WGISTA
Working Group on Impact of Science and Technology on Auditing

EMERGING TECHNOLOGIES

Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

Annex-II

Quality Assurance Certificate of the Chair of the Working Group on Impact of Science and Technology on Auditing

This is to certify that ***Emerging Technologies, Applications in Developing and Maintaining Expertise within Supreme Audit Institutions (SAIs) in the Use of Science and Technology in Auditing (A Project Report)*** which is placed at level 2 of Quality Assurance as defined in the paper on "Quality Assurance on Public goods developed outside Due Process" approved by the INTOSAI Governing Board in November 2017 has been developed by following the Quality Assurance processes as detailed below:

(i) The project proposal was formulated by the Project Team, consisting of WGISTA member SAIs, including the project team Lead SAI Chile as well as SAI India, SAI Pakistan, SAI Thailand, SAI Philippines, SAI Vietnam. Approval for the project proposal was granted by the WGISTA Chair in April 2022,

(ii) The project team developed the project report based on a methodology which involved conducting bibliographic research, online research and interviews with experts,

(iii) The Exposure Draft of report received approval from the WGISTA Chair in February 2023 and was officially endorsed to the INTOSAI Knowledge Sharing Committee,

(iv) Following the protocol for QA level 2 documents; the Exposure Draft was made available for public exposure on the INTOSAI KSC Community Portal from 23rd February to 10th April, 2023,

(i) This Endorsement version has been finalized by the project team after incorporating all the comments and feedback received from WGISTA stakeholders.

The product developed is consistent with relevant INTOSAI Principles and Standards. The structure of the product is in line with the drafting convention of non-IFPP documents.

The product will be subject to review and update every two years or as deemed necessary. As this paper is not directly linked to a specific ISSAI, no expiry clause is included.

[Signature of Chair]
H.E. Humaid Obaid Abushibs
Chair of WGISTA
INTOSAI KSC

INTOSAI
Goal Chairs
Collaboration
PSC – CBC – KSC

Quality Assurance Certificate of the Chair of the Knowledge Sharing and Knowledge Services Committee

Based on the assurance provided by the **INTOSAI Working Group on Impact of Science and Technology in Auditing (WGISTA)** and the assessment by the Goal Chair, it is certified that **"Emerging Technologies, Applications in Developing and Maintaining Expertise within Supreme Audit Institutions (SAIs) in the Use of Science and Technology in Auditing (A Project Report)"** which is placed at level **2 (two)** of Quality Assurance as defined in the paper on "Quality Assurance on public goods developed outside Due Process" approved by the INTOSAI Governing Board in November 2017, has been developed by following the Quality Assurance processes as detailed in the Quality Assurance Certificate given by the Working Group Chair.

The product will be subject to review and update every two years or as deemed necessary. As this paper is not directly linked to a specific ISSAI, no expiry clause is included.

Girish Chandra Murmu
Chair of Knowledge Sharing and
Knowledge Services Committee

Preface

This report has been developed as a WGISTA (Working Group in Science and Technology) project, undertaken by the collaborative efforts of several Supreme Audit Institutions (SAIs). The objective of this project is to provide an overview of new emerging technologies that may be of use to SAIs in their pursuit of improved audit practices and effectiveness.

The WGISTA project was led by SAI Chile, with the active participation of a team of experts from SAIs around the world, each focused on different technology areas. The team members and their respective technology areas are listed below:

- Project Lead: SAI Chile
- Advanced Data Analytics: SAI India
- Robotic Process Automation: SAI Pakistan
- Artificial Intelligence: SAI Thailand
- Machine Learning: SAI Chile
- 5G: SAI Philippines
- Blockchain: SAI Vietnam

The purpose of this report is to provide SAIs with insights into the potential applications and benefits of these emerging technologies in the field of audit. It is hoped that this information will assist SAIs in making informed decisions regarding the adoption and implementation of these technologies, ultimately leading to improved audit outcomes and efficiency.

This report has been prepared in accordance with the requirements of the INTOSAI Goal Chairs and IDI - Quality Assurance Level 2. Throughout the project, great efforts have been made to ensure the accuracy, reliability and relevance of the information presented, taking into account that this is an area of very rapid development.

As per protocol, the report underwent a period of public exposure to allow stakeholders and interested parties to provide their valuable feedback and comments. We are grateful for the active engagement and contributions received during this phase. All comments received have been duly addressed by the project team in the expectation that the final report will reflect a comprehensive understanding of the subject matter.

We would like to express our sincere gratitude to all the individuals and organizations who supported and participated in this project. Their valuable contributions have greatly enriched the quality and relevance of this report.

Contents

Abbreviations

AI: Artificial Intelligence
GAO: U.S. Government Accountability Office
GIS: Geographic Information Systems
GPT-4: Fourth Generation Generative pre-trained Transformer
IIoT: Industrial Internet of Things
IoT: Internet of Things
INTOSAI: International Organization of Supreme Audit Institutions
NAO: UK's National Audit Office
ML: Machine Learning
LLM: Large Language Model
PaLM: Pathways Language Model
RPA: Robotic Process Automation
SAI: Supreme Audit Institution
SCADA: Supervisory Control and Data Acquisition
WGISTA: Working Group on Impact of Science and Technology on Auditing

Introduction

Supreme audit institutions play a vital role in ensuring government accountability and transparency. In recent years, many SAIs have shown a strong commitment to adopting emerging technologies to improve their work. This early adoption of new technologies positions SAIs at the forefront of the public sector innovation and provides them with an opportunity to shape the future of audit and governance.

While SAIs have made significant progress in adopting emerging technologies, there is still much work to be done to reach a level where they can fully capture the best practices in this area. This is an exciting time for SAIs, as they have the opportunity to experiment, learn, and lead the way in using new technologies to enhance their work.

This report summarizes the work executed during 2022 by a group of SAIs for the project to "Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing".

