IIA's Artificial Intelligence Auditing Framework

Fandhy Haristha S,
CIA, CRMA, CCSA, CISA, CISM, CRISC, CGEIT, GRCP, GRCA, CISSP, CEH, CEP-PM, QIA, COBIT5

Agenda

AI Introduction

AI in Real World

IIA AI Auditing Framework

Additional: Machine Learning for Auditing

1	2	3	4	5
Enforcement spreads geographically	Societal action vs unenforced regulation	Automated & preventative compliance	Societies become increasingly cashless	Ethical & transparent businesses

1. $1trillion is paid each year in bribery globally, and $2.6 trillion is lost to corruption, (5% of the global GDP). PwC report 2017
2. More than one in three (36%) organisations experienced economic crime. PwC report
3. Only 50% of respondents globally are using specialist monitoring software to identify fraud risks. EY global fraud survey 2016

2020-2021

1996-1997

2011

AI is not new. The idea of AI dates back to 1950 when Alan Turing first proposed that a machine could communicate well enough to convince a human evaluator that it, too, was human.

4

Agenda

AI Introduction

AI in Real World

IIA AI Auditing Framework

Additional: Machine Learning for Auditing

3 Vs of Big Data

Volume: The amount of data being created is vast compared to traditional data sources

Variety: Data comes from all types of formats. This can include data generated within an organization as well as data created from external sources, including publicly available data.

Velocity: Data is being generated extremely quickly and continuously.
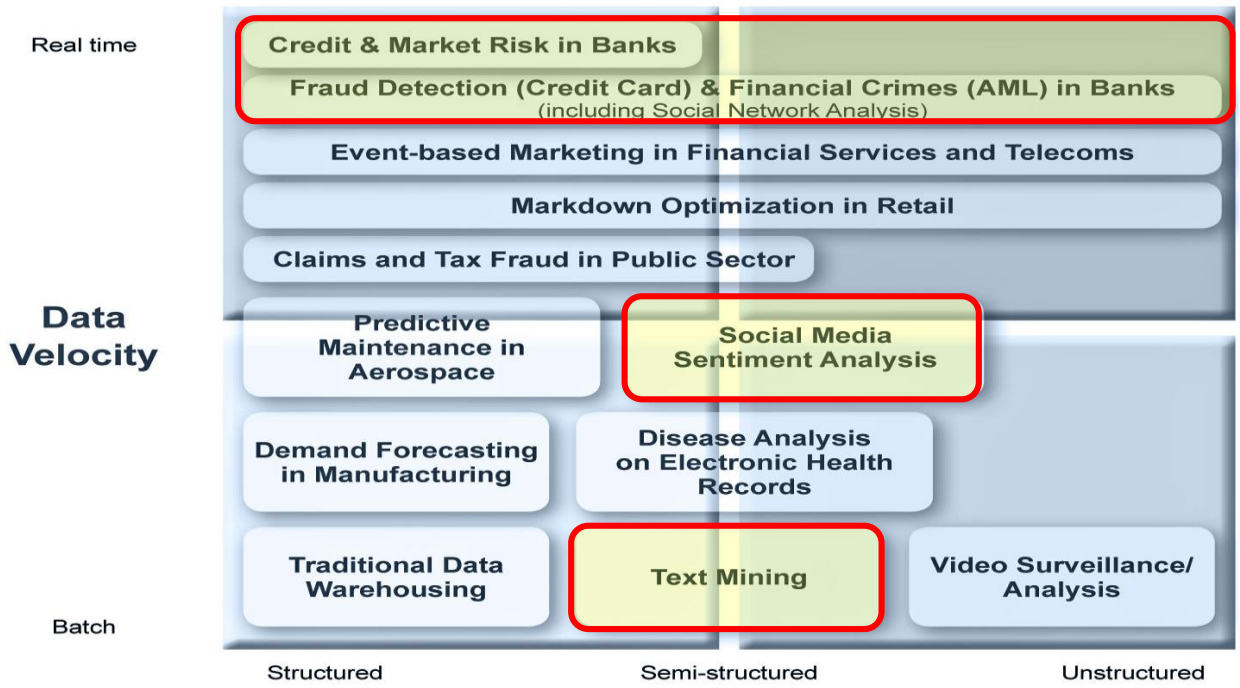
Additional Vs

