits. Resistance to change can arise from a variety of factors, such as fear of the unknown, concerns about job security, and lack of trust in leadership. If not addressed effectively, resistance to change can hinder the success of internal audits and impede progress towards the organisation's objectives. To subdue resistance to change in internal audit, organisations can take the following steps:

   (i) **Communicate the need for change:** Organisations should communicate the need for change to all stakeholders and explain how the internal audit can help the organisation achieve its objectives. It is essential to be transparent about the reasons for the change and how it will benefit the organisation.

   (ii) **Involve stakeholders in the change process:** Involving stakeholders in the change process can help to address their concerns and build support for the internal audit. This can be achieved through consultation, collaboration, and active engagement with all affected parties.

   (iii) **Training and support:** Organisations should provide training and support to all stakeholders affected by the change, including the internal audit team, to help them understand their roles and responsibilities and build their capabilities. This can help to reduce anxiety and increase confidence in the new processes.

   (iv) **Recognise and address concerns:** Organisations should recognise and address any concerns or issues raised by stakeholders. This can be achieved through active listening, empathy, and problem-solving. It is important to acknowledge the validity of concerns and work with stakeholders to find solutions that meet their needs.

   (v) **Provide incentives:** Providing incentives, such as rewards, recognition, or promotions, can help to motivate stakeholders to embrace the change and support the internal audit. Incentives can also help to create a positive culture of change and reinforce the organisation's commitment to achieving its objectives.

   (vi) **Monitor and evaluate progress:** Organisations should monitor and evaluate the progress of the internal audit and the change process regularly. This can help to identify areas of success and areas for improvement and adjust the approach accordingly.

4. **Limited access to information:** Auditors require access to all relevant information to conduct a comprehensive internal audit. However, some business units may be reluctant to provide information, leading to gaps in the audit process.

   While performing internal audits, organisations frequently confront the problem of limited access to information. Limited access to information can arise due to a lack of data, insufficient system integration, or limited access to certain areas of the organisation. This challenge can compromise the quality and effectiveness of the audit process, leading to incomplete or inaccurate findings and recommendations. To conquer the issue of limited access to information in internal audits, organisations can take the following steps:

   (i) **Identify data sources:** Organisations should identify all possible data sources and determine which data is needed for the internal audit. This can include data from various systems, such as accounting systems, HR systems, and operational systems.

(ii) **Develop a data management plan:** Organisations should develop a data management plan that outlines how the data will be collected, stored, analysed, and shared. The plan should also include procedures for securing sensitive data and complying with regulatory requirements.

(iii) **Implement technology solutions:** Technology solutions, such as data analytics software and process automation tools, can help to streamline the data collection and analysis process. These solutions can also provide real-time insights into the organisation's operations, reducing the need for manual data collection.

(iv) **Establish data-sharing agreements:** Organisations should establish data-sharing agreements with relevant stakeholders, such as vendors, partners, and other organisations, to ensure access to necessary data. These agreements should include clear guidelines for data use, sharing, and security.

(v) **Develop a data governance framework:** Organisations should develop a data governance framework that defines the rules and processes for managing data throughout the organisation. The framework should include policies for data quality, security, privacy, and compliance.

(vi) **Train staff on data management:** Organisations should train their staff on data management practices, including data security, privacy, and quality. This can help to ensure that all employees are aware of their responsibilities and can contribute to the success of the internal audit.

5. **Complexity of operations:** Modern business operations are becoming increasingly complex, particularly in large and diversified organizations, which may make it difficult for internal auditors to understand the entire process or identify potential risks. It arises due to the multitude of processes, systems, and business units within an organisation, making it difficult to understand how they all fit together and how they impact the organisation's objectives. This can compromise the quality and effectiveness of the internal audit process, leading to incomplete or inaccurate findings and recommendations. To overcome this challenge in internal audits, organisations can take the following steps:

(i) **Conduct a process mapping exercise:** Organisations should conduct a process mapping exercise to identify all processes within the organisation and understand how they fit together. This can help to identify redundancies and inefficiencies and streamline processes to improve the effectiveness and efficiency of the organisation.

(ii) **Develop a risk assessment plan:** Organisations should develop a risk assessment plan that identifies potential risks associated with each process, system, and business unit. This can help prioritise the areas requiring the most attention and resources during the internal audit process.

(iii) **Establish clear objectives and criteria:** Organisations should establish clear objectives and criteria for the internal audit process. This can help to ensure that the audit team focuses on the areas that are most critical to the organisation's success and measures the effectiveness of the processes against the established criteria.

(iv) **Use data analytics and automation:** Data analytics and automation tools can help to streamline the internal audit process, reducing the time and effort required to analyze complex data sets. These tools can also provide real-time insights into the organisation's operations, enabling the audit team to identify patterns and trends quickly.

(v) **Involve relevant stakeholders:** Organisations should involve relevant stakeholders, such as process owners, system administrators, and business unit leaders, in the internal audit process. This can help to ensure that the audit team has access to the necessary information and can obtain an exhaustive understanding of the organisation's operations.

(vi) **Develop a comprehensive report:** Organisations should develop a comprehensive report summarising the findings and recommendations of the internal audit. The report should be clear and concise, highlighting areas of concern and providing actionable recommendations to address them.

6. **Inadequate communication:** Effective communication is critical for a successful internal audit. However, poor communication can lead to misunderstandings or misinterpretations of audit findings, ultimately undermining the effectiveness of the audit process.

   Inadequate communication can be a significant challenge for organisations conducting internal audits, particularly when different stakeholders have different levels of understanding about the audit process, objectives, and outcomes. Inadequate communication can result in misunderstandings, conflicts, and, ultimately, a lack of trust in the audit process. Organisations can take the following steps to overcome the challenge of inadequate communication in internal audits:

   (i) **Develop a communication plan:** Organisations should develop a communication plan outlining the key messages, audience, and communication channels throughout the audit process. The plan should also identify the stakeholders who need to be kept informed and how frequently they need to be updated.

   (ii) **Establish clear lines of communication:** Organisations should establish clear lines of communication with stakeholders throughout the audit process. This can include regular check-ins, progress reports, and feedback sessions.

   (iii) **Use clear and concise language:** Organisations should use clear and concise language in all communications related to the audit process. This ensures all stakeholders understand the audit process, objectives, and outcomes.

   (iv) **Address stakeholders' concerns:** Organisations should address stakeholders' concerns and questions throughout the audit process. This helps building trust and ensure stakeholders are engaged and invested in the process.

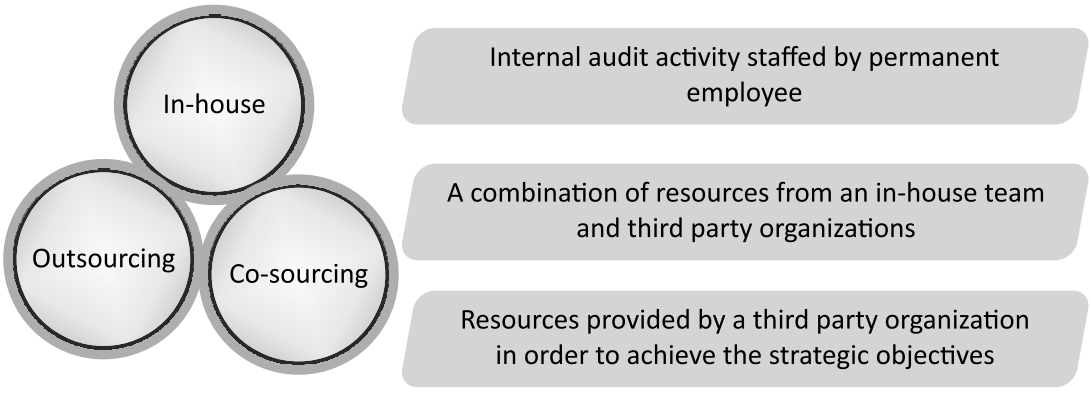
   (v) **Use visual aids:** Visual aids, such as graphs, charts, and diagrams, can help to communicate complex information in a more accessible way. This can help stakeholders to better understand the audit process and outcomes.