The referred project was formulated in the context of the Working Group on Impact of Science and Technology on Auditing (WGISTA), an entity created in 2019 by the International Organization of the Supreme Audit Institutions (INTOSAI). WGISTA is chaired by SAI UAE and vice-chaired by SAI USA with 26 members and 11 observers.

For the emerging technologies stated, the report elaborates on nine main questions, such as its definition and evolution, the organizational changes and resources required for their implementation, privacy, ethical and confidentiality issues that may arise from their design and operation and how to control them, their application to auditing and the international case studies observed, the practical obstacles that can hamper their development and the potential benefits and costs expected from their implementation.

The journey to fully realizing the benefits of emerging technologies is ongoing, but SAIs are well positioned to continue making progress. Through collaboration, learning, and innovation, SAIs can create new opportunities for improving their work, and serve as models for other public sector organizations to follow.

Chair – United Arab Emirates

Vice-chair – United States of America

SAI Chile

SAI India

SAI Pakistan

SAI Philippines

SAI Thailand

SAI Vietnam

Emerging technologies: Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

Advanced Data Analytics

INTOSAI Working Group on Impact of Science and Technology (WGISTA)
Prepared by the Office of Comptroller and Auditor General of India

Advanced Data Analytics

Basic Definition

Data analytics is the application of data science approaches to gain insights from data. It involves a sequence of steps starting from collection of data, preparing the data, and then applying various data analytic techniques to obtain relevant insights.

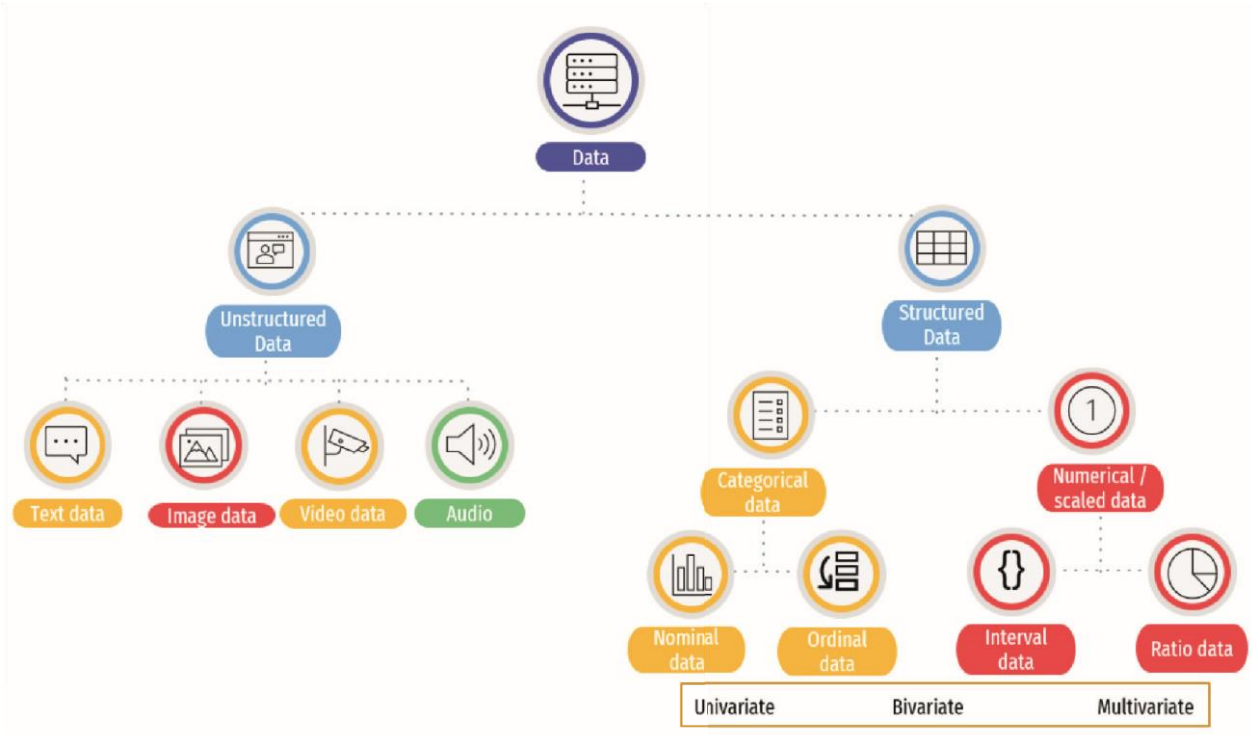
The insights include, but are not limited to:

- Trends and patterns
- Deviations
- Inconsistencies
- Exceptions
- Relationships

among data elements identified through analysis, modelling, or visualization, which can be used while planning and conducting audits.

Types of Data

The core of data analytics is 'data'. Data can be measured, collected, analysed, and visualized to provide meaningful interpretation of facts. Data can be understood and categorised as follows:



Source: Prepared by the author

Unstructured data comprises data such as text, image, audio, or video data, which cannot be readily 'tabulated' for statistical or mathematical analysis. Structured data on the other hand refers to data in tabular form. Structured data could be categorical or numerical.

Categorical data could be nominal (data not amenable to ordering, such as name, gender etc.) or ordinal (data amenable to ordering, such as rank). Numerical data could be interval data (where sum or difference between quantitative measures are possible, such as temperature data) or ratio data (where multiples of quantitative measures is possible, such as all line items of a financial statement being shown as a fraction of the turnover of a company).

Univariate data has only one variable. It is descriptive in nature. Analysis of univariate data involves summarization and identification of patterns in the data of that single variable, usually over the time dimension. Bivariate data has two variables and statistical analysis can be applied to understand the relationship between two variables using techniques such as correlation and linear regression. The data can be represented on X-Y axis and visual representations such as scatter plot are useful in understanding the relationship patterns in this type of data. Multivariate data involves multiple variables. Advanced statistical analysis such as multivariate regression would be required to analyse the data and to discover relationships and dependencies between the variables.