Veracity: Data must be able to be verified based on both accuracy and context.
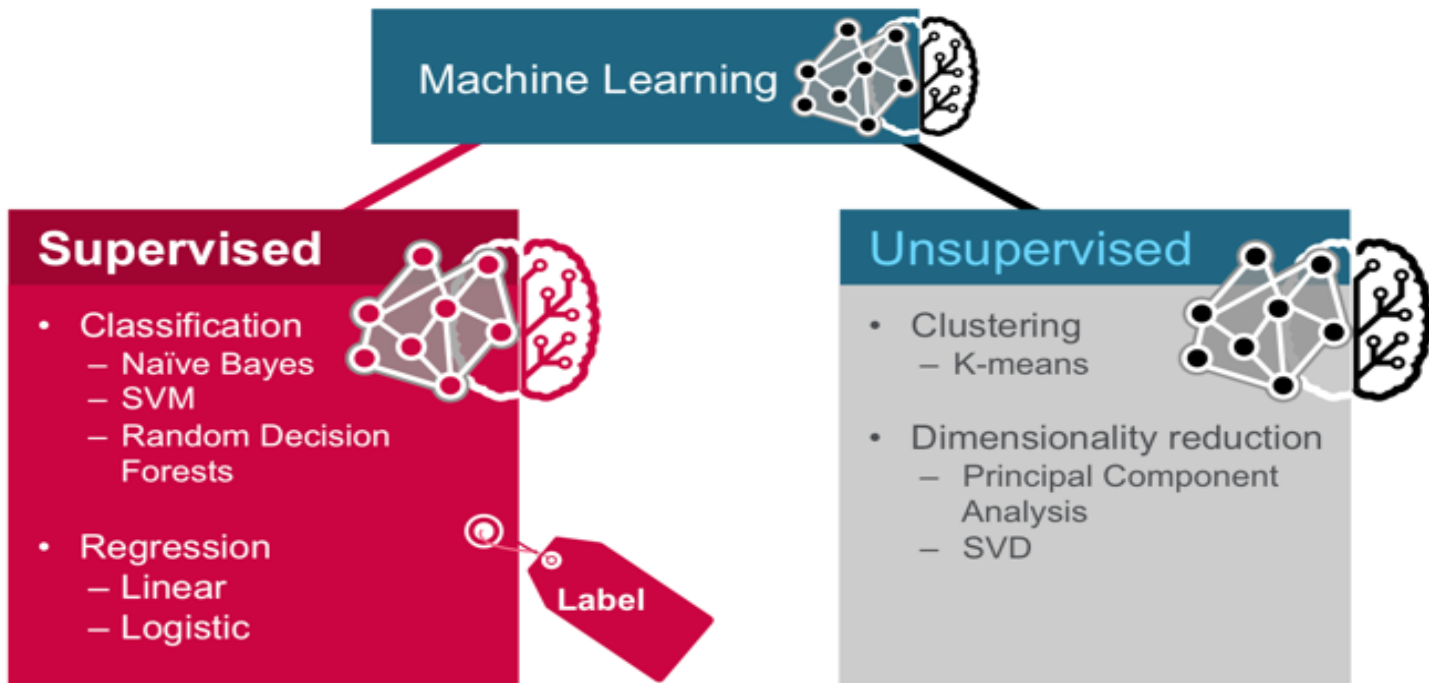
Variability: Big data is extremely variable and always changing.

Visualization: Analytic results from big data are often hard to interpret; therefore, translating vast amounts of data into readily presentable graphics and charts that are easy to understand is critical to end-user satisfaction and may highlight additional insights.

Value: Organizations, societies, and consumers can all benefit from big data. Value is generated when new insights are translated into actions that create positive outcomes.
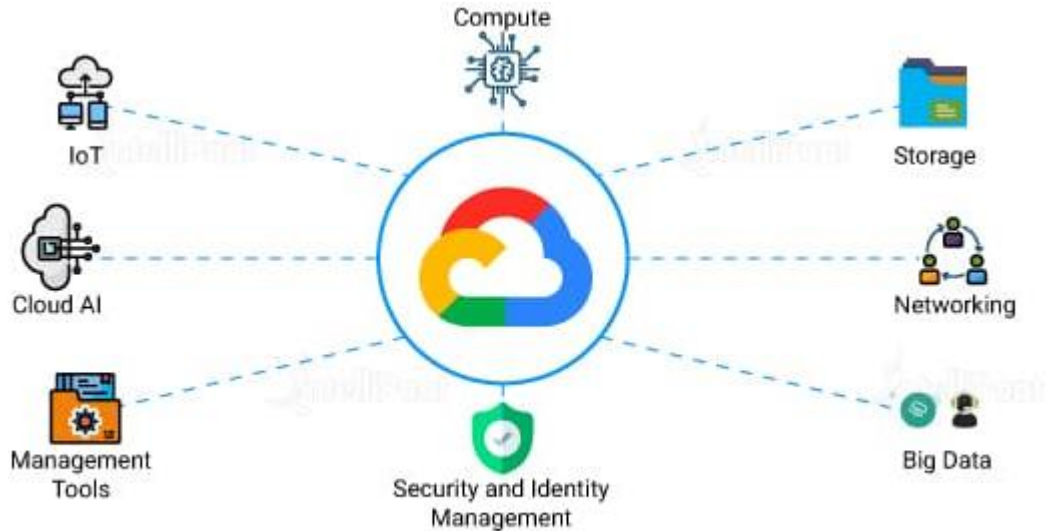
Source: Understanding and Auditing Big Data, Global Technology Audit Guide (GTAG), IIA