   (vi) **Foster an open and collaborative culture:** Organisations should foster an open and collaborative culture that encourages feedback and input from all stakeholders. This ensures that all perspectives are considered in the audit process, and that stakeholders feel valued and invested in the outcome.

IN-HOUSE VS. OUTSOURCING AUDIT ASSIGNMENTS

Internal audit assignments can be conducted either in-house or outsourced to external service providers. Both options have their own advantages and disadvantages, and the decision of whether to use in-house or outsourcing can vary depending on various factors, such as the size and complexity of the organisation, the availability of internal resources, and the cost and quality of external service providers.

Co-sourcing of audit assignments is an approach where an organisation combines in-house resources with external service providers to conduct internal audits. Co-sourcing can provide organisations with the benefits of both in-house and outsourcing options and can be a more flexible and cost-effective approach to internal auditing.



Pic 1: In-house vs. Outsourcing vs. Co-sourcing Internal Audit Assignments

In-house Function

Whether the organization choose to have internal audit as in-house function or otherwise, every choice has a pros and cons. Let's discuss the pros and cons of each option one by one:

Pros	*Cons*
✓ Continuity of Staff ✓ Certain controllable cost ✓ Full control of function ✓ A resource pool for the business ✓ Training ground for employees ✓ Greater cultural alignment ✓ Insiders	× May not be fully employed effectively and efficiently × Difficult to acquire necessary /maintain all skills and experience to meet the risk profile of the business × Need to continually invest in training and development × Recruitment hassles × Ineffective/inefficient start-up × Retention and development strategies required × Reduces opportunities to provide fresh perspective/risk of complacency or familiarity

Every industry is peculiar in nature, it has different ways of functioning and has different nuances. For example, in a pharmaceutical company, you need people that can understand research, manufacturing, design and selling. You need people that understand the underlying business and its risks, and also you need people who are experts in risk, risk management controls and processes.

Organisations can conduct internal audits themselves, but only when the auditor has the qualifications, competency and independence from the management structure to act with objectivity.

In an ideal situation, the organisation might employ someone with an accounting or other business degree; his or her skill set and professional demeanour might dovetail with those required to conduct comprehensive, independent internal audits. Alternatively, an employee may have sufficient cumulative industry experience, background and training to conduct internal audits. The knowledge an in-house internal auditor can acquire about the workings of the organisation can be a great benefit, and if he or she has longevity with the organisation, the historical perspective can be invaluable.

For example, Indian Oil Corporation Limited (IOCL) has a dedicated internal audit department that conducts audits across its various business units, including refining, marketing, and petrochemicals. The internal audit team is responsible for identifying risks, reviewing internal controls, and recommending improvements.

Outsourcing of Internal Audit Function

Should the organization perform internal audit function in-house or outsource it to a firm – which one is the better option? Either model can succeed or fail, but one will offer significant advantages depending on your needs and how you structure the function. Let's discuss the advantages and disadvantages of Outsourcing of the internal audit function:

Pros	*Cons*
✓ Established methodologies and benefits of refreshment based on experiences across different organisations ✓ Up-to-date skilled staff ✓ Ability to draw on a wide range of skills as and when required ✓ No time is taken up by managing service and resources ✓ Clearly defined service level and performance measures ✓ Easily established and quickly effective ✓ Credibility to third parties	× No permanent on-site resource to help other areas of the business × Potential cost impact × Possible lack of staff continuity × Remote from business developments, the culture and politics × Management time to establish and maintain relationships

Why outsourcing is a big risk?

Although outsourcing may seem attractive in theory, there are certain issues with internal capabilities that cannot be resolved, making it advantageous to keep internal audit in-house. The primary reason for outsourcing is to provide audit teams with access to a wide range of technical skills. However, many organizations have attempted to outsource engagements and failed to meet their objectives, prompting them to bring the work back in-house after just a few years.

Outsourcing and in-house approaches to IA each have their own advantages and challenges. Organizations with an in-house IA function are able to maintain complete control over their IA approach and have immediate knowledge of the issues at hand. However, since independence is a critical component of IA, careful consideration is required for the structure and reporting line of an in-house IA function.

Fully outsourcing of internal audit function can provide access to valuable expertise, cost flexibility, and an independent viewpoint that employees may not possess. It can also provide third-party assurance, as well as fresh industry or global perspectives. However, there may be a lack of internal knowledge, or it may take longer to grasp processes.

For example, Tata Steel recently outsourced its internal audit function to Ernst & Young in an effort to improve the efficiency and effectiveness of its internal audit processes. The external service provider is responsible for conducting internal audits across Tata Steel's various business units, including steel production, marketing, and sales.

Co-Sourcing of Audit Assignment

Co-sourcing of audit assignments is an approach where an organization combines in-house resources with external service providers to conduct internal audits. Co-sourcing can provide organizations with the benefits of both in-house and outsourcing options and can be a more flexible and cost-effective approach to internal auditing. Let's understand the advantages and disadvantages of the co-sourcing:

Pros	*Cons*
✓ Long-term permanent onsite presence through Head of Internal Audit ✓ Access to broad range of skills through the partner ✓ Draw on specialist skills as and when, and only when, needed ✓ Continuity through Head of Internal Audit ✓ Pull in up-to-date skills and experience as needed ✓ Quick to implement skills transfer to in-house team ✓ Flexible approach, clearly defined service level and KPI measures ✓ Credibility to third parties ✓ No or reduced training cost	× Time taken to recruit Head of Internal Audit × Possible cost impact × Management resource needed in recruitment and relationship development × Dependency of third part × Possible lack of staff continuity × Other challenges for in-house resources as discussed earlier

Co-sourcing can be particularly beneficial if the organisation has a continued relationship with the external IA supplier, so they can grow to understand the business. Co-sourcing can enable an organisation to top up skill sets, fill staff shortages, or perform work in various locations. An organisation could gain access to innovation in tools, audit techniques, thought leadership and benchmarking.

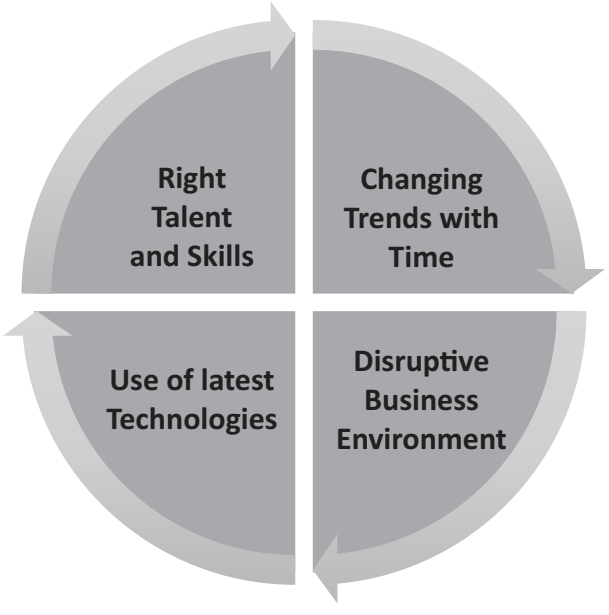
To successfully co-source audit assignments, it is important for the organization to establish clear communication channels, expectations, and roles and responsibilities for both in-house staff and external service providers. The organization should also have a clear understanding of the external service provider's qualifications, experience, and approach to auditing and should work with the provider to ensure that the audit process aligns with the organization's objectives and culture.

The challenges with co-sourcing can include the potential for confusion about responsibility and accountability and a lack of cultural fit if the external provider isn't aligned. Whatever combination of IA is settled upon, it must be judged according to whether it satisfies the expectations of stakeholders. It must demonstrate an awareness of the processes of the business and the risks it faces.

For example, the Indian Railway Catering and Tourism Corporation (IRCTC) recently implemented a co-sourcing model for its internal audit function, working with both in-house and external auditors to ensure that its audit function is aligned with its strategic objectives. The co-sourcing model allows IRCTC to access specialized expertise and gain external perspectives while maintaining control over the audit process.