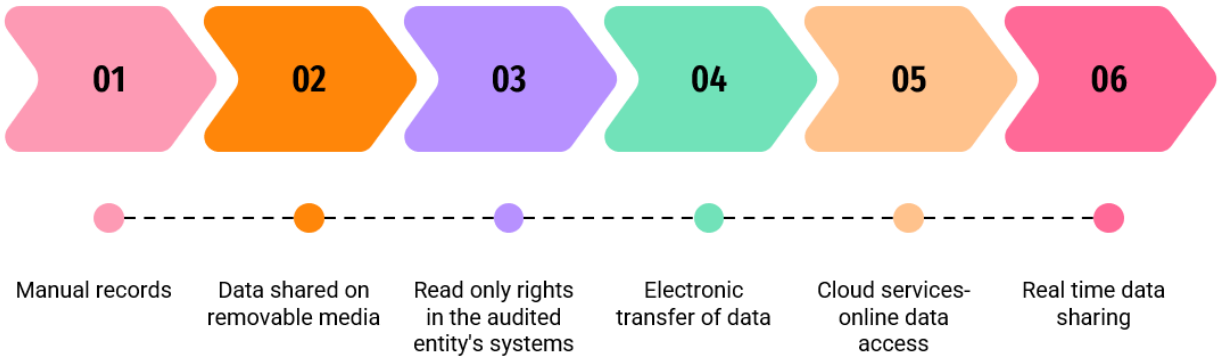
Based on the degree of complexity of the data to be analysed and the degree of sophistication of the statistical techniques required to be used, the application of data analytics in auditing has evolved from basic to advanced levels.

Evolution

Need for Data Analytics

With the increasing adoption of information systems over the previous three decades, technology has become increasingly important for obtaining audit evidence and has made IT-based auditing a necessity. This in turn has accelerated the development of computer-assisted audit techniques and tools.

The evolution of nature of documents and data maintained by the audited entities and ease of access for the auditors may be described as follows:



Source: Prepared by the author

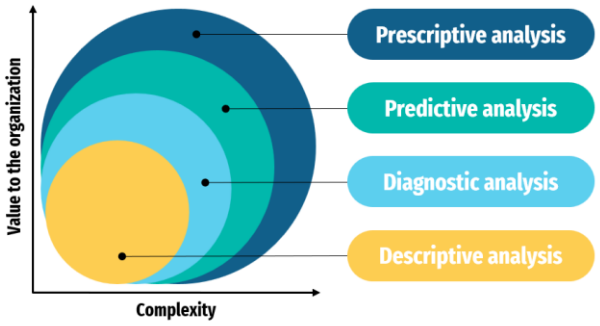
As the extent of data and documents maintained in digital form as well as the ease of access to data has increased, it has become imperative that Auditors develop the capacity to analyse the volume, velocity and the variety of real time data obtained from the audited entities. This data may originate from traditionally structured databases of Enterprise Resource Planning systems and other information systems, continuous data streams from equipment and sensors as well as unstructured data in the form of photographs, videos and audio files and free text. This kind of extensive data access provides almost limitless opportunities to the external Auditors to utilize the full spectrum of basic to advanced data analytics.

The use of Data Analytics in auditing has been discussed in recent audit literature as an effective means to improve the quality of the audit process (in the form of arriving at Audit conclusions on the basis of appropriate statistical analysis) and the audit product (through clear and meaningful visualizations). Increased audit quality is also achieved due to the shift from the use of sampling to the analysis of entire populations and/ or even including analysis of unstructured data. The use of advanced techniques for Data Analytics increases the confidence of Auditors in expressing an opinion. Apart from audit quality, the ability to access client data remotely in conjunction with standardization analytics efforts provides the possibility of achieving efficiency gains for the Audit process itself.

Differences between Basic and Advanced Data Analytics

Irrespective of degree of sophistication, all data analytics techniques are intended to help users to arrive at conclusions and make decisions based on empirical data and present the results of the data analysis in the form of clear and meaningful visualization. The distinction between Basic Data Analytics- which is also referred to as Business Intelligence in the literature- and Advance Data Analytics is mainly in the nature of objectives being addressed. While Basic Data Analytics enables Auditors to analyse mainly structured data to describe financial transactions/ status of compliance/ performance outcomes which have previously occurred at the audited entity, Advanced Data Analytics enables Auditors to analyse both structured and unstructured data to predict the quantum of financial transactions/ status of compliance/ performance outcomes that may occur at the audited entity, as well as prescribe what future actions may have to be taken by the audited entity in order to achieve desirable quantum of financial transactions/ status of compliance/ performance outcomes.

Four types of Data Analytics



Source: Prepared by the author

Advanced Data Analytics encapsulates and builds upon the scope of Basic Data Analytics.

Advanced Data Analytics techniques also involve an element of automation, in the form of enabling execution of repetitive audit checks and tests through pre-defined steps of

algorithms, rather than having to depend on a user executing such checks and tests manually. Once a series of steps is logically described in the form of an algorithm or analytical model, the dataset to be analysed may be modified a number of times and the analytics may be repeated to generated the required audit products in a reliable manner, free from any potential human errors.

The following table illustrates the key differences between Basic Data Analytics and Advanced Data Analytics.

	Basic Data Analytics or BI	Advanced Data Analytics
Orientation	Rearview	Future
Types of questions	What happened When, who, how many	What will happen? What will happen if we change this one thing? What's next?
Methods	Reporting (KPI's, metrics) Automated Monitoring/Alerting (thresholds) Dashboards Scorecards OLAP (Cubes, Slice & Dice, Drilling) Ad hoc query	Predictive Modeling Data Mining Text Mining Multimedia Mining Descriptive Modeling Statistical / Quantitative Analysis Simulation & Optimization
Big Data	Yes	Yes
Data types	Structured, some unstructured	Structured and unstructured
Knowledge Generation	Manual	Automatic
Users	Business Users	Data scientists, Business analysts, IT, Business Users
Business iniciatives	Reactive	Proactive

Source: Prepared by the author.

