THE ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN INTERNAL CONTROL AND AUDIT

A PAPER DELIVERED AT THE MANDATORY CONTINOUS PROFESSIONAL DEVELOPMENT OF THE ASSOCIATION OF NATIONAL ACCOUNTANTS OF NIGERIA ANAN, 2024

BY

OGBU, Godwin Otseme CNA, MNIM, MBA
Managing Partner,
Primegate Professional Services
(Training, Consulting, Audit and Tax Advisory)

Primegate Professional Services

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN INTERNAL CONTROL AND AUDIT

1.0 INTRODUCTION

The advancement in technology has undoubtedly created unprecedented level of disruptions to the way businesses and organisations operate. These disruptions have also caused various business support functions to radically evolve. Businesses are now moving away from traditional systems of operation into employing and leveraging on Artificial Intelligence and Machine learning technologies to deliver superior goods and services to their clients and to maintain competitive advantage. The Internal Control and Audit is one of such functions that has evolved over time. From the known fraud detection and policing perspective, the internal control and audit role is now value adding / business assurances function. The expectations of stakeholders from the internal control and audit function have also increased due to the explosion in technology. For instance, there are calls for a shift from the traditional auditing techniques of sampling to the use of advanced technology with the capability to analyze all the operating activities of a business to improve audit quality. To meet these expectations, the Internal control/audit role must constantly adapt to the pace of technological changes within their organisations and a failure to do this would bring about a 'value-gap' where they are unable to provide value that aligns with the organisation growth pace. However, despite increasing innovation and technology-driven digital growth within organisations, Internal Control and Internal Audit functions are still playing catch up in many areas. These core Business Assurance functions are sometimes slow to realise the changes and digital evolution happening within their organisations, and still deploy traditional methodologies and solutions that cannot efficiently provide the needed assurance at the velocity of change within the organisation.

Artificial Intelligence and Machine Learning are among the most visible technological disruptions in today's business and organisations operations. Thomas (2019) asserts that Artificial Intelligence is the most important general purpose technology of our era, yet highly misunderstood. For the Internal Control/Auditor role to remain relevant, embracing these technologies within the context of how it impacts of his value addition role is very critical both for survival and continuous relevance.

This paper seeks to review the role of Artificial intelligence and Machine learning on the evolving internal control and audit function and to equip professional accountants with the requisite knowledge of innovations in Artificial Control world as it affects the internal control/audit ecosystem.

CONCEPTUALIZING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. It is seen as a system that can interpret external data correctly and learn from it and use those experiences to achieve specific goals and tasks in a manner flexible. The goal of AI is to create systems that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. When applied in business, AI can leverage technologies to enhance and optimize various aspects of business operations, decision-making, and overall performance.

Machine learning is a subset of AI that focuses on the development of algorithms and models that enable computers to learn from data and make predictions or decisions without explicit programming. The mail goal of machine learning is enabling machines to learn from data and improve performance on a specific task without being explicitly programmed. In other words, machine learning allows systems to automatically learn and improve from experience. Examples are image recognition, natural language processing, recommendation systems etc

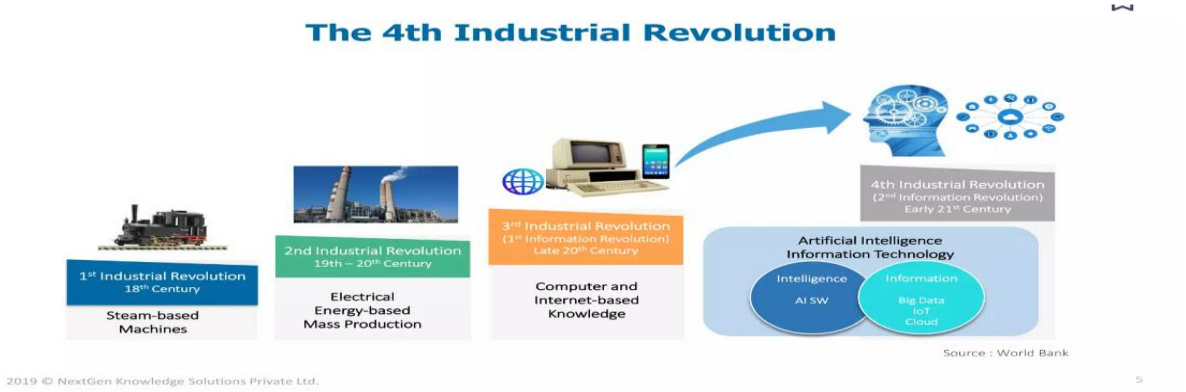
Artificial intelligence, the ability of a computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. Today, Artificial Intelligence (AI) is another, however, strong technological wave that is flattening the business world by providing the ability for a machine to perform cognitive functions, such as perceiving, reasoning, learning and interacting. AI has rapidly entered our lives by solving business problems due to three technological developments that have reached enough maturity and convergence: (1) advancement in algorithms, (2) massive data, and (3) increasing computational power and storage at low cost. According to Thomas (2019), in Havard Business Review assets that, even as significance of AI becomes irrefutable, it remains misunderstood. Executives view AI as a key disruptive technology, employees fear it as a job destroyer, consultant pitch it as a cure all and the media hype and deride it endlessly.

The year 2022 brought AI into the mainstream through widespread familiarity with applications of Generative Pre-Training Transformer. The most popular application is OpenAI's ChatGPT.

AI can be categorized into two main types:

1. **Narrow or Weak AI:** This type of AI is designed to perform a specific task or a narrow set of tasks. It is focused on a particular problem and does not possess the broad cognitive abilities of humans. Examples include virtual personal assistants like Siri or Alexa, image and speech recognition software, and recommendation systems.

2. **General or Strong AI:** This type of AI refers to machines with the ability to understand, learn, and apply knowledge across a wide range of tasks—similar to human intelligence. General AI is still largely theoretical and does not currently exist.