The choice of in-house, outsourcing, or co-sourcing for internal audit assignments in India depends on the organization's size, complexity, and resources, as well as the availability of external service providers with the necessary expertise and experience. Each choice has its own advantages and disadvantages, and organizations should carefully consider their specific needs and objectives before making a decision.

EMERGING ISSUES



1. Changing Trends with Time

The field of internal audit is constantly evolving, and changing trends and times have a significant impact on how internal audits are conducted in the future. Here are some ways in which changing trends and times are likely to impact internal audit in the times to come:

(i) **Increased use of data analytics:** With the increasing amount of data being generated by organizations, internal auditors are expected to use data analytics tools to analyze and interpret data. This will require auditors to have a solid understanding of data analytics and data visualization tools and use them to provide insights and recommendations to management.

(ii) **Focus on risk management:** Internal auditors will be expected to focus more on risk management, including identifying and assessing risks, developing risk management strategies, and monitoring risk mitigation efforts. This will require auditors to have a deep understanding of the business and its risk profile.

(iii) **Emphasis on soft skills:** Internal auditors will be expected to have strong communication, critical thinking, and problem-solving skills. These skills will be crucial in effectively communicating audit findings to management and in collaborating with other departments and stakeholders.

(iv) **Impact of technology:** Technology is constantly changing, and internal auditors will be expected to keep up with the latest developments. This will require auditors to have an understanding of emerging technologies such as blockchain, artificial intelligence, and cybersecurity.

(v) **Increased focus on sustainability:** There is growing pressure on organizations to be more sustainable, and this will impact how internal audits are conducted. Auditors will be expected to assess the organization's sustainability practices and provide recommendations for improvement.

(vi) **Remote working:** With the pandemic, many organizations have shifted to remote working. This has created new challenges for internal auditors, who will need to adapt to conducting audits remotely, including using technology to conduct interviews, review documents, and communicate findings.

In summary, changing trends and times will continue to impact the field of internal audit in the times to come. Internal auditors will need to stay up-to-date with the latest trends and developments and be prepared to adapt their approach to effectively meet the changing needs of their organizations.

2. Disruptive Business Environment

Disruptive business environments can become an emerging issue in internal audit because they often create new risks and challenges for organizations that need to be addressed. These environments can be caused by a variety of factors, including technological innovations, changes in market conditions, regulatory changes, and other external factors.

As organizations adapt to these disruptive environments, they may need to change their business models, adopt new technologies, and revise their processes and procedures. This can create new risks, such as cybersecurity threats, compliance issues, and operational challenges. Internal auditors need to be aware of these risks and challenges and be prepared to assess and manage them.

In addition, disruptive environments can also create new opportunities for organizations, such as entering new markets or developing new products and services. Internal auditors need to be able to identify and evaluate these opportunities to ensure that they are pursued in a way that is consistent with the organization's strategy and objectives.

Overall, internal auditors need to be flexible, innovative, and adaptive in order to effectively address the risks and opportunities created by disruptive business environments. They need to have a deep understanding of the organization's operations and strategy, as well as the external factors that are driving change in the business environment. By doing so, they can provide valuable insights and assurance to the organization's stakeholders, including management, the board of directors, and external auditors.

A real-life example of a disruptive business environment that has become an emerging issue in internal audit is the rise of digital transformation. With the increased adoption of technology and the growth of digital platforms, many organizations are facing new risks and challenges related to cybersecurity, data privacy, and regulatory compliance.

For example, financial institutions are now required to comply with new regulations related to cybersecurity and data privacy, such as the General Data Protection Regulation (GDPR) in the European Union. These regulations require organizations to implement robust cybersecurity and data protection measures to safeguard customer information, which can be a significant challenge for organizations that are still using outdated technology or have limited resources for cybersecurity.

As a result, internal auditors in financial institutions need to be well-versed in the latest cybersecurity and data protection best practices and have the ability to assess and manage the risks associated with digital transformation. They may need to develop new audit procedures, such as reviewing the effectiveness of security controls for cloud-based systems or assessing the organization's ability to detect and respond to cyber threats in real-time.

In addition, the rise of digital platforms has also created new opportunities for financial institutions to innovate and create new products and services, such as mobile banking and online investment platforms. Internal auditors need to be able to identify and evaluate these opportunities and ensure that they are pursued in a way that is consistent with the organization's strategy and objectives.

3. Use of latest technologies

The use of latest technologies in systems in organizations is an emerging issue in internal audit, as it presents new risks and challenges that internal audit must address. Here are some areas that internal audit should focus on when auditing the use of latest technologies in systems:

(i) **Security and Privacy:** With the use of latest technologies, there is an increased risk of cyber threats and data breaches. Internal audit should ensure that the systems are secure and that appropriate measures are in place to protect sensitive data. This includes an assessment of the security protocols, encryption, access controls, and other security measures.

(ii) **Governance and Management:** Internal audit should review the governance structure in place to ensure that there are adequate controls and oversight of the technology initiatives. This should include an assessment of the roles and responsibilities of key stakeholders, including the board, senior management, and the IT team. Additionally, internal audit should review the policies and procedures in place to ensure that they are adequate and up to date.

(iii) **System Development Life Cycle:** Internal audit should ensure that appropriate controls are in place throughout the system development life cycle, from design to implementation to maintenance. This includes an assessment of the testing and validation procedures, as well as the change management process.

(iv) **Business Continuity and Disaster Recovery:** Internal audit should ensure that appropriate measures are in place to ensure business continuity in the event of a system outage or disaster. This includes an assessment of the backup and recovery procedures, as well as the disaster recovery plan.

(v) **Compliance:** Internal audit should ensure that the use of latest technologies is compliant with applicable laws and regulations. This includes an assessment of the data protection laws, industry-specific regulations, and other compliance requirements.

In summary, internal audit should focus on security and privacy, governance and management, system development life cycle, business continuity and disaster recovery, and compliance when auditing the use of latest technologies in systems. By doing so, internal audit can help to ensure that the risks associated with the use of these technologies are effectively managed and that the organization is able to leverage the benefits of these emerging technologies.

Sure, here's a real-life case study from India on the use of latest technologies in systems and the associated risks that internal audit must address.

In recent years, many Indian organizations have started using biometric authentication technology for employee attendance tracking and access control. Biometric authentication involves the use of unique biological characteristics, such as fingerprints or facial recognition, to verify the identity of an individual.

While biometric authentication can provide organizations with many benefits, such as increased accuracy, reduced fraud, and improved security, it also presents new risks that internal audit must address. Here are some examples:

Privacy: Biometric authentication involves the collection and processing of sensitive personal data, such as fingerprints or facial recognition data. Internal audit must ensure that appropriate privacy controls are in place, such as obtaining consent from employees, limiting access to the data, and encrypting the data to protect the privacy of personal data.

Security: Biometric authentication can be vulnerable to hacking, spoofing, or other attacks, which can compromise the security of the organization's systems and data. Internal audit must ensure that appropriate security controls are in place, such as implementing multi-factor authentication, using secure encryption algorithms, and conducting regular vulnerability assessments to protect the organization's systems and data.

Compliance: Biometric authentication is subject to data protection and privacy regulations, such as the Personal Data Protection Bill, 2019, and the Information Technology (Reasonable Security Practices and

Procedures and Sensitive Personal Data or Information) Rules, 2011. Internal audit must ensure that the organization's use of biometric authentication complies with these regulations and that appropriate controls are in place to protect the privacy of personal data.

For example, a leading Indian IT services company implemented a biometric authentication system for employee attendance tracking and access control at its offices. The system was based on facial recognition technology, which involved capturing and storing images of employees' faces for authentication purposes.

To address the risks associated with biometric authentication, the company's internal audit team conducted a review of the system, including an assessment of the privacy, security, and compliance controls. The audit team identified several areas for improvement, such as enhancing the security controls, improving the data retention policies, and conducting regular privacy impact assessments.

Based on the audit findings, the company implemented several changes to the biometric authentication system, such as using better encryption algorithms, limiting the retention of facial recognition data, and obtaining employee consent for the use of biometric authentication. These changes helped the company to manage the risks associated with biometric authentication and to ensure compliance with data protection regulations.