Potential Use Cases for Big Data Analytics

Source: SAS & IDC

Source: Carol McDonald, Demystifying AI, Machine Learning and Deep Learning, MAPR.com
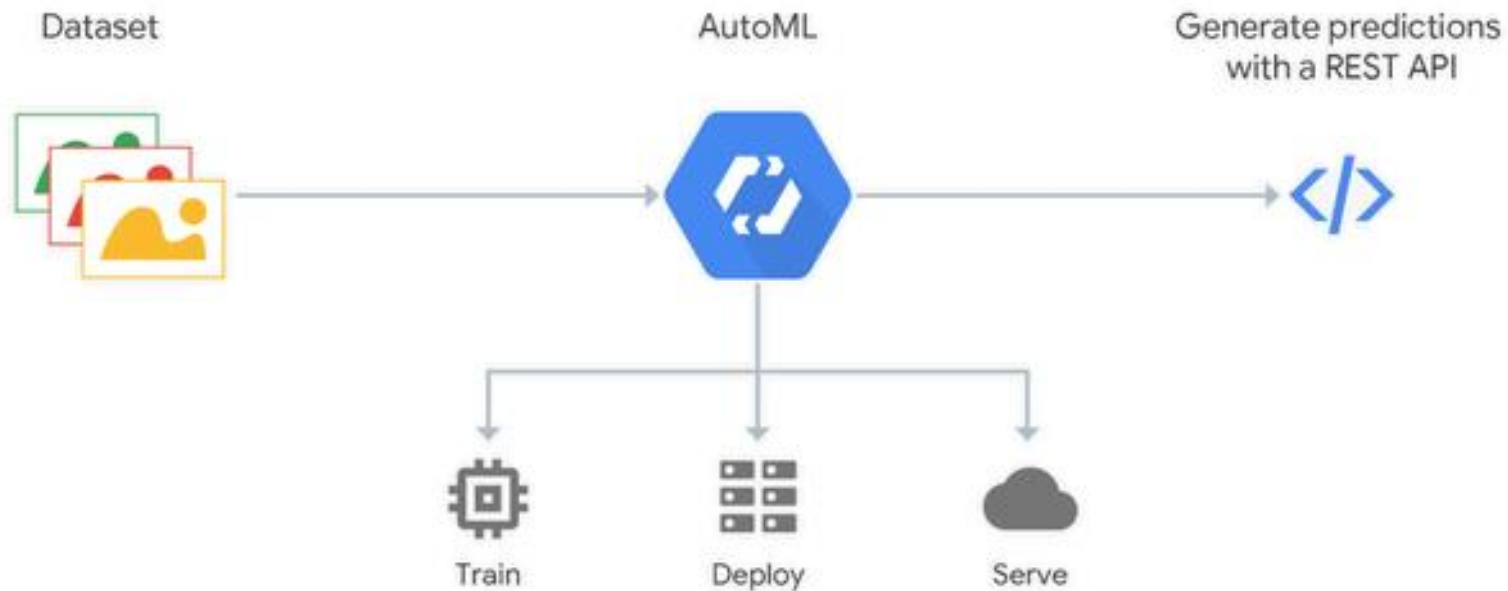
Google AutoML (Auto Machine Learning) memungkinkan kita melakukan analisa, train, dan permodelan atas berbasis cloud data/big data dalam melakukan aktifitas tertentu s ehingga berdasarkan karakteristik pada data tersebut kita bisa membuat prediksi
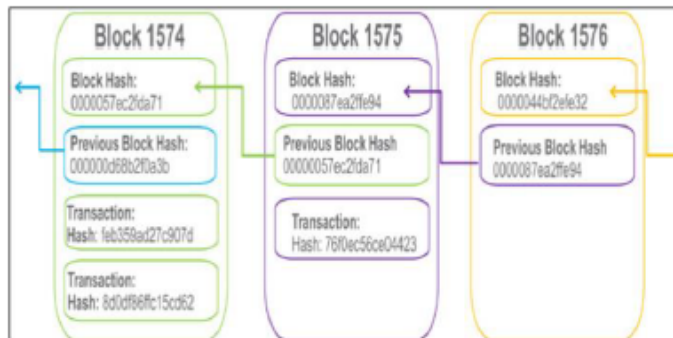
Source: Google