The 4th Industrial Revolution

1st Industrial Revolution
18th Century
Steam-based Machines
2nd Industrial Revolution
19th – 20th Century
Electrical Energy-based Mass Production
3rd Industrial Revolution
(1st Information Revolution)
Late 20th Century
Computer and Internet-based Knowledge
4th Industrial Revolution
(2nd Information Revolution)
Early 21st Century
Artificial Intelligence
Information Technology
Intelligence
AI SW
Information
Big Data
IoT
Cloud

Source : World Bank

2019 © NextGen Knowledge Solutions Private Ltd.

5

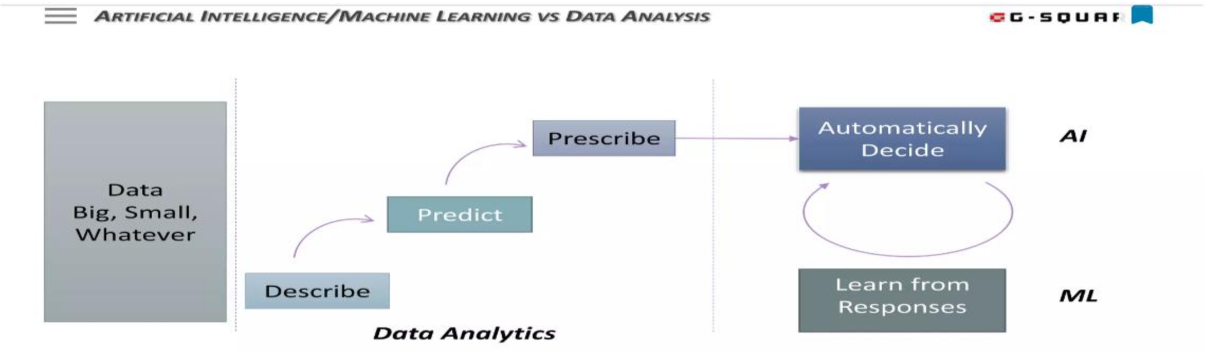
- Artificial Intelligence is a very critical component of the **4th Industrial Reolution.**

1.1. ARTIFICIAL INTELLIGENCE VERSUS DATA ANALYSTICS

It's important to note that AI and data analytics are often complementary, with AI techniques being applied within the field of data analytics to enhance the analysis and decision-making processes.

Feature	**Artificial Intelligence (AI)**	**Data Analytics**
Definition	AI refers to the development of computer systems that can perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and perception.	Data Analytics involves examining, cleaning, transforming, and modelling data to discover useful information, draw conclusions, and support decision-making.
Scope	Broader scope, encompassing various technologies and techniques to enable machines to mimic human intelligence across a range of tasks.	Focused on extracting insights from data to inform business decisions and improve processes.
Objective	Aims to create machines capable of intelligent behavior, learning from experience, and adapting to new situations.	Aims to uncover patterns, trends, and relationships within data to facilitate informed decision-making.
Methods	Includes machine learning, natural language processing, robotics, expert systems, and other advanced techniques.	Involves statistical analysis, data mining, predictive modeling, and other methods to extract meaningful information from data.
Learning	Involves machine learning techniques where systems can learn from data and improve their performance over time.	Emphasizes on understanding historical data to make informed predictions or identify trends.
Use Cases	Wide-ranging applications, including image and speech recognition,	Commonly used in business intelligence, marketing analytics,

Feature	Artificial Intelligence (AI)	Data Analytics
	autonomous vehicles, virtual assistants, and more.	financial analysis, healthcare analytics, etc.
Decision-Making	Capable of autonomous decision-making based on learned patterns and algorithms.	Provides insights and recommendations to support human decision-makers.
Examples	Chatbots, self-driving cars, recommendation systems, facial recognition, etc.	Descriptive analytics, predictive modeling, customer segmentation, fraud detection, etc.



Pictorial representation of Artificial Intelligence Vs Data Analytics

1.2 FACTS AND NUMBERS

From surveys and research conducted regarding Artificial Intelligence and Machine Learning, some of the striking findings readily comes to mind.

- In 2015, a World Economic Forum survey of Executives Predict That Artificial Intelligence Will Revolutionize The Corporate World By Taking Over A Staggering 30% Of Audits In 2025.
- A 2021 survey by the Institute of Management Accountants found that 84% of accounting professionals believe that AI and ML will have a significant impact on the accounting profession.
- A 2022 report by McKinsey & Company predicts that AI and ML could automate up to 45% of the tasks currently performed by accountants and auditors
- In 2023, Mckinsey and Co study predicted that AI could enable automation of up to 70 percent of business activities, across almost all occupations, between now and 2030
- A 2023 study by Deloitte found that AI and ML are already being used by 62% of accounting firms
- A 2023 study by PwC found that 80% of CFOs believe that AI and ML will have a significant impact on their ability to make better business decisions.

2.0 INTERNAL CONTROL

Internal control system is defined as the whole system of controls, financial and otherwise, established by the management to carry on the business of the enterprise in an orderly and efficient manner, ensure adherence and management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. Millichamp(2002). Internal control is defined in the 2013 COSO* Framework as “a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Internal control has essentially evolved as a value addition function within an organisation. In performing its Business Assurance as well as Value addition role, the Internal Control officers are sometimes slow to realise the changes and digital evolution happening within their organisations, and still deploy traditional methodologies and solutions that cannot efficiently provide the needed assurance at the velocity of change within the organisation. As business operations and functions experience unprecedented disruptions via automations and other technology enabled applications, like Artificial Intelligence, AI, Machine Language, ML, Block chain Technology and Robotic Process Automation among others, the internal control function has been challenged to evolve fast to meet these changes.

Despite increasing innovation and technology-driven digital growth within organisations, Internal Control (IC) and Internal Audit (IA) functions must constantly adapt to the pace of technological changes within their organisations and a failure to do this would bring about a ‘value-gap’ where the Business Assurance and value addition functions are unable to provide value that aligns with the organisation’s growth pace.

