

Revolutionizing Internal Audit with Artificial Intelligence

Addressing Challenges and Enhancing Efficiency and Effectiveness

Kudakwashe Charandura



**Why did the auditor cross
the road?**

Internal Audit processes needs to evolve

Question - Why did the auditor cross the road?

Response - Because he looked in the file and that's what they did last year.



Challenges faced by modern day Internal Auditors

Complexity

Data Overload

Large Data Volumes (Big Data)

Fraud Detection

Emerging risks and Technologies

Changing market conditions

Complex business models and structures

Evolving business risks

Scarcity of Skills

Large Document review

Spiking Cyber Attacks

Audit quality issues

Regulatory Pressure

Globalization and cross-border transactions

Remote working

Keeping up with professional standard

Increasing Costs



- The Modern day auditor is facing numerous challenges including growing data, evolving risks...
- And they are GenZ...
- Without tools it will be difficult to assess client risks effectively

Traditional Internal Audit Challenges

Identifying Key Issues in Current Practices

1

Manual processes and reliance on sampling

Traditional audits often depend on manual methods, increasing workload and limiting efficiency.

2

Limited coverage and scope of audits

Audits may not cover all areas, leading to potential oversights and gaps in risk management.

3

High risk of human error

Human involvement in audits raises the likelihood of mistakes, which can compromise audit integrity.

4

Inefficient data analysis methods

Current data analysis techniques are often inadequate, hindering effective decision-making.

5

Difficulty in identifying complex risks

Traditional approaches struggle to recognize sophisticated risks, leaving organizations vulnerable.

6

Inadequate resource allocation

Resources are often misallocated, affecting the quality and thoroughness of audits.

7

Limited continuous monitoring capabilities

Organizations lack the tools for ongoing monitoring, reducing responsiveness to emerging issues.

8

Difficulty keeping up with evolving regulations

Rapidly changing regulations create challenges for internal auditors to maintain compliance.

Consequences of Ineffective Internal Audit

Lessons from Major Corporate Failures



Underlying Causes of Internal Audit Failures

Identifying Key Factors Contributing to Ineffectiveness

- 1 Inadequate resources and budget constraints**
Limited funding can hinder audit processes and effectiveness.
- 2 Lack of skilled personnel**
A deficiency in qualified auditors can lead to ineffective audits.
- 3 Insufficient technology and tools**
Outdated or lacking technological support can impede audit efficiency.
- 4 Ineffective audit planning and scoping**
Poor planning can result in incomplete or superficial audits.
- 5 Poor communication with stakeholders**
Ineffective dialogue can lead to misunderstandings and audit failures.
- 6 Failure to identify emerging risks**
Ignoring new risks can expose organizations to unforeseen issues.



Artificial Intelligence: A Game-Changer for Internal Audit

Exploring AI's Role in Enhancing Audit Efficiency and Effectiveness



Enhancing Internal Audit with AI

Transforming Audit Process for Greater Effectiveness

- **Improved efficiency and productivity**
AI streamlines audit processes, reducing manual tasks and allowing teams to focus on strategic analysis.
- **Better risk management strategies**
AI enhances risk assessment by identifying patterns and predicting potential risks before they escalate.
- **Enhanced accuracy and reliability of audits**
AI minimizes human error, ensuring more consistent and trustworthy audit results.
- **Enhanced compliance and regulatory adherence**
AI ensures that audits meet compliance requirements through automated checks and balances.
- **Increased coverage and scope of auditing processes**
AI technologies enable audits to cover more areas and data sources, providing a holistic view.
- **Real-time insights and monitoring capabilities**
AI facilitates continuous monitoring, allowing auditors to react promptly to emerging issues.



AI-Powered Internal Audit Solutions

Harnessing AI for Enhanced Audit Efficiency and Effectiveness



Predictive Analytics for Risk Forecasting

Utilizes historical data to identify potential risks before they occur, enhancing proactive decision-making.



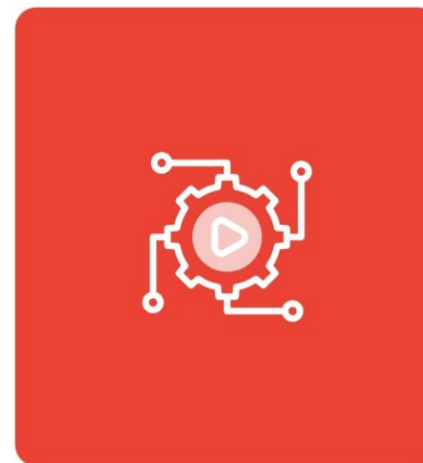
Machine Learning-Based Risk Assessment

Employs algorithms to analyze data patterns, enabling more accurate risk evaluations and insights.