4. Right Talent and Skills

The rapid pace of technological advancement and constantly evolving business models and processes have led to an increased demand for specialised skills in various fields. This is particularly true for the internal audit function, which must keep up with changing trends and technologies in order to effectively identify and mitigate risks within an organisation.

The right talent with the appropriate skills and knowledge is critical for internal audit to be effective in the current business environment. For example, as companies adopt new technologies such as artificial intelligence, the internal audit function must have the skills and expertise to evaluate the effectiveness of these tools and their impact on the organization's risk profile.

Additionally, the increasing importance of data analytics in internal audit means that the function requires talent with skills in data science, statistical analysis, and visualization. Internal auditors must also have a strong understanding of cybersecurity and be able to identify and mitigate potential security risks.

The emerging issue in conducting internal audit is the challenge of finding and retaining talent with the necessary skills and expertise to meet the changing demands of the function. As companies compete for talent in these specialized fields, it can be difficult for internal audit functions to attract and retain top talent.

To address this challenge, organizations may need to invest in training and development programs to help internal auditors acquire the necessary skills and expertise. They may also need to consider alternative talent models, such as partnering with external service providers or leveraging the gig economy to tap into specialized talent on an as-needed basis.

Example: Let's say that a manufacturing company is implementing a new robotic process automation (RPA) system to automate certain tasks in their production line. As part of the implementation process, the internal audit function is tasked with evaluating the effectiveness of the RPA system and identifying any potential risks associated with its use.

To conduct this evaluation, the internal audit team needs to have talent with knowledge and skills in RPA technology, as well as an understanding of the manufacturing processes and associated risks. The team may also need to have experience in evaluating the effectiveness of similar technology systems in other companies.

If the internal audit function does not have the necessary talent with the required skills and expertise, they may struggle to effectively evaluate the RPA system and identify any risks. This could result in the company unknowingly exposing itself to potential risks associated with the use of the technology.

On the other hand, if the internal audit function has the right talent with the appropriate skills, they can provide valuable insights and recommendations to help the company effectively manage risks associated with the RPA system. This highlights the importance of having the right talent with changing pace and trends in internal audit to ensure the function can effectively identify and mitigate risks.

In recent years, the financial services industry has seen a rapid transformation driven by digital disruption and regulatory changes. This has led to a growing demand for specialized skills in areas such as cybersecurity, data analytics, and emerging technologies like blockchain and artificial intelligence.

To keep up with these changes and effectively manage risks, internal audit functions in financial services organizations have had to adapt and evolve. For example, they are increasingly leveraging data analytics to identify potential fraud and other risks, as well as using artificial intelligence to enhance the efficiency and effectiveness of audits.

However, finding and retaining talent with the necessary skills and expertise can be a challenge for these organizations. This is especially true as competition for talent in these areas is high, with technology companies and other industries also competing for these specialized skills.

One way that financial services organizations are addressing this challenge is by investing in training and development programs to upskill their existing staff. They are also exploring alternative talent models, such as partnering with external service providers or leveraging the gig economy to access specialized talent on an as-needed basis.

Overall, this example highlights how talent with changing pace and trends is impacting the internal audit function in financial services organizations, and the need for these organizations to be proactive in addressing this challenge in order to effectively manage risks and ensure compliance with regulatory requirements.

EMERGING AREAS GETTING INTO FOCUS IN INTERNAL AUDIT

Internal audit is a constantly evolving field, with new areas of focus emerging as organisations and industries change. Some emerging areas getting into focus in internal audit include:

1. **Cybersecurity:** With the increasing reliance on technology and the rise of cyber threats, internal auditors are increasingly being called upon to assess and monitor the effectiveness of an organization's cybersecurity measures.

Example 1:

Let's discuss the case of Bank of Baroda, where internal audit played a significant role in cyber security is the 2016 cyber attack. In this incident, hackers managed to steal approximately $13.5 million from the bank by hacking into the bank's SWIFT messaging system.

Following the incident, the bank's internal audit function conducted a comprehensive review of the bank's cyber security policies and procedures. The review identified several weaknesses in the bank's cyber security controls, including a lack of employee awareness and training on cyber security, inadequate incident response procedures, and outdated software systems.

The internal audit team made several recommendations to improve the bank's cyber security posture. These included increasing employee awareness and training on cyber security, implementing stronger access controls, and upgrading the bank's software systems.

The bank implemented these recommendations and took several additional steps to improve its cyber security. These included hiring a chief information security officer, establishing a dedicated cyber security operations center, and implementing a robust incident response plan.

As a result of these measures, the Bank of Baroda was able to strengthen its cyber security posture and prevent further cyber attacks. The incident highlights the critical role of internal audit in identifying and mitigating cyber security risks and the importance of continuous improvement in cyber security policies and procedures.

Example 2:

Another example where internal audit played a significant role in cyber security is the 2020 cyber-attack on Dr. Reddy's Laboratories, one of India's largest pharmaceutical companies.

In October 2020, Dr. Reddy's Laboratories was hit by a cyber attack that impacted its global operations. The attack disrupted the company's manufacturing, research, and development operations, and led to a temporary shutdown of some of its plants.

The company's internal audit function played a critical role in responding to the attack and mitigating its impact. The internal audit team worked closely with the company's IT department to assess the scope and severity of the attack, identify vulnerabilities in the company's cyber security controls, and develop a plan to mitigate the impact of the attack.

The internal audit team identified that the cyber attackers used a phishing email to gain access to the company's systems. They also found that the company's network segmentation was inadequate, which allowed the attackers to move laterally across the company's network and infect multiple systems.

The internal audit team made several recommendations to improve the company's cyber security posture, including the implementation of multi-factor authentication for all employees, improving network segmentation, and increasing employee awareness and training on cyber security risks.

The company implemented these recommendations and took several additional steps to strengthen its cyber security posture. These included increasing its investment in cyber security technologies and tools, hiring additional cyber security personnel, and conducting regular vulnerability assessments and penetration testing.

As a result of these measures, Dr. Reddy's Laboratories was able to recover from the cyber attack and resume its operations. The incident highlights the critical role of internal audit in identifying and mitigating cyber security risks, and the importance of continuous improvement in cyber security policies and procedures to protect against cyber threats.

2. **ESG (Environmental, Social, and Governance):** As environmental, social, and Governance risks are becoming a major concern for organisations, internal auditors are being asked to assess the company's performance in these areas and help to identify potential risks.

Example:

Tata Group is one of the example of ESG from an internal audit perspective. The Tata Group is a multinational conglomerate based in India with interests in various industries including steel, automobiles, and information technology.

The Tata Group has been committed to sustainability and ESG for several years and has made significant efforts to integrate ESG considerations into its business operations. In 2014, the company established a dedicated sustainability department to oversee and manage its ESG initiatives.

To ensure that its ESG efforts are aligned with its business strategy and goals, the Tata Group conducts regular internal audits of its sustainability practices. The internal audit team evaluates the company's ESG performance against various parameters, including resource efficiency, climate change, and social responsibility.

The internal audit team also conducts periodic assessments of the company's supply chain to identify potential ESG risks and opportunities. For example, the team assesses supplier's compliance with the company's code of conduct, which includes requirements related to labor standards, human rights, and environmental stewardship.

The internal audit team at Tata Group also works closely with other departments to identify and address ESG-related issues. For example, the team collaborates with the legal department to ensure compliance with applicable environmental and social regulations.

Through its ESG efforts, Tata Group has been able to improve its environmental performance and social impact, while also creating long-term value for its stakeholders. The company has been recognized for its sustainability leadership, including being ranked as the top Indian company in the Dow Jones Sustainability Index for several years in a row.

3. **Artificial Intelligence (AI):** The use of AI is increasing in various aspects of organisations, and internal auditors are being asked to assess the effectiveness of the controls put in place to manage the risks associated with AI.

Example:

One notable case study on the use of artificial intelligence in internal audit comes from Wipro Limited, a multinational IT services company headquartered in Bangalore.

Wipro Limited implemented an AI-based platform called Holmes, which is designed to help internal audit teams improve their efficiency and effectiveness. The platform uses machine learning algorithms to analyze large volumes of data from various sources, such as financial statements, invoices, and customer feedback.