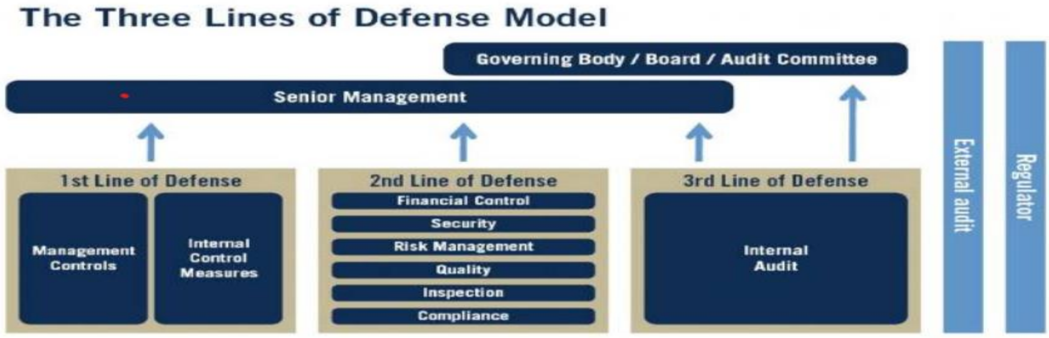
The Internal control and audit functions are increasingly expected to add value to organisations and stakeholders in ways that are beyond the capabilities of the traditional model, as stakeholders continuously demand a more efficient and agile assurance process, especially in the ever-evolving business landscape. It therefore becomes imperative that without a change in approach, the Internal Control and Audit functions may lose alignment with the organisation’s strategic direction and ability to provide assurance over emerging risks arising from the adoption of new technologies.

2.1 INTERNAL CONTROL VERSUS INTERNAL AUDIT

It is quite appropriate at this stage to highlight the point of convergence and divergence between Internal control and internal audit. This is because the two roles though used interchangeably most times have their distinctive areas of focus.

Feature	Internal Control	Internal Audit
Definition	A set of policies, procedures, and processes implemented by management to ensure the achievement of organizational objectives, safeguard assets, and ensure the accuracy of financial reporting.	A systematic and independent examination of an organization's activities, processes, and systems to assess and improve the effectiveness of risk management, control, and governance processes.
Purpose	To provide reasonable assurance regarding the achievement of objectives in the following areas: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations.	To provide an independent and objective assessment of the adequacy and effectiveness of internal controls, risk management, and governance processes.
Responsibility	Primarily the responsibility of management at all levels within an organization. Management designs, implements, and maintains internal control systems.	Typically conducted by internal auditors who are independent of the areas they audit. Internal audit reports to the highest levels of management, but they maintain independence to ensure objectivity.
Nature of Activity	Ongoing and continuous. Internal controls are designed to be in place throughout regular business operations.	Periodic and episodic. Internal audits are conducted periodically, often as part of an annual audit plan, and are not continuous activities.
Focus	Mainly focused on ensuring that organizational goals are achieved and that assets are protected. It includes processes for authorization, segregation of duties, and documentation.	Primarily focused on evaluating the effectiveness of internal controls, risk management processes, and governance structures in place within an organization.
Reporting	Management is responsible for reporting on the effectiveness of internal control systems in financial statements.	Internal auditors report their findings and recommendations directly to the audit committee and senior management. Internal audit reports are separate from financial statements.
Relationship	An integral part of an organization's day-to-day operations and is owned and executed by management.	Independent of the activities it evaluates, ensuring an unbiased assessment. Internal audit provides recommendations for improvement but does not implement changes.

2.2 INTERNAL CONTROL THREE LINES OF DEFENCE MODEL



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

- Internal Control is a first line of defence put in place by management of an organisation while internal audit is the third line of defence.
- For this discussion, Internal control and internal audit could be used interchangeably.

2.3 THE CHANGING DYNAMICS OF INTERNAL CONTROL

As stated earlier, the Internal Control function has evolved and still evolving. Leveraging on the existing technology to optimize productivity appears the only option available for the internal control officer.- Table below presents the present and future outlook of the internal control/audit role.

Aspect	**Present Outlook**	**Future Outlook**
Technology Integration	Many organizations are incorporating technology into internal control processes, such as automation tools, AI, and data analytics.	The future will see an increased reliance on advanced technologies, including machine learning, blockchain, and predictive analytics, for more efficient and effective control measures.
Risk Management	Risk assessment and management are key components of internal control, with a focus on identifying and mitigating potential risks.	The future will see a more dynamic and real-time approach to risk management, leveraging data-driven insights and scenario analysis to adapt quickly to changing risk landscapes.
Audit Sampling	Audit are based on small random sampling which can be expanded based on risk perception.	`100% audit sampling due to the use of technological tools with ability to sample large data.
Audit Planning	Annual Audit plan is gradually becoming irrelevant due to frequent changes in business	Audit plan is responsive to distruptions and flexes to meet shifting strategic demands.

Aspect	Present Outlook	Future Outlook
Strategic decision making	Not involved in strategic decision of organisations.	Very much involved in high level conversations, board meetings and C-Suites
Regulatory Compliance	Organizations comply with various regulations, and internal controls are designed to ensure adherence to legal requirements.	Anticipation of regulatory changes will become integral, with proactive adjustments to internal controls to address evolving compliance landscapes.
Cybersecurity	With the increasing frequency of cyber threats, internal controls include measures to safeguard information systems and data.	Future internal controls will have an enhanced focus on cybersecurity, incorporating advanced threat detection, encryption, and continuous monitoring practices.
Frequency of Checks	Periodic and most times quarterly	Continuous and real time checks and audit now a reality
Remote Work Challenges	The COVID-19 pandemic necessitated adjustments to internal controls to accommodate remote work setups.	The future will involve a hybrid approach to internal control, considering the ongoing prevalence of remote work and ensuring controls are adaptable to different working models.
Expertise	Most Internal Control and audit professionals have audit expertise only	Internal Control and Audit personnel posses a mix of business, audit, technology and analytic skills
Data Privacy	Protection of sensitive data is a critical aspect of internal controls, with an emphasis on compliance with data privacy regulations.	Future internal controls will prioritize data privacy, with increased scrutiny on data handling processes and mechanisms to ensure compliance with evolving privacy standards.
Internal Auditing	Internal audits play a role in evaluating the effectiveness of internal controls.	Internal audit functions will evolve to become more data-centric, leveraging technology for continuous monitoring and real-time auditing to provide timely insights.
Cultural Awareness	Establishing a culture of control awareness is essential for the success of internal controls.	Future internal control frameworks will focus on cultivating a strong control culture, integrating control awareness into everyday operations and decision-making.
Environmental, Social, and Governance (ESG) considerations	The present sees an increasing awareness of ESG factors, influencing internal control practices.	The future will witness a more comprehensive integration of ESG considerations into internal controls, aligning with global sustainability goals and stakeholder expectations.