The range of techniques classified as Basic Data Analytics attempt to answer specific questions which the Auditors may be interested in, as users. They enable relatively simple monitoring of key metrics through Dashboards, Scorecards, Online Analytical Processing, and specific ad-hoc queries.

The range of techniques classified as Advanced Data Analytics attempt to answer broader questions which are in the nature of open-ended hypotheses which the Auditors may be interested in, as users. They enable exploratory analysis through predictive models which can consider various scenarios, perform data mining on traditional structured databases as well as on meta data associated with text, audio, video and photographic files, and invoke statistical techniques to conduct simulations and optimization exercises. These are crucial in order to achieve the objectives of data driven prediction and potential prescription by the Auditors.

Organizational changes and resources required

Vision, Structures and Processes

Formulation of Vision and Policy/ Guidelines for Data Analytics by SAI

Organizational culture is a very broad theme that has been discussed expansively in the literature. It permeates all the functions of the organization, including innovation and changes for adoption of new technologies or processes. Organizational culture has been identified as a significant factor which impacts potential resistance to changes. The main subthemes for organizational culture derived from the literature that have been found to influence technology adoption are: Vision, Strategy and organizational values.

For SAIs looking to adopt Data Analytics into their core functioning, the subtheme of Vision is important as it sets the tone at the top and provides clarity in direction and focus for the organization as a whole. The Vision statement of the SAI on Data Analytics should specifically emphasize the degree of alignment between the purpose of adoption of Data Analytics at scale, and organizational values such as professional excellence and objectivity.

The Vision of the SAI for Data Analytics should ideally be sufficiently coherent to form the basis of preparation of formal Policy/ Guidelines on this subject matter.

Congruence between the Vision and the Policy/ Guidelines, clear articulation and communication of these documents is vital in facilitating adoption of Data Analytics at scale within the SAI and overcoming possible organizational barriers or resistance to change.

Constitution of distinct organizational unit within SAI for Data Analytics

SAIs should consider constituting a distinct organizational unit which can fulfil the horizontal functional requirements related to all aspects of Data Analytics, cutting across all the verticals (Defence, Welfare, Infrastructure, Taxes etc.) for different types of audit engagements.

The organizational unit dedicated to the Data Analytics function may be entrusted with responsibility for the achievement of three objectives:

- Building capacity and developing skills for personnel within the SAI

This would involve addressing gaps in professional abilities and skills in the audit teams, related to Data Analytics. In the short term, SAIs having skilled personnel may consider in-house development of sophisticated analytical models while SAIs facing a deficit in skills may consider engagement of external professionals as per specific requirements of individual audits. But there should be a clear plan for medium and long-term capacity building through identification of the universe of skills which need to be developed within the SAIs, engagement of human resources (internal and external) who can facilitate training sessions (in-person or virtual) as well as creation of content for self-learning modules which are made available to personnel.

SAIs may also consider encouraging personnel to obtain professional certifications for skills related to Data Analytics, through suitable incentives.

- Knowledge Management and dissemination of best practices

The importance of Knowledge Management has been discussed extensively in recent literature. Knowledge Management has been defined as a process of capturing, storing, sharing and using knowledge (both tacit/ informal as well as formal/ documented) gained from the work experience of individuals and teams in the organization.

SAIs should accord high priority to effective Knowledge Management for the Data Analytics function, as it can significantly accelerate its adoption at scale within the organization. The dedicated organizational unit should:

- Establish a shared vocabulary across the organization to harvest and subsequently disseminate knowledge for the Data Analytics function, through well-defined ontology and taxonomy frameworks specific to this function.
- Identify specific and actionable best practices and techniques in the use of Data Analytics from audit engagements across the organization and disseminate them on time to personnel/ teams who are best placed to replicate/ apply them during their current work, through the Knowledge Management technology platform.
- Maintaining interfaces with academia and the corporate sector.

Such interfaces are vital, to ensure that the audit practitioners within the SAI have access to the latest innovations and developments, from both best-in-class researchers as well as external professionals.

The dedicated organizational unit for Data Analytics may leverage such interfaces to identify high quality human resources for internal capacity building for the SAI, as well as incorporating inputs received at periodic intervals on best practices from academia and the corporate sector to further improve the quality of the internal Knowledge Management function for Data Analytics. Adoption of well-defined processes for Data Analytics

To ensure quality control over the audit process and product during the initial period of use of Data Analytics, SAIs may adopt formal, well documented processes for:

- Individuals/ teams to seek expert inputs from the dedicated organizational unit for Data Analytics
- Engagement of external experts when deemed necessary by the dedicated organizational unit
- Building internal capacity through training/ self-learning basis
- Dissemination of best practices and thought leadership
- The need for organization-wide clarity on these processes has been discussed previously.

Funds, People and Technology

Allocation of sufficient budgetary resources for Data Analytics

SAIs should allocate the budgetary resources required by the dedicated organizational unit to execute its mandate. The budgetary support would be necessary for procurement and maintenance of software, hardware and infrastructure as well as engagement of expert external professionals as required.

Allocation of high performing individuals to lead Data Analytics

SAIs should allocate human resources required by the dedicated organizational unit to achieve its objectives. These personnel should be highly motivated and performance oriented individuals who can effectively coordinate internally with multiple teams working under different verticals within the SAI as well as externally with academia and the corporate sector, as discussed previously.