Holmes can perform a variety of tasks, such as identifying patterns and anomalies in data, detecting potential fraud and errors, and generating reports with insights and recommendations. The platform can also learn from past audits to improve its accuracy and effectiveness over time.

Wipro Limited has reported significant benefits from using Holmes in its internal audit process. For example, the company has been able to reduce the time and effort required for audits by up to 30%, while also increasing the coverage and accuracy of its audits. The platform has also helped the company identify and mitigate potential risks more effectively, which has contributed to better overall business outcomes.

4. **Regulatory and Risk compliance:** With constantly evolving regulatory landscape, internal auditors are required to stay up-to-date with changes in regulations and help ensure that the organisation complies with them.

CASE STUDY

Volkswagen's Emissions Scandal

In 2015, the German automaker Volkswagen (VW) was found to have installed software in its diesel cars that could cheat emissions tests. The software, known as a "defeat device," was designed to detect when the car was being tested for emissions and to reduce the emissions to comply with regulations. However, in real-world driving, the cars emitted up to 40 times the legal limit of nitrogen oxide (NOx) emissions.

The scandal was a result of the company's non-compliance with emissions regulations, which led to serious legal, financial, and reputational consequences. VW was forced to recall millions of cars and pay billions of dollars in fines, settlements, and compensation to customers. The company also faced criminal charges and had to make significant changes to its corporate culture and Governance.

The scandal also had a ripple effect on the automotive industry as a whole, leading to increased scrutiny of emissions testing and regulatory compliance. It also raised questions about the role of regulators and their ability to detect and prevent similar violations in the future.

The VW scandal demonstrates the importance of regulatory and compliance risks in the automotive industry and beyond. Companies must ensure that their products and practices comply with regulations and standards, and they must be transparent and accountable to regulators and customers. Failure to do so can result in serious legal, financial, and reputational consequences, as well as harm to public health and the environment.

CASE STUDY

PNB's Fraudulent Transactions

In 2018, Punjab National Bank (PNB), one of the largest public sector banks in India, discovered a fraudulent transaction of approximately Rs. 14,000 crore ($1.8 billion) at its Brady House branch in Mumbai. The fraud involved the bank's employees colluding with companies owned by Nirav Modi, a billionaire jeweler, to obtain unauthorised loans and letters of credit.

The fraud was a result of the bank's non-compliance with banking regulations and internal controls, which allowed the employees to bypass the bank's systems and processes. The employees were able to issue unauthorised letters of credit to Modi's companies without collateral or guarantees, and the transactions went undetected for several years.

The fraud had serious legal, financial, and reputational consequences for the bank and its stakeholders. PNB's stock price and credit ratings fell, and the bank had to make provisions for the fraudulent transactions, which led to a significant loss. The fraud also raised questions about the effectiveness of the bank's internal controls and the role of regulators in detecting and preventing such frauds.

The PNB fraud highlights the importance of regulatory and compliance risks in the banking industry in India. Banks must comply with the regulatory requirements and ensure the effectiveness of their internal controls to prevent frauds and other financial crimes. The fraud also underscores the need for transparency and accountability in the banking sector and the importance of the role of regulators in enforcing regulations and protecting the interests of stakeholders.

5. **Supply chain risks:** The COVID-19 pandemic has highlighted the risks associated with global supply chains. Internal auditors are being asked to assess the organization's supply chain risks and help identify potential vulnerabilities.

Example 1:

A very good example on supply chain risk from an internal audit perspective is the 2019 Indian Auto Parts Manufacturer (APM) crisis. The APM company was a major supplier of auto parts to various automobile manufacturers, including some of the biggest names in the industry.

The crisis began when the company faced financial difficulties due to a severe cash crunch, which was caused by a combination of factors, including high debt levels, poor financial management, and delays in payments from customers. As a result, the company was unable to pay its suppliers for the raw materials required to manufacture auto parts.

This led to a cascading effect on the supply chain, with the company unable to meet its delivery commitments to its customers. The automobile manufacturers, in turn, faced production delays, which impacted their ability to meet their own delivery commitments to their customers. This led to a ripple effect on the entire supply chain, causing significant disruptions and losses for all parties involved.

This crisis highlighted the importance of assessing supply chain risks and ensuring the implementation of robust risk management processes. A key lesson learned from this crisis was the need for better financial management and transparency in the supply chain, including a focus on timely payment of suppliers and effective cash flow management.

The crisis also demonstrated the need for greater collaboration and communication across the supply chain, including regular monitoring of supplier performance and contingency planning to mitigate potential disruptions. This highlights the importance of regular internal audits and risk assessments to identify potential areas of weakness in the supply chain and to implement effective controls and contingency plans to minimize the impact of any potential disruptions.

Example 2:

Another example on supply chain risk is the 2020 COVID-19 pandemic and its impact on the pharmaceutical industry in India. The pandemic had a significant impact on the global supply chain, with disruptions in the transportation of goods, delays in customs clearance, and reduced availability of raw materials. These disruptions had a direct impact on the pharmaceutical industry, which relies heavily on imports of raw materials and intermediate products from China and other countries.

This crisis highlighted the importance of assessing and managing supply chain risks, including the need for contingency planning to address potential disruptions. The crisis also emphasised the need for greater collaboration and communication across the supply chain to mitigate the impact of any potential disruptions.

The pharmaceutical industry in India responded by implementing a range of measures to mitigate the impact of the pandemic on the supply chain, including increasing the inventory of critical raw materials, diversifying suppliers, and building strategic partnerships with local manufacturers. These measures helped to mitigate the impact of the pandemic on the pharmaceutical industry in India, ensuring the continuity of critical supplies and medicines.

The crisis also underscored the need for regular internal audits and risk assessments to identify potential areas of weakness in the supply chain and to implement effective controls and contingency plans to minimize the impact of any potential disruptions. In addition, it highlighted the importance of monitoring supplier performance, identifying potential risks, and building stronger partnerships with key suppliers to ensure the continuity of critical supplies.

6. **Data privacy:** As organisations collect more and more data, internal auditors are being asked to assess the effectiveness of the organization's data privacy controls and help identify potential risks.

Example:

The 2018 Cambridge Analytica scandal involving Facebook is a very good example of data privacy concerns. Cambridge Analytica was a political consulting firm that used data from millions of Facebook users without their consent to create targeted political ads and influence the 2016 US presidential election.

The scandal came to light after a whistleblower, Christopher Wylie, revealed that Cambridge Analytica had obtained data from an app developed by researcher Aleksandr Kogan. The app, called "This Is Your Digital Life," was a personality quiz that collected data on not only the users who took the quiz but also their friends on Facebook.

While Facebook's policies at the time allowed third-party developers to collect user data, they were not allowed to share that data without explicit user consent. It was later revealed that Cambridge Analytica had obtained data from 87 million Facebook users, most of whom had not given their consent for their data to be shared.

The scandal sparked widespread outrage and calls for greater data privacy protections. In response, Facebook made several changes to its policies and platform, including limiting third-party access to user data and implementing more stringent privacy controls.

The Cambridge Analytica scandal serves as a cautionary tale about the importance of protecting personal data and the potential consequences of failing to do so. It highlights the need for greater transparency and accountability in how companies collect, store, and use personal data, as well as the importance of giving users control over their own data.

CASE STUDY

Whatsapp

Another recent example of a data privacy concern is the 2021 WhatsApp privacy policy update controversy. WhatsApp is a popular messaging app used by millions of people in India and around the world. In January 2021, the company announced an updated privacy policy that would allow it to share certain user data with its parent company, Facebook.

The announcement sparked concerns among Indian users and led to widespread backlash, with many people expressing concerns about the potential misuse of their data. Some users began to migrate to alternative messaging apps such as Signal and Telegram, which have stricter privacy policies and do not share user data with third parties.

The Indian government also became involved in the controversy, with the Ministry of Electronics and Information Technology issuing a notice to WhatsApp asking the company to withdraw the updated privacy policy. The government expressed concerns that the policy violated the privacy of Indian users and was not in compliance with Indian laws.