The table above further buttresses the strategic role technology-including Artificial intelligence will play in the future of the internal control role.

2.4 COMPONENTS OF INTERNAL CONTROL

internal control consists of **five interrelated components** which are derived from the way management runs a business and are integrated with the management process. COSO (2013)
They apply to entities of all sizes, although smaller organizations are likely to implement them in a more informal manner. The components are:

- **Control Environment**—This sets the tone for the organization, providing the foundation for all other components of internal control. It includes integrity, ethical values and the competence of the people.
- **Risk Assessment**—This is the identification and analysis of relevant risks, internal and external, to the achievement of the objectives, forming a basis for determining how the risks should be managed.
- **Control Activities**—These helps ensure that the necessary actions are taken to address risks relating to the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions.
- **Information and Communication**—Internal and external information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also must occur in a broader sense, flowing down, across and up the organization.
- **Monitoring**—Internal control systems need to be monitored, a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

3.0 ROLE OF ARTIFICIAL INTELLIGENCE IN BUSINESS

It has earlier been established that the modern role of Internal audit exists within the business processes and function, hence, to understand the impact of Artificial Intelligence on internal control, it is pertinent to appreciate the role of Artificial Intelligence on Business. According to Palanivelu and Vasanthi, (2020),The applications of Artificial Intelligence range from detecting trends in data to mitigate market risks, enhancing customer service through virtual personal assistants, or even analysing millions of documents across a company's servers to find compliance failures. But it is only recently that companies have been able to anticipate and envision the possibilities that Artificial Intelligence and robotics can bring to the future of the business world.

The goal of AI in business is to leverage artificial intelligence technologies to enhance and optimize various aspects of business operations, decision-making, and overall performance. AI can be applied across a wide range of industries and functions, and its goals in business can be diverse. Some of the key objectives include:

1. **Automation:** AI can automate routine and repetitive tasks, allowing employees to focus on more complex and creative aspects of their work. This can lead to increased efficiency and productivity.
2. **Data Analysis:** AI systems can analyze large volumes of data quickly and accurately, extracting valuable insights that can inform strategic decisions. This data-driven approach helps businesses make more informed choices and improve overall performance.
3. **Personalization:** AI enables businesses to deliver personalized experiences to customers. Through the analysis of customer data, AI systems can tailor products, services, and marketing efforts to individual preferences, leading to increased customer satisfaction and loyalty.
4. **Customer Service:** AI-powered chatbots and virtual assistants can provide 24/7 customer support, addressing inquiries and resolving issues in real-time. This improves customer service efficiency and enhances the overall customer experience.
5. **Predictive Analytics:** AI algorithms can predict future trends and outcomes based on historical data, helping businesses make proactive decisions and anticipate market changes.
6. **Supply Chain Optimization:** AI can be used to optimize supply chain management by predicting demand, managing inventory, and improving logistics. This leads to cost savings and a more efficient supply chain.
7. **Fraud Detection and Security:** AI algorithms can detect unusual patterns and anomalies in transactions, helping businesses identify and prevent fraudulent activities. Additionally, AI can enhance cybersecurity measures to protect sensitive business information.
8. **Innovation:** AI fosters innovation by enabling the development of new products and services. Businesses can explore novel ideas, create prototypes, and test hypotheses more rapidly with the assistance of AI.
9. **Cost Reduction:** Through automation and efficiency improvements, AI can contribute to cost reduction in various business processes, leading to increased profitability.
10. **Competitive Advantage:** Adopting AI technologies can give businesses a competitive edge in the market. Those who embrace and implement AI effectively are often better positioned to adapt to changing market conditions and stay ahead of the competition.

3.1 HOW ARTIFICIAL INTELLIGENCE HAS CHANGED THE LANDSCAPE OF SPECIFIC BUSINESS OPERATIONS

According to Buntak etál (2021), the benefits of using AI in the business are several and benefits are additionally arising with development of industry 4.0 and with an increase of AI use. With collecting and creating large amounts of data, organizations can, thought the usage of AI, conduct different kinds of simulations which can lead to identifying future trends as well as the needs of stakeholders in the organizational environment.

No doubt, the introduction of Artificial Intelligence has radically transformed the landscape of business operations across various sectors. These transformations present a renewed challenge for operators to either shape in, by getting acquainted or shape out by way of extinction due to irrelevance.

Industry	**Business Operation**	**AI Impact**
Healthcare	Diagnostics and Imaging	AI-powered algorithms analyze medical images for faster and accurate diagnosis and prescription assisting healthcare professionals. Telemedicine etc
Energy	Energy Management	Detection of Energy Theft, predicting generation capacity and even grid collapse, Big Data Analysis etc
Agriculture	Precision Farming	AI analyzes data from sensors and drones to optimize crop management, improve yields, and reduce resource usage.
Manufacturing	Predictive Maintenance	AI analyzes sensor data to predict equipment failures, enabling proactive maintenance and minimizing downtime.
E-commerce	Personalized Recommendations	AI algorithms analyze customer behavior to provide tailored product recommendations, enhancing the shopping experience.
Transportation and Logistics	Route Optimization	AI optimizes delivery routes, reducing fuel costs, and improving overall efficiency in logistics operations.
Marketing	Targeted Advertising	AI analyzes user data to deliver personalized and targeted advertisements, increasing the effectiveness of marketing campaigns.
Education	Adaptive Learning	AI-driven adaptive learning platforms customize educational content based on individual student performance and needs.
Human Resources	Recruitment and Hiring	AI automates resume screening, streamlines recruitment processes, and identifies suitable candidates through data analysis.