Dataset — AutoML — Generate predictions with a REST API

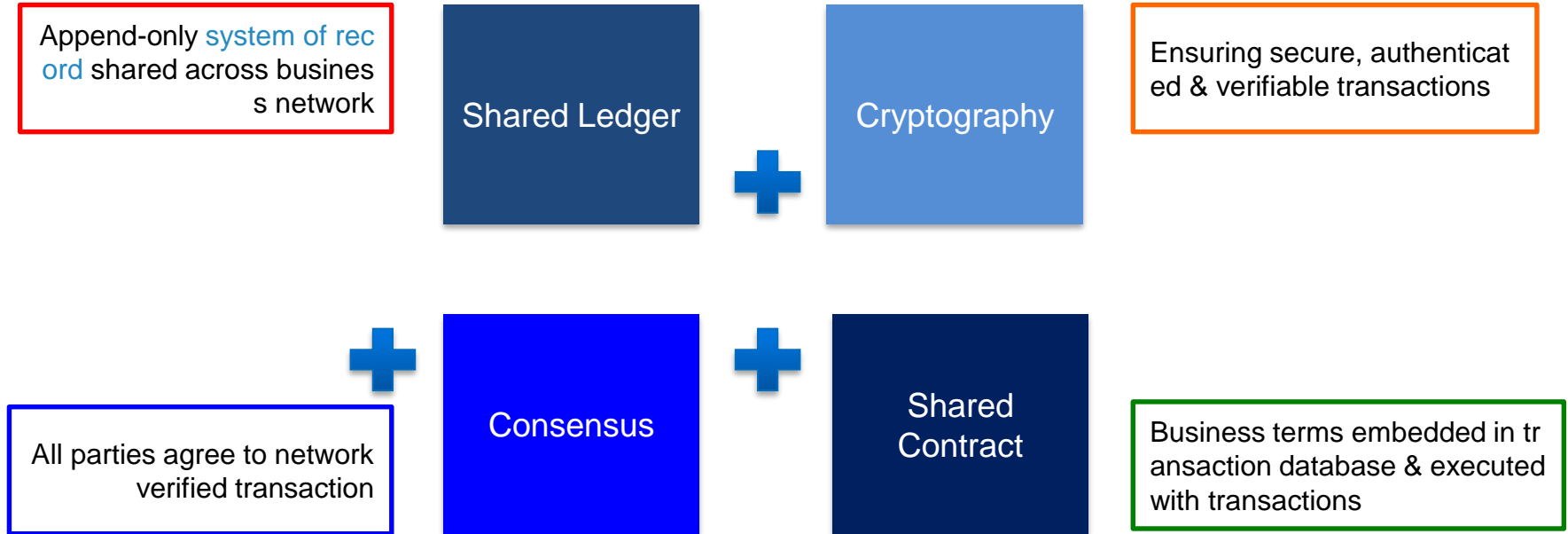Train   Deploy   Serve

Source: Google

10

Blockchain is an algorithm and a distributed data structure for managing data without a central administrator among people who know nothing about one another. Originally designed for the crypto-currency Bitcoin, the blockchain architecture was driven by a rejection of money and bank-controlled payments.

- Blockchain owes its name to the way it stores transaction data — in blocks that are linked together to form a chain (**Shown in Figure**). As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed on by the network participants.
- Each block contains a hash (a digital fingerprint or unique identifier), timestamped batches of recent valid transactions, and the hash of the previous block.
- The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain.
- The method renders the blockchain tamper-evident, lending to the key attribute of immutability (explained in the next slide).

Block 1574	Block 1575	Block 1576
Block Hash: 0000057ec2fda71	Block Hash: 0000087ea2ffe94	Block Hash: 0000044bf2efe32
Previous Block Hash: 000000d68b2f0a3b	Previous Block Hash 00000057ec2fda71	Previous Block Hash 0000087ea2ffe94
Transaction: Hash: feb359ad27c907d	Transaction: Hash: 76f0ec56ce04423	
Transaction: Hash: 8d0df86ffc15cd62		

Blockchain in a nutshell

Append-only system of record shared across busines s network

Shared Ledger + **Cryptography**

Ensuring secure, authenticat ed & verifiable transactions

All parties agree to network verified transaction

+ **Consensus** + **Shared Contract**

Business terms embedded in tr ansaction database & executed with transactions

Broader participation, lower cost, increased efficiency

Source: Lets talk Payments, IBM Blockchain 2015

o Improving quality of Audit

o Frequency of Audit

o Entire population of data instead of a random sample

o Avoiding misstatement

o Faster audit

o Ability for Real-time fraud monitoring and detection

o Deep learning focused on finding anomalies

Consensus

For a transaction to be valid, all participants must agree on its validity.

Provenance

Participants know where the asset came from and how its ownership has changed over time.

Immutability

No participant can tamper with a transaction after it's been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible.

Finality

A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

Source: IIA International Conference 2018

2015

Exploration & Investment

- Initial capability & use case assessments
- Early adoption likely for internal reconciliation

2016–2017

Early Adoption

- Leading-edge banks see the value of blockchain and begin deployments for asset classes that are bilaterally traded and/or have no central clearing authority
- Regulatory certainty drives adoption for external uses
- Regulatory authorities realize the benefits of blockchain for auditing and compliance, and rule-making begins

2018–2024

Growth

- Banks begin to see the benefits accorded to early adopters and – combined with regulatory guidance and certainty – the network effect takes hold
- New service providers and models emerge
- Deployments go viral across numerous asset classes
- New products and services are created; incumbent processes and services are discarded

2025

Maturity

- Blockchain adoption is considered mainstream and integral to the capital markets ecosystem

Source: Accenture Research

➢ RPA is not a **physical "robot" but a configurable software**, that **sits on top of a company's existing IT infrastructure**, pulling data, performing algorithms, and creating reports.

➢ The "robot" is configured to complete the same process steps, follow the **business rules**, and **use the same systems that a human does** today.

➢ RPA makes the most significant impact on **manual work processes**, that are **repetitive and recurring**, and often have **high human error rates**.

➢ A single "robot" can be configured to performed a variety of processes enabling **multi-use** robots, and **variability as your business needs change**.

➢ The initial implementation of RPA can happen in weeks and typically delivers an **ROI of greater than 5:1**, often recouping the investment in the first year.