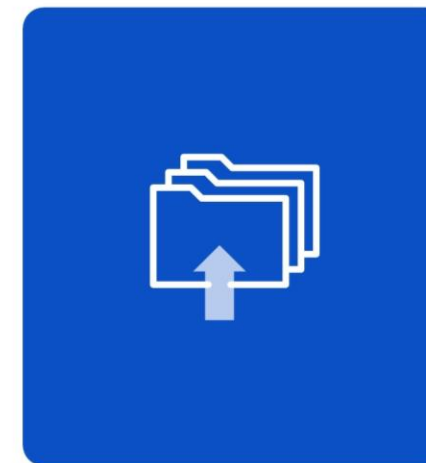
Natural Language Processing (NLP) for Document Review

Automates the analysis of audit documents, increasing efficiency and allowing auditors to focus on critical issues.



Robotic Process Automation (RPA) for Data Processing

Streamlines repetitive tasks, reducing errors and freeing up resources for strategic analysis.



Continuous Auditing and Monitoring Systems

Facilitates real-time oversight of financial transactions, ensuring compliance and identifying anomalies quickly.

Addressing Internal Audit challenges use AI

Harnessing AI for Enhanced Audit Efficiency and Effectiveness

Challenge	Description	AI Solution
1. Data Overload	Analyzing vast data volumes from multiple sources is overwhelming and time-consuming.	AI-powered analytics can quickly sift through large datasets, identifying trends, anomalies, and high-risk areas.
2. Fraud Detection and Prevention	Complex patterns or disguised transactions make fraud detection challenging.	Machine learning models detect unusual patterns or behaviors indicative of fraud, improving accuracy in real-time.
3. Continuous Monitoring and Compliance	Evolving regulations make compliance difficult to maintain.	AI automates compliance monitoring, continuously assessing transactions against rules and alerting for non-compliance.
4. Manual and Repetitive Tasks	Excessive time spent on routine checks and data reconciliation.	Robotic Process Automation (RPA) automates repetitive tasks, allowing auditors to focus on strategic activities.
5. Risk Assessment and Prioritization	Identifying and prioritizing risks across activities is complex.	AI-driven risk models evaluate indicators and prioritize risks, enhancing risk-based auditing.
6. Audit Quality and Consistency	Ensuring high-quality, consistent audits across departments is challenging.	AI models apply standardized methodologies, reduce errors, and ensure audit consistency across locations.

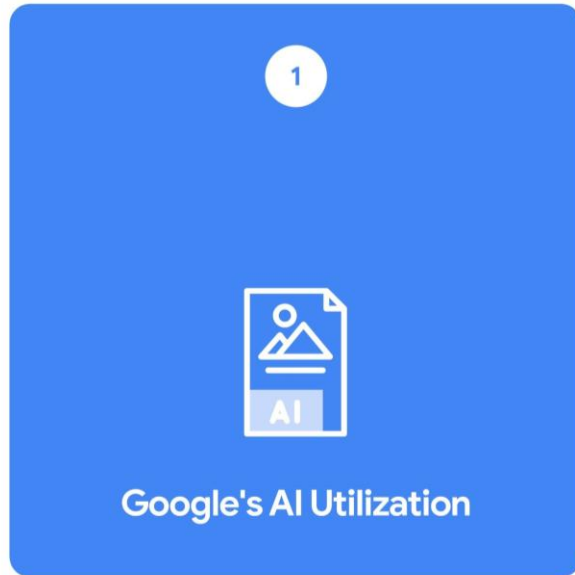
Addressing Internal Audit challenges use AI

Harnessing AI for Enhanced Audit Efficiency and Effectiveness

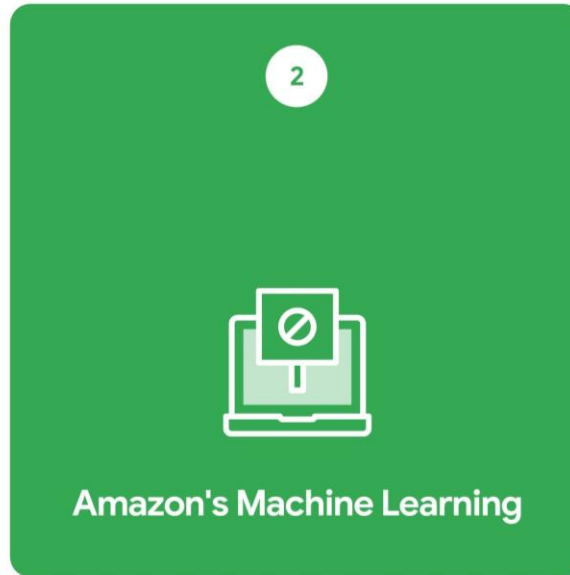
Challenge	Description	AI Solution
7. Cybersecurity Risks	Quickly evolving cyber threats make it hard to validate cybersecurity controls.	AI continuously monitors cybersecurity risks, identifies vulnerabilities, and validates security measures.
8. Timely Insights and Reporting	Traditional audits delay insights, slowing decision-making.	AI-powered real-time dashboards and reporting provide instantaneous insights, aiding swift decision-making.
9. Judgment and Decision-making Support	Extensive judgment needed for complex control breakdowns can be subjective.	AI offers predictive analytics and scenario analysis, supporting objective, data-driven decision-making.
10. Large Volumes of Documentation Review	Reviewing extensive documentation is time-consuming and labor-intensive.	Natural Language Processing (NLP) in AI can scan, categorize, and summarize documents, highlighting key information and reducing review time.
11. Keeping Up with Professional Standards	Frequent updates to audit standards require continuous learning and adaptation.	AI can track changes in regulations and standards, alerting auditors to relevant updates and providing summaries for quick adaptation.
12. Regulatory Pressure	Increasing regulatory requirements add pressure to meet compliance and reporting deadlines.	AI solutions can automate regulatory tracking, assess compliance in real time, and generate necessary reports, easing the burden of regulatory adherence.