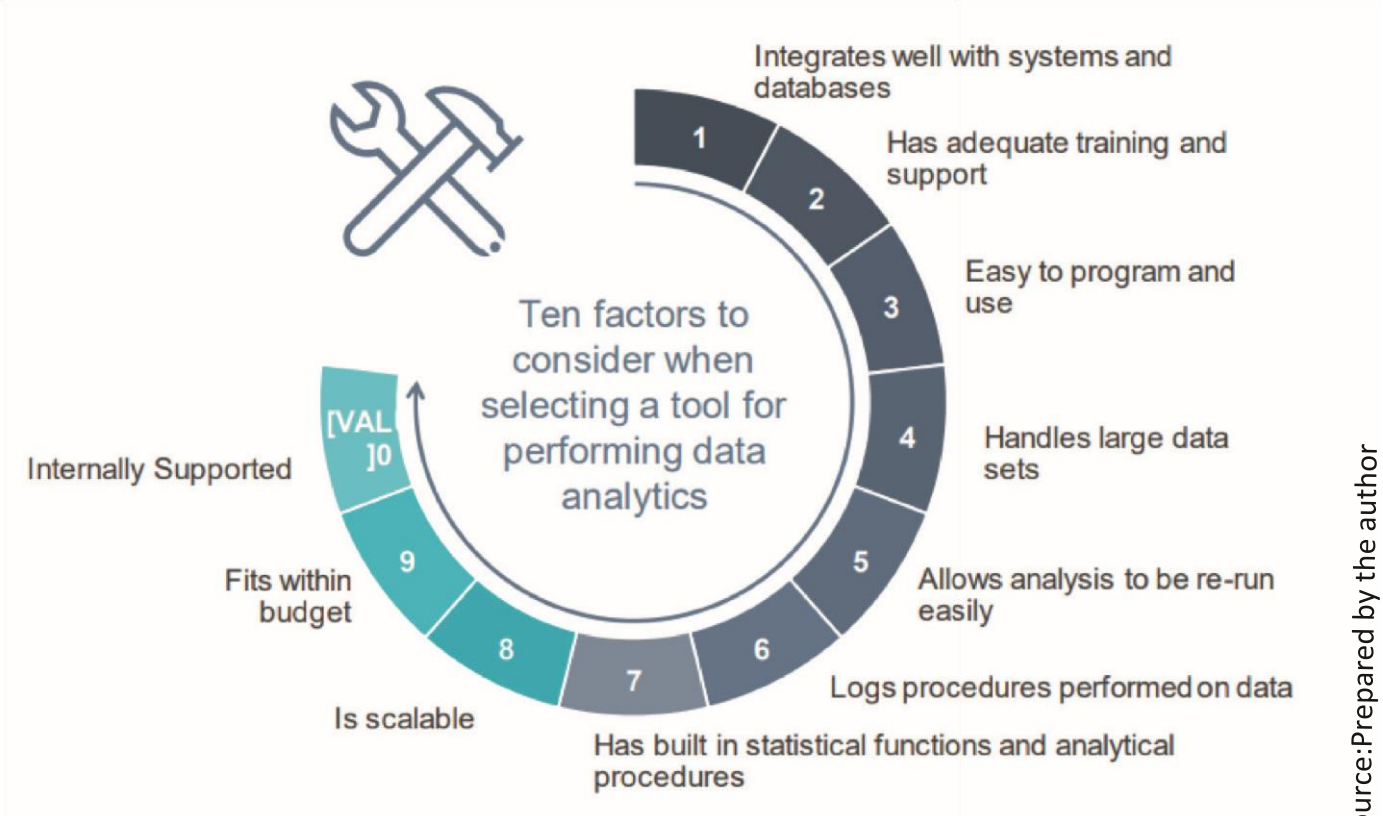
As with any new function/ change being introduced into an organization, SAIs would benefit immensely from assigning individuals who possess

- A natural curiosity and spirit of learning
- Inclination and deep interest in latest technologies

Assessment and adoption of latest technologies for Data Analytics

The choice of appropriate software application/ tool for Data Analytics may be made by SAIs based on the following considerations.

SAIs may also ensure that they continuously track innovations and developments in other emerging or established technologies which can increase the scope of application of Data Analytics to auditing, through generation and collection of granular data.



Source:Prepared by the author

For example, SAIs may track the availability of rich sources of data pertaining to the audited entities such as:

- Satellite and Geographic Information System (GIS) data to examine and analyse the physical boundaries of land and mining leases; crops and forest cover etc.

- Application Programming Interfaces to link with Supervisory Control And Data Acquisition (SCADA) applications' data streams, to examine and analyse real time data on railway or air traffic flows; generation, transmission and distribution of electricity; manufacture of regulated substances such as alcoholic products etc.

- Data obtained from the use of Unmanned Aerial Vehicles/ Drone mounted cameras, similar use cases as Satellite and GIS data, but data collected from a lower altitude and therefore potentially more granular. Such data sources could be used to supplement data published/ hosted in the public domain by the audited entities, and the data repositories available with SAIs themselves. SAIs should consider creating and maintaining large repositories of data, which can be updated across time as well as expanded in scope through addition of new data sources.

Privacy, Ethics and Confidentiality

Widespread adoption and use of emerging technologies such as Advanced Data Analytics and AI systems are inevitable, due to the immense benefits which will accrue in terms of efficiency, economy and effectiveness in various fields of human endeavour. However, there are also some fundamental ethical concerns which arise from the pervasive use of these emerging technologies, such as potential for:

i. Embedding and exacerbation of human biases, resulting in discrimination, inequality, digital divides and exclusion
ii. Lack of transparency and understandability with regard to how Data Analytics works, resulting in information asymmetry and lack of accountability as per established legal frameworks
iii. Maximizing short term gains from utilization of finite natural and environmental resources, by ignoring principles of sustainable development and inter-generational equity
iv. Lack of compliance with the statutory frameworks for data privacy and consumer protection
v. Subordinating human rights, dignity, welfare and safety, which are non-negotiables

Due to these ethical concerns, there has been extensive recognition and strong advocacy to generate awareness for the responsible use of emerging technologies such as Data Analytics and AI across governments, businesses and civil society organizations.