Example of Bank Reconciliation using RPA

Treasury

START → Save monthly Bank Statement to G:\

RPA Bot

Searches email folder for new statement → Opens and reads statement data → Extracts statements data online from the banks website

Opens previous months "Recap file" → Date the mode of receiving statement

Statement received? — No → Check for any bank activity for previous month → Any activity? — No → Mark & date as "No Activity" → STOP

Any activity? — Yes → Follow-up with treasury / online

Statement received? — Yes → Look-up a/c# electronic statement with a/c# on recap sheet → Input region #, district# & district name on electronic statement → Mark and place statements in respective files by regions (30)

Lookup date range for the month → Reconcile statement with FIN → Does it reconcile? — Yes → Change status to 'finalize', date and initial "RPA" → STOP

Does it reconcile? — No

FIN Team

Determine reason for missing entry → Entry found? → Call office to gather missing inputs

- Zero balance transfer
- Journal entry
- Verify deposit
- Bank activity

→ Change status to 'finalize', date and initial "Person"

www.rgp.com

17

Source: RGP – RPA The Impact on Internal Audit

Agenda

AI Introduction

AI in Real World

IIA AI Auditing Framework

Additional: Machine Learning for Auditing

GLOBAL PERSPECTIVES AND INSIGHTS

The IIA's Artificial Intelligence Auditing Framework