3.2 APPLICATION OF ARTIFICIAL INTELLIGENCE TO INTERNAL CONTROL/AUDIT

According to Al-sayyed et ál (2021), The audit profession has substantially changed over time because of technological change. Many changes in this profession have already been witnessed. They include an increase in the number and sophistication of the auditing rules, numerous changes in the standards of professional ethics, an improved quality of the audit work, growing competition among the audit firms, reduced audit fees, and provision of new services to the customers (e.g., financial and computing advices). Additionally, this profession has witnessed development of new audit types and services. These factors have together made the auditing profession more and more competitive than ever before.

Having highlighted the role of Artificial Intelligence in Business, it is important to know that these roles brought some forms of disruptions to businesses to which the internal control function must respond to in order to add value to business processes and operations. Some of the specific ways AI can be applied on the Internal Control function are;

1. **Data Analysis and Monitoring:**
    - AI can analyze large volumes of data quickly and accurately, identifying patterns, anomalies, and trends that may be indicative of control weaknesses or potential risks.
    - Continuous monitoring using AI algorithms allows for real-time detection of irregularities, reducing the reliance on periodic audits.

2. **Fraud Detection and Prevention:**
    - AI can be employed to develop predictive models for detecting fraudulent activities by analyzing transactional data and identifying unusual patterns or behaviors.
    - Machine learning algorithms can adapt over time, improving their ability to detect new and evolving forms of fraud.

3. **Automation of Routine Tasks:**
    - AI can automate repetitive and routine tasks in the internal control process eg call overreducing the likelihood of human error and allowing staff to focus on more complex and strategic activities.
    - This includes tasks such as data entry, reconciliation, and routine compliance checks.

4. **Risk Assessment:**
    - AI tools can assess and quantify risks by analyzing historical data and identifying potential risk factors.
    - Predictive analytics can be used to forecast potential future risks, enabling proactive risk management and mitigation.

5. **Natural Language Processing (NLP):**
    - NLP allows AI systems to understand and interpret human language, which is useful for analyzing unstructured data such as emails, contracts, and regulatory documents.
    - NLP can help in identifying language patterns that may indicate non-compliance or other issues.

6. **Audit Trail Analysis:**
    - AI can analyze audit trails and transaction logs to reconstruct events and identify any deviations from normal operations.
    - This helps in ensuring the integrity and reliability of the information system and detecting any unauthorized or suspicious activities.
7. **Predictive Analytics for Compliance:**
    - AI models can predict potential compliance issues by analyzing historical compliance data and regulatory changes.
    - This enables organizations to proactively address compliance requirements and avoid penalties.
8. **Machine Learning for Decision Support:**
    - AI-driven decision support systems can assist in making more informed and data-driven decisions related to internal controls.
    - These systems can provide insights into the effectiveness of existing controls and recommend improvements based on the analysis of historical data.

9. **Cybersecurity Enhancements:**
    - AI can strengthen cybersecurity measures by continuously monitoring network traffic, identifying potential threats, and responding in real-time to cyber-attacks.
    - This is crucial for maintaining the confidentiality, integrity, and availability of sensitive information.

3.3 HOW ARTIFICIAL INTELLIGENCE HAS CHANGED LANDSCAPE OF INTERNAL CONTROL ON KEY HIGH RISK AREAS.

Prior to the deployment of AI tools, internal control/audit has been largely manual or at best with the use of some basic computer tools for adding figures and report writing. With the -deployment of AI, the audit control ecosystem around specific high risk audit areas are highlighted below.

It should be noted however that, whether in terms of its breadth or depth, application of AI in the audit industry is still in embryo. Complexity of the AI technology and shortage of experience in its use have created big difficulties for its adoption and development. Hence, a long way is still ahead to walk for development of AI in the audit area. Al-sayyed et'al (2021)

3.3.1 Cash

Cash is the most sensitive, liquid and volatile asset that constitute high risk in internal control and audit. Its importance and risk cuts across manufacturing and service entities. The involvement of AI has greatly impacted on the landscape of control over this very vital resource of an organization.

Control Aspect	Internal Control Operations Before AI	Internal Control Operations with AI	AI Tool Used
Cash and Bank Reconciliation	Regular (daily, weekly and monthly) manual reconciliation of cash transactions and bank statements and detecting anomalies long after infractions have occurred	AI software reconciles transactions in real-time, flagging discrepancies.	Intelligent Automation Software, e.g., UiPath, Automation Anywhere.
Access control to cash areas	Physical controls to safeguard cash, such as safes and locked storage, use of registers to track movements within cash areas etc	Advanced biometric authentication like Biometric scans (fingerprint, retina) required for access to cash storage. for access to cash storage areas, enhancing physical security.	Biometric Access Control Systems, e.g., Face recognition systems, fingerprints etc
Audit Trail	Reviewing and documenting transaction manually or by samples based on materiality trails to detect anomalies.	AI algorithms analyze patterns and detect anomalies in cash transactions, helping to identify potential fraud.	Machine Learning (ML) models, e.g., TensorFlow, IBM Watson.

3.3.2 Inventory

This is also a high-risk area especially for entities involved in manufacturing, e commerce, healthcare etc.