WhatsApp initially defended the policy, claiming that it did not compromise the privacy of users and that the company was committed to protecting user data. However, in response to the backlash and government pressure, WhatsApp delayed the implementation of the policy and began a campaign to educate users about its privacy practices.

The WhatsApp privacy policy update controversy highlights the importance of transparency and user control in data privacy. It also underscores the need for companies to comply with local laws and regulations and to take the concerns of their users seriously. The incident has spurred discussions about data privacy in India and the need for stronger privacy protections for Indian users.

7. **Fraud prevention:** Fraud prevention is an important aspect of any organisation's risk management framework. Internal audit can play a crucial role in fraud prevention by identifying and assessing the risks of fraud, evaluating the effectiveness of existing controls, and recommending improvements to prevent and detect fraud.

   The internal audit team of the Indian subsidiary received an anonymous tip-off that an employee was colluding with a vendor to submit inflated invoices for goods and services that were never actually provided. The employee was working in the finance department and was responsible for processing vendor invoices and making payments to vendors.

   The internal audit team decided to investigate the tip-off and found that the employee had indeed colluded with the vendor to submit inflated invoices. The employee had created fictitious purchase orders and approved the invoices for payment without verifying the goods and services had been received. The vendor would then transfer a portion of the payments back to the employee as kickbacks.

Here's how the internal audit team helped to prevent the fraud from occurring:

- **Identifying Weaknesses in Controls:** The internal audit team found that there were several weaknesses in the control environment around the vendor invoice process, which had allowed the employee to collude with the vendor.
- **Recommending Controls Improvements:** The internal audit team recommended several control improvements to strengthen the vendor invoice process and prevent fraud in the future. The recommendations included segregation of duties, more stringent vendor onboarding procedures, and more rigorous verification of vendor invoices.
- **Preventing Further Losses:** The internal audit team's timely intervention and recommendations helped the company to prevent further losses and take corrective action against the employee and the vendor. The employee was terminated, and the vendor was blacklisted.

In short, the internal audit team's proactive approach and diligent investigation helped to prevent fraud from occurring by identifying weaknesses in controls and recommending improvements to prevent similar frauds in the future. This highlights the importance of internal audit's role in fraud prevention, not just detection, and the need for organizations to take a proactive approach to managing fraud risks.

8. **Social media:** Social media is a powerful tool for organisations, but it also presents new risks, such as reputational damage and cybersecurity threats. Internal auditors are being asked to assess the organization's social media strategy and help identify potential risks associated with social media use.

   Social media has had a significant impact on organizations, and internal auditors play a crucial role in assessing and managing the associated risks. Here are some perspectives on the impact of social media on organizations from an internal audit perspective:

   (i) **Reputational risk:** Social media has given organizations a powerful tool for communication and brand building. However, it has also exposed them to significant reputational risk. Negative comments, complaints, and criticism can spread rapidly and damage an organization's reputation. Internal auditors need to evaluate the organization's social media presence and ensure that appropriate controls and monitoring mechanisms are in place to manage this risk.

   (ii) **Information security risk:** Social media platforms collect and store a vast amount of personal and organizational information. This information can be used for cyber attacks, social engineering, and other security breaches. Internal auditors should evaluate the organization's social media policies and practices to ensure that information security risks are effectively managed.

   (iii) **Compliance risk:** Social media use is subject to numerous regulatory requirements, such as data privacy laws, advertising regulations, and social media guidelines. Internal auditors need to assess whether the organization's social media activities comply with these regulations and guidelines.

   (iv) **Employee productivity and conduct:** Social media can impact employee productivity and behavior. Internal auditors should evaluate the organization's policies and practices related to social media use by employees and ensure that they are consistent with the organization's values and culture.

   (v) **Business opportunities:** Social media can also provide new business opportunities, such as social media marketing and e-commerce. Internal auditors should evaluate the organization's social media strategy and assess the risks and benefits associated with social media use for business purposes.

By evaluating social media policies and practices and implementing appropriate controls, internal auditors can help organizations leverage the benefits of social media while minimizing the associated risks.

Example 1:

Aadhaar is a unique identification number issued by the Indian government, and it is linked to an individual's biometric and demographic data. In 2017, it was reported that the Aadhaar database had been breached, and personal data of millions of Indian citizens was leaked online.

This highlights the information security risks associated with social media use. The leaked data was reportedly being sold on social media platforms, raising concerns about how easily personal information could be accessed and misused. Internal auditors would have needed to evaluate the government's social media policies and practices to ensure that appropriate controls were in place to protect sensitive data.

This incident also underscores the compliance risk associated with social media use. Aadhaar is subject to numerous regulatory requirements, including data privacy laws and information security guidelines. Internal auditors would need to assess whether the government's social media activities related to Aadhaar were compliant with these regulations and guidelines.

In response to the incident, the Indian government took several measures, such as strengthening the security protocols for Aadhaar and establishing a dedicated authority for data protection. Internal auditors would also need to evaluate the effectiveness of these measures in managing the risks associated with social media use and information security.

Example 2:

In July 2020, it was reported that several high-profile Twitter accounts, including those of Barack Obama, Elon Musk, and Bill Gates, had been hacked, and a bitcoin scam was posted from these accounts.

This incident highlights the information security risks associated with social media use. The hackers reportedly gained access to Twitter's internal systems and tools, allowing them to take control of high-profile accounts and post the scam message. Internal auditors would have needed to evaluate Twitter's social media policies and practices to ensure that appropriate controls were in place to prevent unauthorized access to sensitive data and systems.

This incident also underscores the reputational risk associated with social media use. The hack received widespread media attention and caused significant damage to Twitter's reputation. Internal auditors would need to assess whether Twitter's incident response plan was adequate to manage the reputational risks associated with such incidents.

In response to the incident, Twitter made several changes to its security protocols and procedures, such as implementing two-factor authentication for all accounts and restricting access to internal tools. Internal auditors would also need to evaluate the effectiveness of these measures in managing the risks associated with social media use and information security.

9. **Culture audit:** Culture is an important factor in organisational success and can have a significant impact on risk management. Internal auditors are being asked to assess the culture of the organization and help identify potential cultural risks that may affect the organization's objectives.

   Organisational culture can have a significant impact on the effectiveness of an organization's Governance, risk management, and control processes. Here are a few ways in which internal auditors can evaluate and assess organizational culture:

   (i) **Conduct culture assessments:** Internal auditors can conduct culture assessments to gain insight into the organization's values, beliefs, and behaviors. This can involve conducting interviews, surveys, and focus groups with employees at all levels of the organization.

(ii) **Evaluate tone at the top:** Internal auditors can assess the tone at the top by evaluating the leadership's behavior and how it influences the organization's culture. Tone at the top can affect the behavior of employees, and therefore, has a significant impact on the effectiveness of risk management and control processes.

(iii) **Review policies and procedures:** Internal auditors can review policies and procedures to ensure that they are consistent with the organization's values and culture. Policies that are inconsistent with the organization's culture can lead to employees feeling disconnected from the organization's values and beliefs.

(iv) **Assess employee engagement:** Internal auditors can assess employee engagement to determine how engaged employees are with the organization's culture. Engaged employees are more likely to understand and follow the organization's values and beliefs, leading to a more effective risk management and control environment.

(v) **Evaluate training and communication:** Internal auditors can evaluate the organization's training and communication programs to determine how well they promote the organization's culture. Training and communication programs that are aligned with the organization's culture can help employees understand the importance of the organization's values and beliefs.

Example:

In 2018, the U.S. Olympic Committee (USOC) commissioned a culture audit in response to a sexual abuse scandal involving USA Gymnastics, one of its national governing bodies. The audit aimed to assess the organizational culture within the USOC and identify any systemic issues that may have contributed to the abuse scandal.

The culture audit involved conducting interviews with over 150 people, including current and former athletes, coaches, staff, and board members. The audit also included a review of policies and procedures, as well as an analysis of the organization's leadership and communication practices.