Practical Applications, Part A

Special Edition

The Institute of Internal Auditors | Global
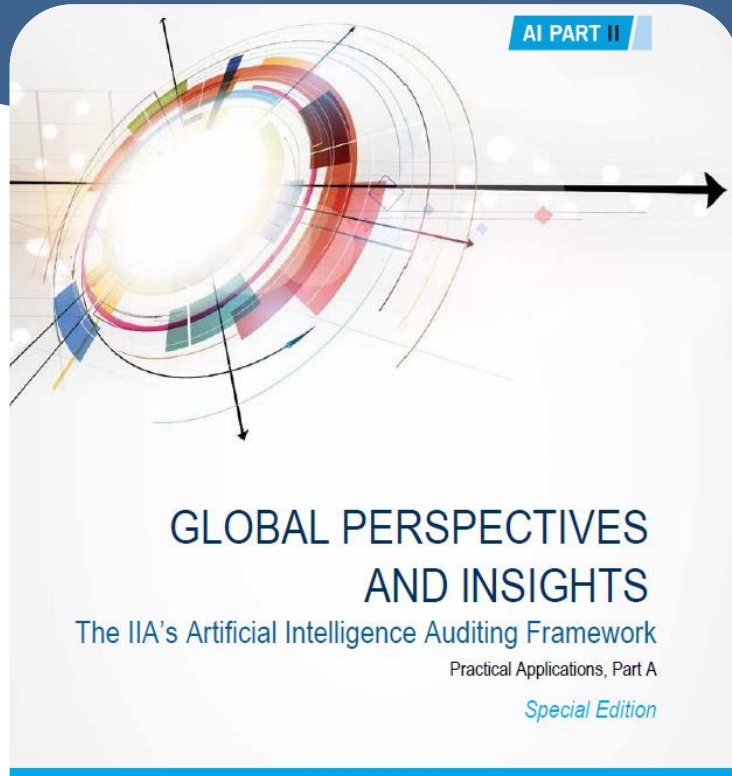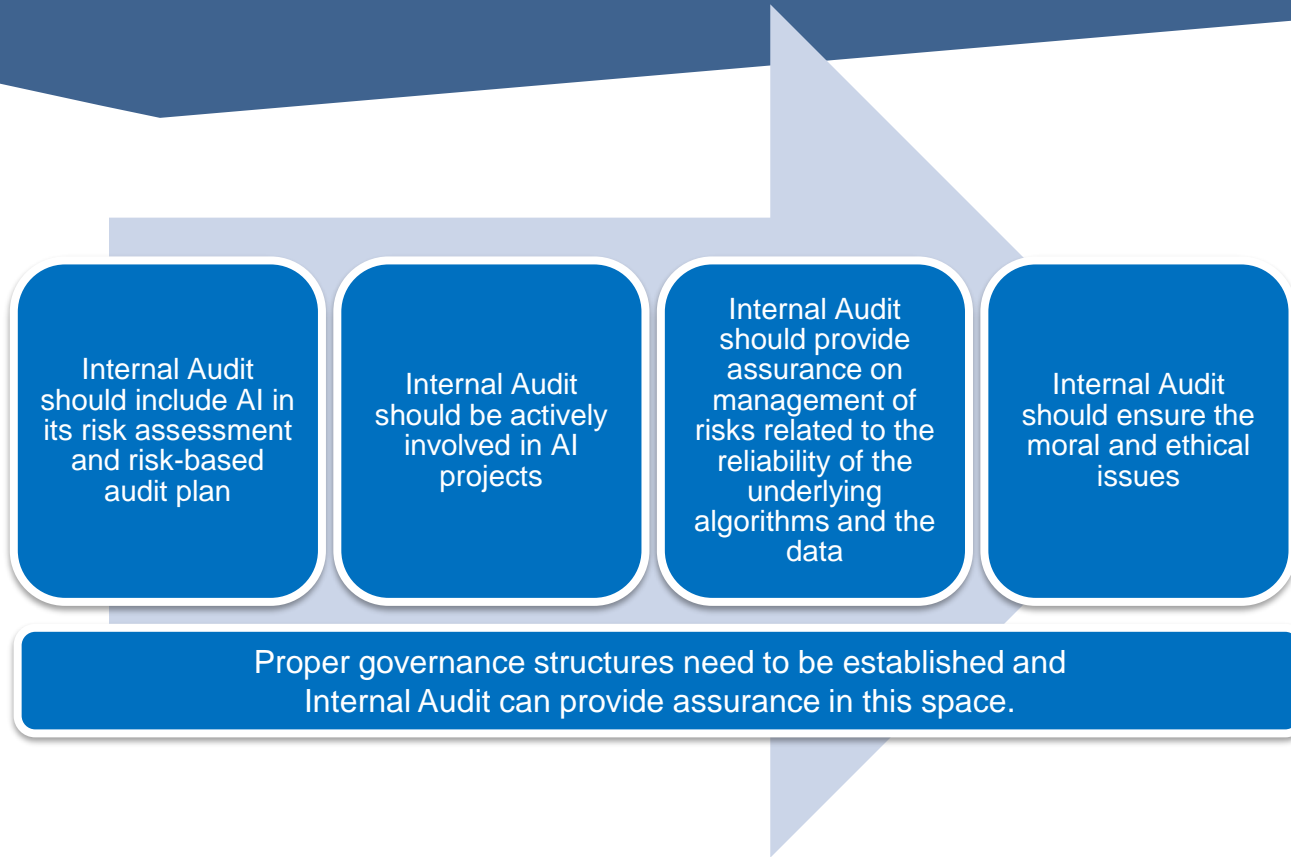
Internal audit's role in AI is to "help an organization evaluate, understand, and communicate the degree to which artificial intelligence will have an effect (negative or positive) on the organization's ability to create value in the short, medium, or long term."
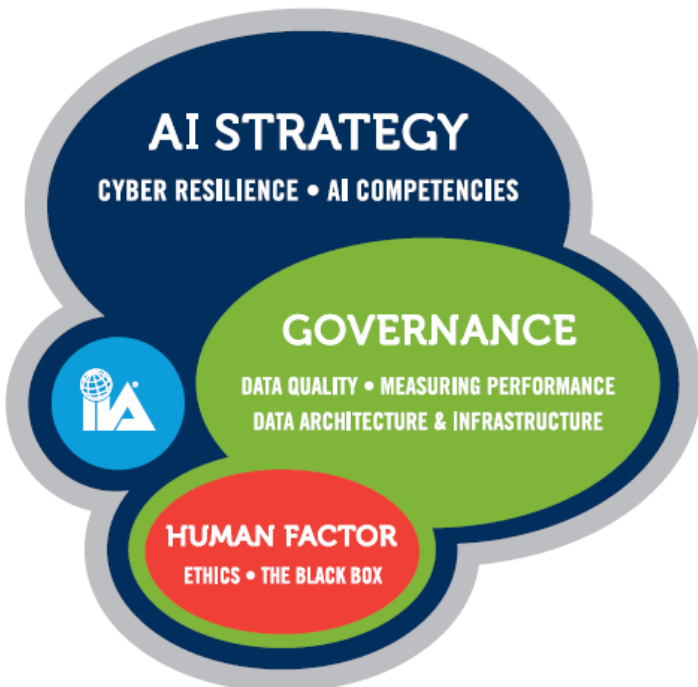
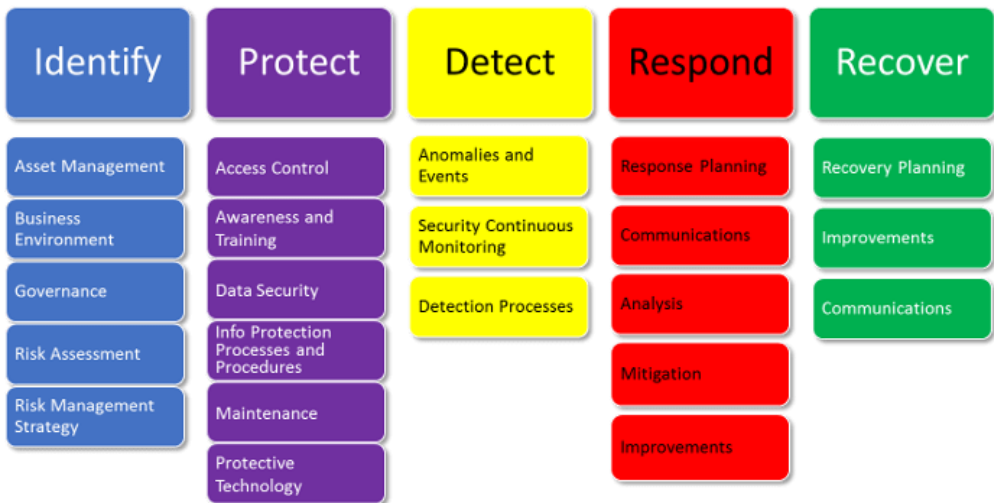The IIA's AI Auditing Framework in providing AI-related advisory, assurance, or blended advisory/assurance services as appropriate to the organization. The Framework comprises three overarching components — AI Strategy, Governance, and the Human Factor — and seven elements: Cyber Resilience; AI Competencies; Data Quality; Data Architecture & Infrastructure; Measuring Performance; Ethics; and The Black Box.

20

Internal Audit should include AI in its risk assessment and risk-based audit plan

Internal Audit should be actively involved in AI projects

Internal Audit should provide assurance on management of risks related to the reliability of the underlying algorithms and the data

Internal Audit should ensure the moral and ethical issues

Proper governance structures need to be established and Internal Audit can provide assurance in this space.