Control Aspect	Internal Control Operations Before AI	Internal Control Operations with AI	AI Tool Used
Inventory Monitoring and Tracking	Manual tracking through spreadsheets, periodic physical counts, and reconciliation.	Continuous real-time monitoring through AI-powered systems that use sensors, RFID technology, and computer vision for accurate and instantaneous inventory tracking.	Radio Frequency Identification Technology and Computer Vision.
Fraud Detection	Limited ability to detect sophisticated fraud schemes.	Advanced AI algorithms capable of detecting anomalies and patterns indicative of fraud or theft, enhancing fraud prevention.	Splunk or SAS Fraud Framework are used to identify unusual patterns indicative of fraudulent activities.
Forecasting and Demand Planning	Reliance on historical data and basic forecasting models.	AI-driven predictive analytics that consider a multitude of variables, improving accuracy in demand forecasting and inventory optimization.	Rapid Miner, Alteryx, Liamasoft Supply Chain Guru, Gradient Boosting Machines etc
Reporting and Analytics	Manual generation of reports with limited insights.	AI-powered analytics platforms providing real-time and comprehensive reports, enabling data-driven decision-making.	Power BI, Zebra BI, IBM Watson Chain Insight, etc

3.3.3 Property Plant and Equipment (PPE)

The changes that has occurred with the use of AI in internal control for PPEs are highlighted below

Internal Control Aspect	Before AI	After AI	Examples of AI Tools
Asset Identification	Manual tracking and tagging of assets.	Automated asset tagging using computer vision.	RFID (Radio-Frequency Identification) for tracking assets. Computer Vision for Tagging, Geocoordinates for locations
Asset Valuation	Manual appraisal and periodic assessments.	AI-driven valuation models for real-time updates.	Machine learning algorithms for predictive asset valuation eg ARIMA AutoRegressive Integrated Moving Average.
Maintenance Scheduling	Scheduled maintenance based on predefined plans.	Predictive maintenance using AI algorithms.	IoT sensors and AI analytics for predictive maintenance.
Fraud Detection	Reliance on manual audit trails and sampling.	AI-driven anomaly detection for real-time monitoring.	Machine learning algorithms for identifying unusual patterns.
Reporting and Analytics	Manual reporting with periodic reviews.	AI-driven analytics for real-time insights.	Business Intelligence tools with AI-based analytics features like Tableau, Power BI, Sisense, ThoughtSpot etc

3.3.4 HUMAN CAPITAL (EMPLOYEE)

It is important to note that while AI tools can significantly enhance internal controls over human capital, they should be implemented with careful consideration of ethical and legal implications, and human oversight remains crucial for decision-making. Additionally, the specific tools mentioned may evolve or new tools may emerge in the rapidly advancing field of AI.

	Before AI	With AI (Using Specific AI Tools)
Recruitment and Hiring	Traditional resume screening, interviews	AI-driven resume parsing (e.g., HireVue, Ideal), predictive analytics for candidate matching (e.g., IBM Watson Talent Insights)
Employee Onboarding	Manual onboarding processes	Chatbots for automated onboarding (e.g., Talla, WorkBright)
Training and Development	Instructor-led training, manual tracking	AI-driven personalized learning platforms (e.g., Cornerstone OnDemand, Degreed)
Performance Management	Annual reviews, subjective evaluations	Continuous performance monitoring with AI analytics (e.g., Reflektive, 15Five)
Workforce Planning	Manual forecasting, limited	AI-driven predictive analytics (e.g.,

	Before AI	With AI (Using Specific AI Tools)
	data analysis	Visier, Oracle HCM) for strategic workforce planning
Employee Engagement	Surveys, feedback forms	AI-driven sentiment analysis tools (e.g., Glint, Qualtrics) for real-time feedback analysis
Time and Attendance	Manual timesheets, traditional clocking systems	AI-based automated time tracking (e.g., Kronos, Deputy) with facial recognition or biometric authentication
Compliance Monitoring	Manual audits, periodic checks	AI-powered compliance monitoring tools (e.g., Compl.ai, AuditBoard) for real-time risk detection
Health and Well-being	Employee self-reporting, wellness programs	AI-based health monitoring (e.g., BioBeats, Welltok) for proactive health interventions
Succession Planning	Limited succession plans, manual updates	AI-driven talent analytics (e.g., SAP SuccessFactors, Talentsoft) for automated succession planning

3.4 ISSUES EMANATING FROM THE USE OF ARTIFICIAL INTELLIGENCE IN INTERNAL CONTROL

Despite the numerous benefits, the use of AI has on the internal audit process, it is not without challenges or issues. Key among the issues are highlighted below.

1. **Lack of Interpretability:**
   - Many AI models, especially deep learning models, operate as "black boxes," making it difficult for auditors to understand and interpret the reasoning behind their decisions. This lack of interpretability and transparency can make it difficult for auditors and stakeholders to understand and trust the decisions made by AI systems, potentially raising concerns about accountability, reliability and compliance.

2. **Data Quality and Integrity:**

   - **Challenge:** AI systems heavily rely on data for training and decision-making. If the data used is incomplete, inaccurate, of poor quality or biased, it can lead to flawed outcomes, inaccurate and unfair audit results.
   - **Concern:** Inaccurate data could result in incorrect conclusions and decisions, potentially undermining the effectiveness of internal controls.

3. **Ethical Concerns:**
   - The use of AI in auditing raises ethical considerations, such as privacy concerns, data security, and the potential impact on employment.

Auditors must carefully navigate these ethical issues to ensure responsible and transparent use of AI in their processes.

4. **Regulatory Compliance:**
    - Auditors must comply with various regulations and standards, and the use of AI may pose challenges in meeting these requirements. Ensuring that AI systems align with regulatory frameworks and standards is crucial to avoid legal and compliance issues.
5. **Overreliance on Technology:**
    - There is a risk of overreliance on AI technology, leading to a reduction in human involvement in the audit process. While AI can automate routine tasks, human judgment and expertise remain essential for complex decision-making, understanding business context, and addressing unexpected situations.
6. **Continuous Monitoring and Updating:**
    - AI models require continuous monitoring and updating to stay relevant and effective. Changes in business environments, regulations, or technology can impact the performance of AI models. Auditors need to invest in ongoing training and updates to keep their AI systems up-to-date.
7. **Cybersecurity Risks:**
    - AI systems can be vulnerable to cybersecurity threats, including attacks that manipulate data or compromise the integrity of AI algorithms. Auditors must implement robust cybersecurity measures to protect AI systems and the sensitive data they handle.
8. **Skill Gap:**
    - The implementation of AI in audit requires a certain level of technical expertise. There may be a skill gap among auditors in terms of understanding and effectively utilizing AI tools. Training and education are essential to bridge this gap and ensure that auditors can leverage AI technology effectively.
9. **Cost and Resource Constraints:**
    - Implementing AI in audit may require significant financial investments in technology, training, and infrastructure. Small and mid-sized audit firms may face challenges in allocating resources for AI adoption, potentially leading to disparities in the industry.