The audit identified several areas where the USOC's culture needed improvement, including:

- Lack of transparency: The audit found that there was a lack of transparency in the USOC's decision-making processes, which contributed to a lack of trust among athletes and other stakeholders.
- Inadequate communication: The audit found that there was a lack of clear and consistent communication within the USOC, which led to confusion and misunderstandings.
- Focus on winning at all costs: The audit found that the USOC's emphasis on winning medals sometimes overshadowed its commitment to athlete safety and well-being.

As a result of the audit, the USOC implemented several changes to its culture and Governance, including the establishment of an Athlete Ombudsman, increased funding for athlete safety and support programs, and the creation of a new Ethics and SafeSport Division.

This demonstrates how a culture audit can be a valuable tool for identifying and addressing systemic issues within an organisation. By assessing an organisation's culture, internal auditors can help to create a more ethical, transparent, and inclusive environment for all stakeholders.

10. **Audit of automated processes:** With the increasing use of automation in business processes, internal auditors are being asked to assess the effectiveness of controls put in place to manage the risks associated with automated processes. This includes assessing the effectiveness of automated controls and ensuring that they are properly designed and implemented.

CASE STUDY

Increased Automation in Internal Audit - The Role of Robotics Process Automation (RPA) in Hindustan Unilever Limited (HUL)

Hindustan Unilever Limited (HUL) is a subsidiary of Unilever, a multinational consumer goods company. HUL operates in India and is one of the largest fast-moving consumer goods companies in the country. The company has a robust internal audit process to ensure compliance with regulations, identify potential risks, and make recommendations for improvement. To enhance the effectiveness and efficiency of the internal audit process, HUL implemented Robotics Process Automation (RPA).

The internal audit team at HUL faced several challenges that made it difficult to achieve its objectives. First, the team was heavily reliant on manual processes, which made it difficult to analyse large volumes of data effectively. Second, the team was struggling to keep up with the ever-increasing regulatory requirements, which put a strain on their resources. Third, the team was struggling to identify and mitigate risks in a timely manner, which exposed the company to potential financial and reputational harm.

To address these challenges, HUL decided to implement RPA in the internal audit process. RPA is a software technology that automates repetitive and rule-based tasks that are typically performed by humans. The implementation of RPA has significantly enhanced the effectiveness and efficiency of the internal audit process at HUL.

The RPA system at HUL automates various aspects of the internal audit process, including risk assessment, testing, and reporting. The system uses data analytics and machine learning to identify potential risks and anomalies in large volumes of data, enabling the internal audit team to focus their efforts on the most critical areas of the business. The system also automates the testing process, making it easier for the internal audit team to conduct tests across multiple systems and processes. The automated testing process allows for more comprehensive testing, increasing the accuracy and reliability of the audit results. Finally, the system provides automated reporting, making it easier for the internal audit team to communicate the results of the audit to key stakeholders.

The implementation of RPA in the internal audit process has yielded several benefits for HUL. First, the system has enabled the internal audit team to identify potential risks and anomalies in a more timely and accurate manner, reducing the risk of financial and reputational harm to the company. Second, the automated system has increased the efficiency of the internal audit process, allowing the team to focus their efforts on more critical areas of the business. Finally, the automated reporting process has improved communication with stakeholders, making it easier to ensure that the recommendations of the internal audit team are implemented.

The implementation of RPA in the internal audit process has significantly enhanced the effectiveness and efficiency of the internal audit process at HUL. The use of RPA has enabled the internal audit team to identify potential risks and anomalies in a more timely and accurate manner, reducing the risk of financial and reputational harm to the company. The automated system has increased the efficiency of the internal audit process, allowing the team to focus their efforts on more critical areas of the business. The automated reporting process has improved communication with stakeholders, making it easier to ensure that the recommendations of the internal audit team are implemented. As organisations in India and around the world continue to face ever-increasing complexity and regulatory requirements, it is becoming increasingly important for internal audit teams to embrace automation and leverage the power of data analytics and machine learning to enhance their effectiveness and efficiency.

11. Legal & Company Secretarial

In recent years, legal and company secretarial functions have become increasingly important for internal auditors. This is due to several factors, including the growing complexity of business operations, the

proliferation of regulations and compliance requirements, and the need to ensure that companies are operating ethically and in accordance with their stated values.

Internal auditors are responsible for evaluating a company's internal controls and processes to ensure that they are operating effectively and efficiently. This includes assessing the company's compliance with legal and regulatory requirements, as well as its adherence to ethical standards.

The legal function is concerned with ensuring that a company is complying with all applicable laws and regulations. This includes everything from employment and labor laws to environmental regulations to data privacy and cybersecurity laws. Internal auditors need to be familiar with these regulations and assess whether the company is complying with them.

The company secretarial function is responsible for ensuring that a company is in compliance with its own internal policies and procedures. This includes maintaining accurate records of meetings, ensuring that all relevant documentation is properly filed and stored, and advising on issues related to corporate governance.

Internal auditors need to work closely with legal and company secretarial teams to assess the effectiveness of a company's internal controls and processes. This includes evaluating the company's risk management framework, assessing its internal controls over financial reporting, and evaluating the effectiveness of its compliance program.

In addition to working with legal and company secretarial teams, internal auditors also need to be familiar with emerging areas such as data privacy and cybersecurity. With the proliferation of data breaches and cyber attacks, companies need to ensure that they are protecting their customers' sensitive information and intellectual property.

Overall, the emergence of legal and company secretarial as key focus areas for internal auditors reflects the growing importance of risk management and compliance in today's business environment. By working closely with these teams, internal auditors can help companies stay on top of emerging risks and ensure that they are operating in a responsible and ethical manner.

12. Financial Crime

Financial crime is an emerging area that is increasingly getting into focus in internal audit. Financial crime refers to a broad range of illegal activities that are committed for financial gain, including fraud, money laundering, bribery, corruption, and terrorism financing. The impact of financial crime is significant, as it undermines the integrity of financial systems, damages the reputation of organizations, and poses a threat to national security.

Internal audit plays a crucial role in helping organizations prevent, detect, and investigate financial crime. Internal auditors can assist in identifying and assessing the risks associated with financial crime, evaluating the adequacy of controls, and providing recommendations for improving the effectiveness of the organization's anti-fraud and anti-money laundering measures.

In recent years, there has been an increased focus on financial crime within the regulatory environment, with regulators and governments taking a more proactive approach to combatting financial crime. This has resulted in a growing number of new regulations and guidelines that organizations must comply with, such as the Fifth Anti-Money Laundering Directive in Europe and the Bank Secrecy Act in the United States.

Internal auditors are expected to have a strong understanding of these regulations and guidelines, as well as the emerging trends and risks related to financial crime. This requires ongoing training and development to ensure that internal auditors have the necessary knowledge and skills to effectively identify and address financial crime risks within their organizations.

Financial crime is an emerging area that is getting into focus in internal audit. Internal auditors have an important role to play in helping organizations prevent, detect, and investigate financial crime. By staying up to date with the latest regulations, guidelines, and emerging trends, internal auditors can help their organizations protect themselves against financial crime risks and ensure their ongoing success.

Example 1:

One very prominent example of financial crime that has received significant attention in India in recent years is the Nirav Modi-PNB fraud case. In 2018, it was revealed that the well-known diamond merchant Nirav Modi had fraudulently obtained over $1.8 billion in loans from Punjab National Bank (PNB), one of the largest public sector banks in India.

Nirav Modi and his associates had allegedly obtained these loans by using fraudulent letters of undertaking (LoUs) issued by PNB employees. The LoUs were issued without proper documentation and without following the bank's internal controls and procedures. Modi and his associates then used these funds to finance their business and personal expenses, including the purchase of properties and luxury goods.

The fraud was eventually detected by PNB's internal audit team, which alerted the authorities. The case was then investigated by the Central Bureau of Investigation (CBI) and the Enforcement Directorate (ED), who uncovered a complex web of shell companies, bogus invoices, and other fraudulent transactions.

The Nirav Modi-PNB fraud case highlights the importance of strong internal controls and effective internal audit in preventing and detecting financial crime. It also underscores the need for ongoing training and development for internal auditors to keep up with emerging risks and trends related to financial crime. The case has led to increased scrutiny of banks and financial institutions in India, and has resulted in new regulations and guidelines aimed at improving the effectiveness of anti-fraud and anti-money laundering measures.