- An organization's AI strategy might be an obvious extension of the organization's overall digital or big data strategy.
- The AI strategy should clearly articulate the intended result of AI activities.
- The AI strategies should be developed collaboratively between the organization's business leaders who can articulate the intended result of AI activities
- Both business leaders and technology professionals also need to be involved in managing the execution of the AI strategy.

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

- The organization's ability to resist, react to, and recover from cyberattacks, including the intentional misuse of an organization's AI technologies for nefarious means, is becoming increasingly important.
- CAEs need to rapidly build cybersecurity competencies within their teams, continuously monitor AI/cybersecurity risks, and communicate to executive management and the board the level of risk to the organization and efforts to address such risk.

23

- Know how AI works.
- Understand the risks and opportunities AI presents.
- Determine whether AI outcomes are as expected.
- Be capable of recommending or taking corrective action if needed.

Such competencies will be needed within internal audit and among the first and second lines of defense.

Relevant AI Strategy Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Be actively involved in AI projects from their beginnings, providing advice and insight contributing to successful implementation.	**Attend** AI project team meetings.
The organization has a defined AI strategy.	**Determine** whether an AI strategy has been documented and if so, **verify** that the strategy: ■ Articulates the intended results of AI activities (strategic objectives). ■ Articulates at a high level how the AI objectives will be accomplished (strategic plan).
Provide assurance over the readiness and response to cyber threats.	**Leveraging** an established cybersecurity framework, **work** collaboratively with IT and other parties to ensure effective defenses and responses are in place.
There are sufficient resources (staff and budget) to implement the AI strategy.	**Review** process for determining staff and budget needs to support AI.
Advise on whether the strategy adequately considers AI threats and opportunities.	**Review** any existing assessments of AI threats and opportunities. If no assessments exist, **make recommendations** for moving forward (how the organization could plan to identify AI threats and opportunities).

AI governance refers to the structures, processes, and procedures implemented to direct, manage, and monitor the AI activities of the organization, that:

1. Establishes accountability, responsibility, and oversight.
2. Helps to ensure that those with AI responsibilities have the necessary skills and expertise.
3. Helps to ensure that AI activities and AI-related decisions and actions are consistent with the organization's values, and ethical, social, and legal responsibilities.

26

Relevant AI Governance Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Provide assurance that AI governance structures have been established, documented, and are working as designed.	**Review** business models and organizational structure; **determine** if business models and organizational structure reflect the organization's AI strategy. **Review** AI policies and procedures; **determine** whether organizational policies and procedures clearly identify AI roles and responsibilities related to AI strategy, governance, data architecture, data quality, ethical imperatives, and measuring performance.
Assess whether those with AI responsibilities have the necessary competencies to be successful. For example, those responsible for ethical imperatives should be competent in assessing the ethical behavior of those who provide human input into the AI, and should be independent of the AI activity.	**Interview** those with AI responsibilities. **Review** AI job descriptions, requisite skills, etc., and **verify** whether those responsible have their stated qualifications.
Provide assurance that AI policies and procedures have been established and documented.	**Review** AI policies and procedures and **determine** if they sufficiently address AI risks. **Determine** if policies and procedures provide for periodic "what if" analysis or scenario planning.

Relevant AI Governance Objectives and Activities or Procedures

Assess whether those with AI responsibilities have the necessary competencies to be successful. For example, those responsible for ethical imperatives should be competent in assessing the ethical behavior of those who provide human input into the AI, and should be independent of the AI activity.	**Interview** those with AI responsibilities. **Review** AI job descriptions, requisite skills, etc., and **verify** whether those responsible have their stated qualifications.
Provide assurance that AI policies and procedures have been established and documented.	**Review** AI policies and procedures and **determine** if they sufficiently address AI risks. **Determine** if policies and procedures provide for periodic "what if" analysis or scenario planning.
Provide assurance that AI activity audit trails provide sufficient information to understand what AI decisions were made, and why.	**Review** AI audit trails. **Determine** whether audit trails provide sufficient information to understand what decisions were made, and why.
Provide assurance that policies and procedures have been implemented and are working as designed, and that employees are compliant.	**Observe** employees implementing AI procedures. **Review** helpline/hotline reports and **follow up** on any reports alleging noncompliant or malicious activities related to AI. **Interview** a random sample of employees and **determine** if they are knowledgeable about AI policies and procedures. **Identify** and **review** AI access policies and procedures. **Evaluate** access policies and **test** access controls. **Assess** whether regulatory control objectives reflect emerging regulations, standards, and guidance.

28

Relevant AI Governance Objectives and Activities or Procedures

Assess whether those with AI responsibilities have the necessary competencies to be successful. For example, those responsible for ethical imperatives should be competent in assessing the ethical behavior of those who provide human input into the AI, and should be independent of the AI activity.	**Interview** those with AI responsibilities. **Review** AI job descriptions, requisite skills, etc., and **verify** whether those responsible have their stated qualifications.
Provide assurance that AI policies and procedures have been established and documented.	**Review** AI policies and procedures and **determine** if they sufficiently address AI risks. **Determine** if policies and procedures provide for periodic "what if" analysis or scenario planning.
Provide assurance that AI activity audit trails provide sufficient information to understand what AI decisions were made, and why.	**Review** AI audit trails. **Determine** whether audit trails provide sufficient information to understand what decisions were made, and why.
Provide assurance that policies and procedures have been implemented and are working as designed, and that employees are compliant.	**Observe** employees implementing AI procedures. **Review** helpline/hotline reports and **follow up** on any reports alleging noncompliant or malicious activities related to AI. **Interview** a random sample of employees and **determine** if they are knowledgeable about AI policies and procedures. **Identify** and **review** AI access policies and procedures. **Evaluate** access policies and **test** access controls. **Assess** whether regulatory control objectives reflect emerging regulations, standards, and guidance.