10. **Algorithmic Bias:**
    - **Challenge:** AI algorithms may inherit biases present in historical data, leading to discriminatory or unfair outcomes.
    - **Concern:** If internal control decisions are influenced by biased algorithms, it can result in discriminatory practices or the perpetuation of existing biases within the organization.

To address these challenges, organizations need to carefully plan and implement AI solutions, ensuring that ethical considerations, regulatory compliance, and transparency are prioritized throughout the process. Regular monitoring, updates, and collaboration between human experts and AI systems are essential for successful integration into internal control frameworks.

3.5 CHALLENGES INTERNAL CONTROL OFFICERS ENCOUNTER IN THE FACE OF AI USE IN BUSINESS.

The integration of AI poses several challenges for internal control practitioners, particularly in areas related to data security, decision-making, and the overall effectiveness of internal controls. Here are some challenges and potential ways to overcome them:

1. **Understanding and Managing AI Risks:**
    - **Challenge:** Internal control practitioners may struggle to understand and manage the risks associated with AI, including biases in algorithms, data privacy concerns, and potential security vulnerabilities.
    - **Solution:** Regular training and education programs for internal control teams can help enhance their understanding of AI risks. Collaborating with data scientists and AI experts can provide valuable insights into the technology and its potential impact on internal controls.
2. **Ensuring Transparency and Explainability:**
    - **Challenge:** AI algorithms, particularly deep learning models, can be complex and difficult to interpret. Ensuring transparency and explainability of AI-driven decisions is crucial for internal control practitioners.
    - **Solution:** Use AI models that offer explainability features or integrate third-party tools that provide insights into model decisions. Establishing clear documentation and communication channels about how AI is used in decision-making processes enhances transparency.

3. **Data Quality and Integrity:**
    - **Challenge:** AI heavily relies on data, and poor data quality or integrity issues can lead to inaccurate predictions and decisions, impacting internal controls.
    - **Solution:** Implement robust data governance practices to ensure data quality and integrity. Regularly audit and clean data to identify and rectify inconsistencies. Establish data validation processes to detect anomalies and errors in real-time.
4. **Addressing Bias in AI:**
    - **Challenge:** AI models can inadvertently perpetuate biases present in training data, leading to unfair or discriminatory outcomes.
    - **Solution:** Conduct thorough bias assessments on AI models and take steps to mitigate biases. Implement diverse and representative

datasets during model training. Regularly update models to adapt to evolving patterns and biases.

5. **Cybersecurity Concerns:**
   - **Challenge:** The increased use of AI introduces new attack vectors, and AI systems can be vulnerable to adversarial attacks.
   - **Solution:** Strengthen cybersecurity measures by employing encryption, secure APIs, and regular security audits. Develop and implement response plans for potential AI-related security incidents.
6. **Adapting to Rapid Technological Changes:**
   - **Challenge:** The field of AI is dynamic, with rapid advancements and changes. Internal control practitioners may find it challenging to keep up with evolving technologies.
   - **Solution:** Foster a culture of continuous learning within the organization. Establish partnerships with external experts and stay informed about the latest developments in AI through conferences, training programs, and industry publications.
7. **Legal and Ethical Compliance:**
   - **Challenge:** Ensuring that AI applications comply with legal and ethical standards can be challenging, particularly in evolving regulatory landscapes.
   - **Solution:** Stay informed about relevant laws and regulations governing AI in the specific industry and region. Establish ethical guidelines for AI use within the organization and regularly review and update them to align with changing standards.

By addressing these challenges through a combination of education, technology integration, and proactive risk management, internal control practitioners can better navigate the complexities introduced by AI. Regular collaboration with IT, data science, and legal teams is essential to ensure a comprehensive and effective approach to AI integration within the organization.

3.6 LEGAL AND ETHICAL CONCERNS IN THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN BUSINESS

As pointed out in the issues and challenges posed using artificial intelligence and machine learning, the legal and ethical concerns are key to the deployments, acceptance and future of this technology. While ethical issues speak to the morality, fairness, accountability, and the impact of the technology on individuals and society, the legal angle addresses the concerns around the laws in place in various jurisdictions the technology will be applicable, This will be discussed below;

- **Ethical Issues:**

1. **Transparency and Accountability:**

- There is a growing demand for transparency in AI and ML systems, especially those used in critical applications like healthcare and criminal justice.
- Accountability for the decisions made by AI systems is crucial to ensure responsible use.

2. **Fairness and Bias:**
    - Addressing bias in AI algorithm and the ML is a significant ethical concern. Algorithms should be designed and trained to avoid discrimination and treat all individuals fairly.
3. **Privacy:**
    - AI and ML applications often involve the processing of large amounts of personal data. Protecting individuals' privacy is a key ethical consideration, and regulations like GDPR (General Data Protection Regulation) in the European Union reflect this concern.
4. **Security:**
    - Ensuring the security of AI and ML systems is crucial to prevent malicious uses, hacking, or manipulation of algorithms.
5. **Autonomy and Accountability:**
    - Determining the level of autonomy for AI and MLs systems and establishing who is accountable for their actions are ongoing ethical debates.