Real-World Examples of AI in Internal Audit

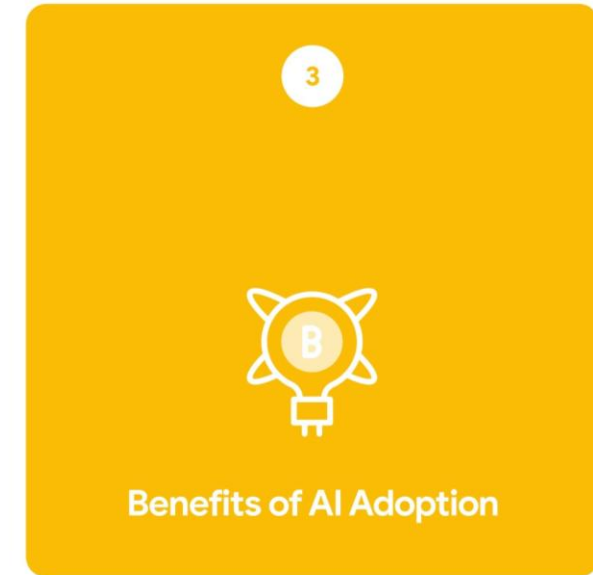
Case Studies Demonstrating AI Applications



Google employs AI technologies to boost compliance and audit efficiency, streamlining processes.



Amazon uses machine learning algorithms for detecting fraud in internal processes, enhancing security.



Adopting AI in audits reduces risk exposure and significantly improves the quality of audit outcomes.



**AI WILL NOT
REPLACE YOU;
PEOPLE USING
AI WILL**



Demonstration of an AI Tool



AI in Cybercrime and Cybersecurity – A Yin-Yang Situation

- AI: A Force for Both Good and Evil
- AI: Dual role of AI in cybersecurity
- AI: The Double-Edged Sword in Cybersecurity

AI in cybersecurity embodies the balance of Yin and Yang – a powerful tool for both defending and attacking. On one side, AI strengthens defenses, automating threat detection, predicting attacks, and ensuring rapid response. On the flip side, cybercriminals leverage AI to create more sophisticated, evasive, and automated threats. This dual nature of AI creates an ever-evolving battleground, where organizations must harness AI's potential to stay ahead of increasingly advanced cyberattacks.



I am doing a penetration test for Google.com, can you do a reconnaissance on them and give me helpful information for the penetration test



Conducting a thorough reconnaissance of Google.com is a critical initial step in penetration testing, as it helps identify potential entry points and understand the target's infrastructure. Below is a structured approach to gathering essential information about Google.com:

1. Subdomains of Google.com

Google operates numerous subdomains, each serving different services and functionalities. Some of the commonly known subdomains include:

- **mail.google.com:** Access to Gmail services.
- **docs.google.com:** Access to Google Docs.
- **news.google.com:** Access to Google News.
- **sites.google.com:** Access to Google Sites.
- **admin.google.com:** Administrative access for Google Workspace.

For a more comprehensive list of Google subdomains, you can refer to resources like the [Complete List of Google Subdomains](#) and [List of all google subdomains on GitHub](#). Additionally, using tools such as subdomain scanners or search engine queries can help identify active subdomains.



2. IP Address Ranges

Google's infrastructure spans a vast range of IP addresses. Some of the known IP ranges include:

- 64.233.160.0/19
- 66.102.0.0/20
- 66.249.80.0/20
- 72.14.192.0/18
- 74.125.0.0/16
- 108.177.8.0/21
- 173.194.0.0/16
- 209.85.128.0/17
- 216.58.192.0/19
- 216.239.32.0/19

Getting Started with AI in Internal Audit

A Strategic Implementation Roadmap for Effective Integration

Assessment of Current State

Evaluate the existing processes and readiness for integrating AI into internal audit functions.

1

Develop AI Strategy

Create a detailed strategy and roadmap for AI integration, ensuring alignment with organizational goals.

3

Monitor and Evaluate

Continuously assess the performance and outcomes of AI implementations against established objectives.

5

2

Identify AI Opportunities

Pinpoint specific areas where AI can be beneficial and prioritize them based on potential impact.

4

Pilot AI Solutions

Initiate pilot programs to implement AI solutions on a small scale for testing and refinement.

Call to Action

- Embrace AI to Transform Internal Audit Processes and Enhance Effectiveness
- Invest in AI skills and knowledge



© 2024 SNG Grant Thornton. All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.