Data Architecture & Infrastructure

Three major areas of software development to ensure the success of AI integration:

- **Data integration** — data from multiple sources must be integrated before AI can be incorporated into the organization's applications and systems.
- **Application modernization** — software updates will need to be made on a regular basis. Frequent, less intensive updates should replace infrequent, more intensive updates that slow down or disrupt systems.
- **Employee education** — software developers, project managers, and other technology staff need to keep up with machine learning and every aspect of the technology "stack" (the software and components that run AI).

The way that data is accessible

Information privacy and security

Roles and responsibilities for data ownership and use

Relevant Data Architecture & Infrastructure Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Provide assurance that the organization is cyber resilient. Cyber resilience includes, but is broader than, cybersecurity alone. Cyber resilience encompasses security (resistance), reaction, and recovery.	**Understand** and audit big data (see The IIA's Practice Guide: Understanding and Auditing Big Data). **Assess** whether the organization is preparing for compliance with new technology regulations, such as the EU's General Data Protection Regulation (GDPR). **Assess** whether the organization's disaster recovery protocols include AI failures, including the breakdown of controls that maintain the rules set forth by AI governance.
Provide assurance that the data infrastructure has the capacity to accommodate the size and complexity of AI activity set forth in the AI strategy.	**Assess** whether the infrastructure is capable of handling structured and unstructured data.
Provide assurance that the organization has established a data taxonomy. **Evaluate** the quality, completeness, and consistency of use for the enterprisewide data taxonomy.	**Assess** whether the taxonomy is robust enough to accommodate the size and complexity of AI activities.

Understanding and Auditing Big Data

- The completeness, accuracy, and reliability of the data on which AI algorithms are built are critical.
- For AI to be successful, organizations need access to vast amounts of high quality data — data that is well-defined and in standardized formats.
- Often, systems do not communicate with each other or do so through complicated add-ons or customizations. How this data is reconciled, synthesized, and validated is also critical

Relevant Data Quality Objectives and Activities or Procedures

| Engagement or Control Objective(s)	Activities or Procedures
Provide assurance over the reliability of AI's underlying algorithms and the data on which algorithms are based.	**Obtain** a sample of the raw data that are inputs to AI. **Verify** that the organization has implemented methodologies to validate AI outcomes with actual, real-world outcomes, and that policies and procedures are in place to continuously measure, monitor, escalate, and rectify inconsistencies between the two.
Provide assurance that data input is reconciled and normalized to maximize accuracy.	**Verify** that the organization has policies and procedures in place to continuously measure, monitor, escalate, and rectify data accuracy and integrity issues. **Confirm** that the organization is consistently following and monitoring a formalized data reconciliation framework, which includes a rationale for differing methodologies and results should they exist.
Provide assurance that aggregated data is complete.	**Verify** that the organization has policies and procedures in place to limit data input bias.
Provide assurance that the completeness of data is measured and monitored and that any material exceptions that impact decision-making are identified and explained. This should be done whether the exceptions are determined by humans or AI.	**Review** AI metrics and metric reports. **Assess** whether those responsible for decision-making have received and considered explanations on material exceptions related to data quality.

33

HOW AI IS BEING USED FOR ADVERTISING

1 Facebook takes personal information about users

2 Facebook feeds this data into "FBLearner Flow," its name for an internal machine learning tool

3 FBLearner Flow runs a branching "decision tree" simulation that can be used to predict outcomes, such as consumer behaviors
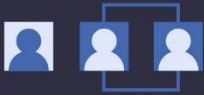
4 Facebook takes the results from FBLearner Flow and packages them into a group of people expected to behave similarly

5 Facebook provides corporations with the ability to target these individuals with advertisements on the basis of either preventing or reinforcing this predicted outcome

The Intercept_

Facebook's Corrective Actions

Facebook's challenges with AI have been widely reported. The behemoth social network has been under scrutiny over how its algorithm-fueled technologies have been used — or misused — for malicious means.

Timeline of Major Concerns:

- In Fall 2016, ProPublica reported that advertisers could use Facebook's ad-targeting tools to exclude certain races — a potential violation of federal housing and civil rights regulations.

- In September 2017:
  - Facebook disclosed that holders of fake accounts based in Russia purchased sizeable ads on divisive issues leading up to the 2016 presidential election.
  - ProPublica reported that Facebook's ad targeting tools enabled advertisers to target self-described ethnic "haters."

- In October 2017, concerns about fake news resurfaced when Facebook (and Google) posted false information about the mass shooting in Las Vegas.

- In testimony to a Senate judiciary subcommittee in late October, Facebook said the reach of Russia-backed ads stretched much further than they had originally known, reaching as many as 126 million Americans before and during the 2016 presidential election.

34

Thank you