- **Legal Issues**

1. **Privacy and Data Protection:**
    - Data Collection and Consent: AI systems often require large amounts of data for training. Ensuring informed consent and transparent data collection practices are crucial to comply with privacy regulations.
    - Personal Data Handling: AI systems may process sensitive personal information, raising concerns about how this data is handled and protected under privacy laws such as GDPR (General Data Protection Regulation) in the European Union**.**
2. **Bias and Discrimination:**
    - Algorithmic Bias: AI algorithms may inadvertently perpetuate or amplify existing biases present in training data. Discriminatory outcomes can lead to legal challenges, especially in areas such as employment, lending, and law enforcement.
    - Anti-discrimination Laws: If AI systems result in discriminatory practices, they may violate anti-discrimination laws. Developers and organizations may be held accountable for biased outcomes.
3. **Intellectual Property:**
    - Ownership of AI-generated Content: Determining ownership of content generated by AI can be challenging. Questions arise regarding

copyright, patent, and trademark laws in instances where AI contributes to creative or innovative outputs**.**

4. **Liability and Accountability:**
    - Responsibility for AI Actions: Identifying who is responsible for the actions or decisions made by AI systems is a legal challenge. If an AI system causes harm, determining liability can be complex and may involve developers, users, or even the AI itself.
    - Product Liability: Manufacturers and developers could be held liable for defects or failures in AI systems, particularly if they result in harm.
5. **Security Concerns:**
    - Cybersecurity: AI systems may be vulnerable to cyber-attacks or manipulation. Ensuring the security of AI systems is crucial to prevent unauthorized access, data breaches, and other malicious activities.
6. **Regulatory Compliance:**
    - Compliance with Laws and Regulations: Adhering to existing laws and regulations, as well as adapting to new ones specific to AI, is a major legal challenge. Different jurisdictions may have varying rules regarding the development, deployment, and use of AI.
7. **Transparency and Explainability:**
    - Explainability Requirements: As AI systems make decisions, there is a growing demand for transparency and explainability. This is particularly important in sectors like finance and healthcare, where clear justifications for AI decisions are necessary to comply with regulations.
8. **Employment and Labor Laws:**
    - Impact on Jobs: The integration of AI in the workplace may raise concerns about job displacement and changes in employment dynamics. Legal issues may arise related to workforce adaptation, retraining, and potential job losses.

3.6 CONCLUSION

The issues highlighted above creates opportunities rather than constitutes a threat to the internal auditor. The question on whether or not AI has come to stay in our businesses and operations has long been answered, adjustment to the rapidly evolving technology is the only way not just for survival but remaining relevant to perform the value added function that internal control has evolved to become. Consequently, by proactively addressing the challenges associated with AI-enabled devices and systems, internal auditors can contribute to the overall effectiveness of internal controls and risk management within their organizations.

3.7 RECOMMENDATION- THE WAY FORWARD

The integration of AI-enabled devices in organizations introduces new challenges and opportunities for internal auditors. To prepare for this evolving landscape, internal auditors should consider the following actions:

1. **Stay Informed about AI Technology:**
    - Regularly update your knowledge about AI technologies, their applications, and potential impact on internal controls.
    - Attend training programs, workshops, and conferences focused on AI in business and audit.
2. **Understand AI Risks and Controls:**
    - Develop a deep understanding of the risks associated with AI, including biases, security vulnerabilities, and the potential for fraud.
    - Identify and assess the effectiveness of controls designed to mitigate AI-related risks.
3. **Collaborate with IT and Data Analytics Teams:**
    - Foster collaboration with IT and data analytics teams to understand the organization's AI systems, algorithms, and data management practices.
    - Participate in joint training sessions to enhance cross-functional understanding.

4. **Update Audit Methodologies:**
    - Modify audit methodologies to incorporate considerations for AI-enabled systems. This may include specialized audit procedures for assessing algorithms, data integrity, and model outputs.
    - Ensure that audit procedures are flexible and can adapt to rapid technological changes.
5. **Enhance Data Analytics Skills:**
    - Strengthen your data analytics skills to effectively audit AI systems, which often involve large datasets and complex algorithms.
    - Explore tools and techniques for auditing machine learning models and algorithms.
6. **Focus on Ethical and Regulatory Compliance:**
    - Emphasize the importance of ethical considerations in AI adoption within the organization.
    - Stay informed about relevant regulations and standards pertaining to AI and ensure that the organization is in compliance.
7. **Evaluate AI Governance Frameworks:**
    - Assess the organization's governance frameworks for AI, including policies, procedures, and oversight mechanisms.
    - Ensure that there are clear lines of responsibility and accountability for AI-related decisions.
8. **Conduct Risk Assessments:**

- Include AI-related risks in regular risk assessments and prioritize them based on potential impact and likelihood.
- Develop risk mitigation strategies specific to AI technologies.

9. **Promote Continuous Learning:**
    - Foster a culture of continuous learning within the internal audit team to keep pace with evolving AI technologies.
    - Encourage team members to pursue relevant certifications and training programs.
10. **Collaborate with External Experts:**
    - Engage with external experts, such as AI specialists, data scientists, or consultants, to gain insights into best practices and emerging trends in AI auditing.

References

Al-Sayyed, S., Al-Aroud, S & Zayed, L. (2021). The effect of artificial intelligence technologies on audit evidence.*Accounting*, 7(2), 281-288.

Buntak, K., Kovačić, M., & Mutavdžija, M. (2021). Application of Artificial Intelligence in the business. *International journal for quality research*, *15*(2), 403.

Earley, C. E. (2015). Data analytics in auditing: Opportunities and challenges. Business Horizons, 58(5), 493-500.

EY. 2019. Audit innovation. Available at: https://www.ey.com/en_us/audit/innovation [Retrieved 2022-02-07]

Ergen, M. (2019). What is artificial intelligence? Technical considerations and future perception. Anatolian J. Cardiol, 22(2), 5-7

Haenlein, M., Kaplan, A.: A brief history of artificial intelligence: on the past, present, and future of artificial intelligence. California Manag. Rev. 61(4), 5–14 (2019). https://journals.sag epub.com/doi/pdf/10.1177/0008125619864925. Accessed 2 May 2020

https://www.cpajournal.com/2019/06/19/machine-learning-in-auditing/

https://www.accountingtoday.com/opinion/ai-and-the-future-of-the-accounting-profession

https://tax.thomsonreuters.com/blog/the-impact-of-artificial-intelligence-on-the-tax-and-accountingprofession/

Palanivelu, V. R., & Vasanthi, B. (2020). Role of artificial intelligence in business transformation. *International journal of advanced science and technology*, *29*(4), 392-400.

Thomas H, D (2019), The State of AI in Business. Artificial Intelligence. Insight you need from Havard Business Review series. www.hbr.org