Strengthening mechanisms for international collaboration to facilitate responsible use and access to AI systems and technologies is necessary to address the ethical challenges and systemic risks that arise.

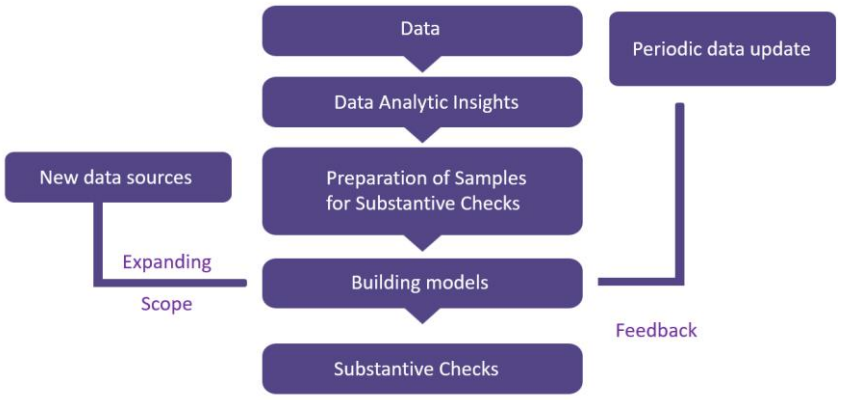
For Supreme Audit Institutions, which exercise oversight over the policies and actions of governments related to Data Analytics, it is vital to derive assurance that a sound risk management framework has been adopted and is operational, to identify and mitigate such

risks. This is very much essential to ensure that ethical values and principles are adhered to, while realizing the full potential benefits from the use of Data Analytics.

With respect to the responsible use of Data Analytics as applied to auditing, SAIs may ensure adherence to the following broad principles in the application of Data Analytics to auditing:

- Ownership of the data sets remains that of the audited entity.
- Auditors hold the data only in fiduciary capacity.
- SAIs should exercise such controls on security and confidentiality of the data as envisaged for the data owner in the audited entity.
- The concerns and statutory frameworks for data confidentiality and privacy of individuals should be ascertained, prior to obtaining access to data.
- Compliance with Rules, procedures and agreements regarding data security, confidentiality and use of data of the audited entity/ third party must be ensured by SAIs.
- Adoption of zero tolerance policy for breaches of ethical standards is vital.

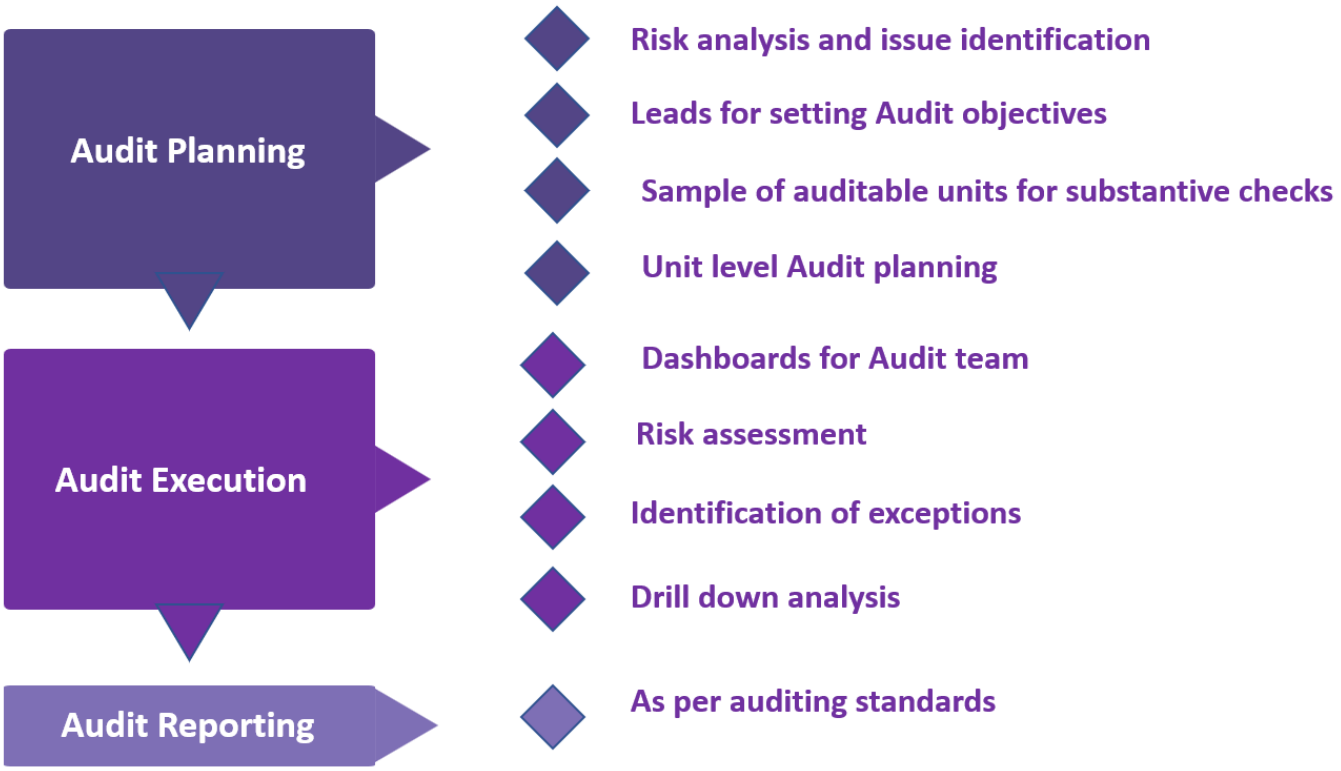
Application of Advanced Data Analytics to Auditing