Example 2:

Another very famous case of financial crime in India is the Satyam Computer Services fraud case, also known as India's Enron scandal. In 2009, the founder and chairman of Satyam Computer Services, Ramalinga Raju, admitted to having committed financial fraud worth over $1 billion.

Raju had manipulated the company's financial statements by inflating revenues and profits, creating fake invoices, and forging bank statements. He had also misappropriated company funds for personal gain, including the purchase of properties and other assets.

The fraud was eventually uncovered by the company's internal auditors, who alerted the authorities. The case was investigated by the Central Bureau of Investigation (CBI) and the Serious Fraud Investigation Office (SFIO), leading to Raju's arrest and conviction.

The Satyam Computer Services fraud case had significant implications for the Indian corporate sector, as it led to a loss of investor confidence and raised concerns about the quality of corporate governance and internal controls in Indian companies. The case also highlighted the crucial role that internal audit plays in preventing and detecting financial fraud, and the need for ongoing training and development for internal auditors to keep up with emerging risks and trends.

The Satyam Computer Services fraud case resulted in the implementation of new regulations and guidelines aimed at improving the effectiveness of corporate governance and internal controls in India. The case also led to increased awareness of the importance of ethical business practices and transparency in financial reporting.

13. Third Party Risk Management

Third-party risk management is an emerging area of focus in internal audit, and it is gaining more attention due to the increasing reliance on third-party vendors by organizations. Many companies now outsource critical business functions to third-party vendors to reduce costs, increase efficiency, and gain access to specialized expertise. However, this outsourcing exposes organizations to new and evolving risks, such as data breaches, cyber attacks, financial fraud, regulatory non-compliance, and reputational damage.

Internal auditors are responsible for assessing and managing risks within their organizations, and third-party risk management is an area where they can add significant value. Internal audit can help to identify potential risks associated with third-party relationships, evaluate the effectiveness of controls, and make recommendations to management on how to mitigate risks.

In the context of third-party risk management, internal auditors can perform the following key activities:

(i) Assess the adequacy of the organization's third-party risk management program.

(ii) Evaluate the due diligence process for selecting and onboarding third-party vendors.

(iii) Review the contracts and service level agreements with third-party vendors to ensure compliance with regulatory requirements and internal policies.

(iv) Evaluate the effectiveness of monitoring and oversight activities, such as ongoing vendor assessments, audits and reporting.

(v) Analyze the organization's response plan to incidents involving third-party vendors, such as data breaches or disruptions in service.

By focusing on third-party risk management, internal auditors can help organisations ensure that they have the necessary controls in place to manage their relationships with third-party vendors effectively and protect their reputation and assets.

Example:

In early 2021, MobiKwik, one of India's leading mobile wallet and digital payment platforms, suffered a data breach that exposed the personal information of millions of its users. The breach was discovered by a security researcher, who found that MobiKwik's database was being sold on the dark web. The database contained personal information such as names, phone numbers, email addresses, dates of birth, and hashed passwords of millions of MobiKwik users.

The investigation into the data breach revealed that a third-party vendor of MobiKwik, a company called "GigIndia," was responsible for the breach. GigIndia was responsible for providing MobiKwik with a customer verification service, which involved collecting user data and verifying it against government-issued IDs. GigIndia had stored the user data in an unsecured Amazon Web Services (AWS) S3 bucket, which was easily accessible to anyone with the correct URL.

MobiKwik was found to have failed to properly vet and monitor the security practices of GigIndia, and had not ensured that the third-party vendor was in compliance with data protection laws and regulations. The company had also failed to take appropriate action after being notified of the vulnerability by the security researcher.

The data breach had a significant impact on MobiKwik's customers, leading to a loss of trust in the platform, and exposing them to potential fraud and identity theft. The incident also raised concerns among regulatory authorities, who launched an investigation into MobiKwik's data protection practices.

The case study highlights the importance of effective third-party risk management for companies, especially those that handle sensitive user data. Companies that engage with third-party vendors need to implement a robust risk management process that includes:

- **Adequate Due Diligence:** Companies need to conduct thorough due diligence on third-party vendors before engaging with them. This includes verifying their security controls and practices, and ensuring that they are in compliance with data protection laws and regulations.
- **Clear Contractual Provisions:** Contracts between companies and third-party vendors need to include clear provisions that outline specific security requirements and obligations, including data protection, breach notification, and liability.
- **Ongoing Monitoring:** Companies need to establish a process for monitoring third-party vendors regularly to ensure they comply with the contractual provisions, and to detect any potential vulnerabilities or breaches.
- **Effective Incident Response:** Companies need to have an effective incident response plan in place to respond to security breaches effectively, including notifying affected customers, regulators, and law enforcement, and taking appropriate action to mitigate the impact of the breach.

This case focuses and bring out the importance of implementing effective third-party risk management processes to minimise the risks associated with engaging with third-party vendors. Companies need to conduct thorough due diligence on vendors, ensure that contractual provisions are in place to manage risks, regularly monitor vendors, and have an effective incident response plan in place. By doing so, companies can protect themselves from the reputational and financial damage that can result from a breach of third-party vendors.

LESSON ROUND-UP

- Financial accounting is the process of recording, classifying, and summarising financial transactions to provide useful information in making business decisions. The three primary financial statements are the balance sheet, income statement, and cash flow statement. Financial accounting also includes preparing reports for taxation, regulatory compliance, and management decision-making.
- There are several risks associated with financial accounting, which can be broadly categorised into two main types:
    1. Financial risks; and
    2. Funding risks.
- **Financial risks** include the risk of errors or omissions in financial statements, the risk of fraud or misappropriation of assets, and the risk of non-compliance with laws and regulations.
- **Funding risks** include the risk that sufficient funds will not be available to meet obligations when they fall due, the risk of losing access to funding sources, and the risk of incurring additional costs in order to raise additional funds.
- Conducting an internal audit of business can be a challenging task, and some of the common **business-related challenges** that may arise during the process include:
    1. Conflict of Interest

2. Lack of Resources
3. Resistance to Change
4. Limited access to information
5. Complexity of operations
6. Inadequate communication

- Internal audit assignments can be conducted either **in-house or outsourced** to external service providers. Both options have their own advantages and disadvantages, and the decision of whether to use in-house or outsourcing can vary depending on various factors, such as the size and complexity of the organisation, the availability of internal resources, and the cost and quality of external service providers.
- **Co-sourcing** of audit assignments is an approach where an organisation combines in-house resources with external service providers to conduct internal audits. Co-sourcing can provide organisations with the benefits of both in-house and outsourcing options and can be a more flexible and cost-effective approach to internal auditing.
- Emerging Issues
    1. Changing Trends with Time
    2. Disruptive Business Environment
    3. Use of latest Technologies
    4. Right Talent and Skills
- Internal audit is a constantly evolving field, with new areas of focus emerging as organisations and industries change. Some emerging areas getting into focus in internal audit include:
    1. Cyber Security
    2. ESG (Environmental, Social, and Governance)
    3. Artificial Intellegence (AI)
    4. Regulatory and Risk compliance
    5. Supply Chain Risks
    6. Data Privacy
    7. Fraud Prevention
    8. Social Media
    9. Culture Audit
    10. Audit of Automated Process
    11. Legal & Company Secretarial
    12. Finaicial Crime
    13. Third Party Risk Management

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. What is Financial Accounting? Explain the risks involved in Financial Accounting?
2. What is Funding Risks? How it can be avoided?
3. What measures to be taken to avoid financial accounting risk?
4. What are the various business related challenges one can face while conding internal audit?
5. What are the Prons and Cons of In-house Internal Audit function?
6. What are the Prons and Cons of Outsourcing of Internal Audit function?
7. What are the Prons and Cons of Co-sourcing of audit assignment?
8. Why outsourcing is considered as a big risk?
9. Elaborate the various emerging areas to be focused while conducting Internal Audit.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's
- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

PART II

FORENSIC AUDIT