Source: Prepared by the author

SAIs may begin using Data Analytics with the identification and collection of various data sources for a particular audit. The analysis of data through various data analytic techniques will yield insights on the working of the audited entity. The risk areas or areas of interest identified through such an exercise will assist in identifying audit objectives and developing an Audit Design Matrix. Data Analytics will also assist in identifying the sample of audit units where substantive checks will be conducted. The various analyses can then be built into a re-executable Data Analytic Model. This will ensure that results of data analysis can be used repetitively with periodic updating of data. Establishing a mechanism for receiving data periodically will be crucial for such an incorporating the feedback from substantive checks and bringing in additional data sources. Thus, data analytics in IA&AD is not envisaged to be a one off process for a specific audit, but is expected to evolve over time. The schematic diagram for the process is below.

A schematic representation of the salient uses of data analytics across the standard processes of audit planning, execution and reporting is given below.



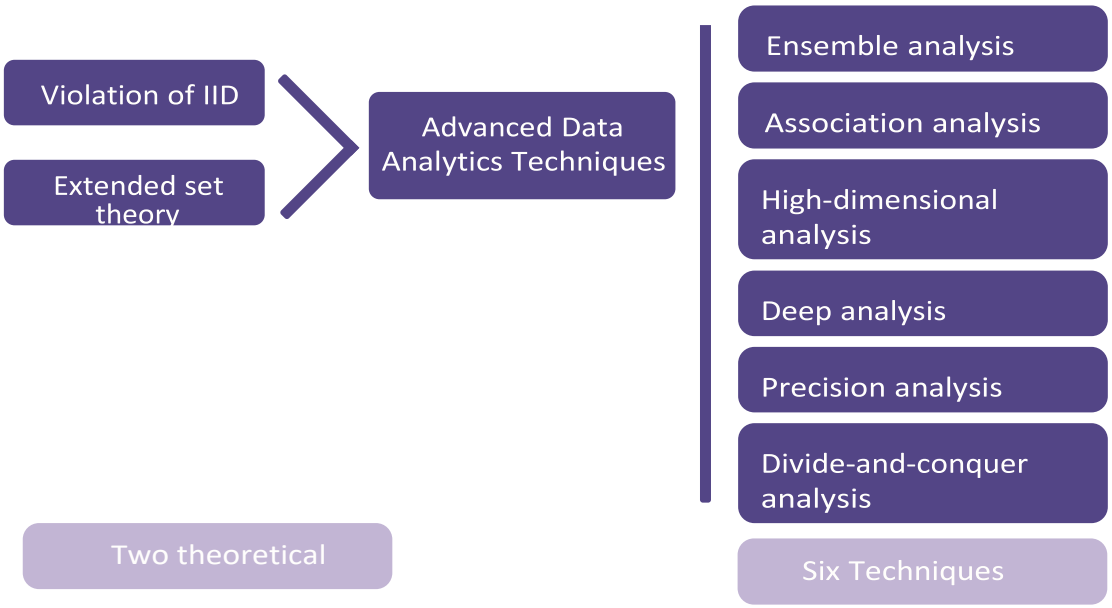
Source: Prepared by the author

The following are the indicative potential use cases for the application of Data Analytics techniques to Auditing:

- **Classification**: Categorization of transactions as Fraud/ No Fraud
- **Clustering**: Identifying transactions having similar characteristics
- **Association**: Identifying correlations between transactions or actions
- **Summarization**: Computing the impact of certain category of transactions
- **Link analysis**: Identification of related entities across multiple levels of connections
- **Deviation detection**: Identification of transactions which are significantly different from the norm (average, median, mode etc.)
- **Prediction:** Estimation of quantity/ materiality of transactions
- **Visualization:** Analysis of data trends and patterns visually sophisticated attempts to evade detection of non-compliant actions/ frauds often evade detection by the simple rules of Basic Data Analytics.

Advanced data analytics techniques aim to detect such sophisticated cases of potentially noncompliant actions/ frauds, if all the relevant information, (i.e. data fields) which may be relevant have been identified and included in the data, even though it may not be clear to the Auditors a priori as to how the data fields may be correlated.

The following are six indicative Advanced Data Analytics techniques which exhibit high potential for application to auditing.



Source:Prepared by the author

The two theoretical bases for the application of the Advanced Data Analytics techniques are:

i. Violation of the assumption of Independent and Identical Distribution (IID) of data
ii. Violation of principles and axioms of Extended Set Theory

The following is a brief and simplified description of the six indicative Advanced Data Analytics techniques:

1. Ensemble Analysis: It is a classification technique which generates an ensemble of classification models i.e. multiple classification models with differing criteria/ assumptions and then computes the predicted classification of the data field of interest (for example, classification of financial transactions data into Fraud/ No Fraud categories) under each model. The classification results from the ensemble of models are then combined into a single predictive classification, which would have significantly higher predictive accuracy than any of the individual classification models in the ensemble.

2. Association Analysis: It is a technique of discovering associations or relationships between different data fields in a large data set, which were not previously known to the Auditor. The discovery of such associations enables the Auditor to identify interesting patterns in numeric or text mining, which in turn enable predictions to be made with high accuracy. The associations may be represented by association rules, which are typically written in the form {A} {B}, where the two data fields A and B exhibit an associative relationship.

3. High-dimensional analysis: It is a technique which is used when the number of data fields/ columns in each row/ tuple large and complex data set is of comparable size, or larger than the total number of data rows/ tuples themselves. The main objective is to reduce the number of data fields to be analysed into a manageable number, such that other Data Analytics techniques can be carried out on the reduced and manageable number of data fields without loss of significant predictive power for the Auditor.

4. Deep Analysis: It is a Machine Learning technique which uses high volume of training data to enable a machine to learn how to predict data outcomes on its own, by recognizing patterns using layers of processing.

5. Precision Analysis: It is a technique used to refine the existing meta data definition for selective data columns based on the actual data values that are present in the column. The objective of the technique is to make the data set more precise, in cases where the original column definition was set without knowledge or regard to the actual data values that the column would subsequently contain. Auditors can use this technique for data cleansing, prior to application of other Data Analytics techniques. storage or computational time. The combined results will provide statistical predictive power which is similar to the one from

6. Divide and Conquer Analysis: It is a technique which has multiple-steps: first splitting a large data set into several smaller ones; then analysing each set separately; finally combining results from each analysis together. This technique is effective in handling large data sets that are unsuitable to be analysed entirely by a single Audit team due to limits either from memory, storage or computational time. The combined results will provide statistical predictive power, which is similar to the one from analysing the entire data set as a whole.

International Applications

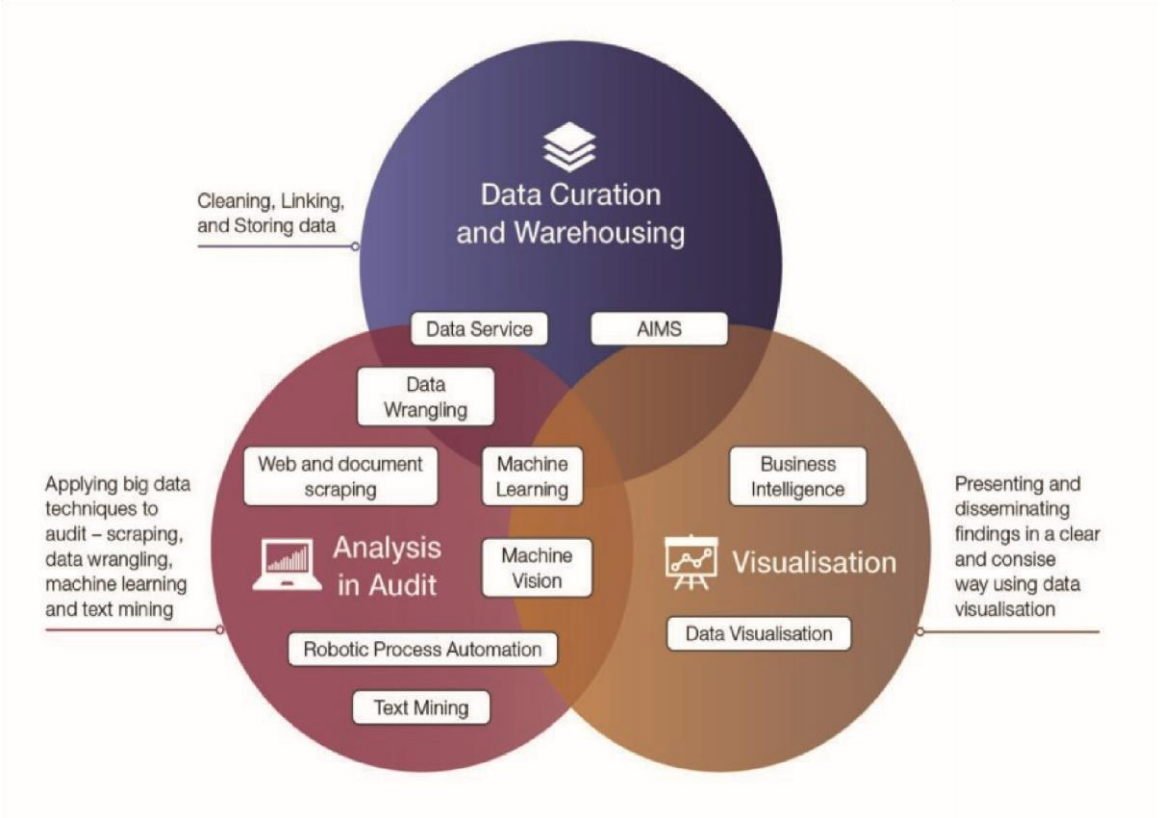
Best Practices on adoption of Data Analytics from two SAIs: the National Audit Office UK and the Government Accountability Office USA are briefly summarized below: i. NAO, UK

Data analytics is an integral part of the audit process. A few years previously, the SAI had been exploring and creating tactical solutions to problems. However, by July 2020, the NAO had developed a strong capability and is making significant progress towards the widespread adoption of data analytics across all elements of its audit work.

Data analytics was being leveraged in three ways:

- Increasing productivity: driving efficiencies through automation, especially in relation to handling large volumes of data
- Adding insight: creating new insights through linking together data and mining for patterns and anomalies
- Improving quality: improving consistency and avoiding errors, and enabling tests to be performed on large or complex data sets where a manual approach would not be feasible

A wide range of technologies and techniques were being used as part of Data Analytics, which could be grouped into three core areas: data curation and warehousing; analysis in audit; and data visualization.



Source: https://www.nao.org.uk/insights/how-data-analytics-can-help-with-audits/

ii. GAO, USA

The SAI has a dedicated organizational unit named Applied Research and Methods (ARM), which is responsible for its Data Analytics function. The SAI has allocated specialists in data analysis, statistics, economics and modelling in ARM. While the Audit teams are multidisciplinary, specialists from ARM are assigned as necessary depending on Data Analytics methods required to be used.

The SAI has clearly defined processes for:

- Consultation with the specialists by the Audit team
- Identification of appropriate data to be analysed
- Assignment of data analysts and other specialists as needed
- Conduct of analysis by specialists
- Synthesis of analyses
- Consultation with the specialists on the reporting of overall results

The SAI uses the following tools for Data Analytics

- Extensive use of SAS and Stata
- Limited use of open-source tools and scripting to conduct analyses and automate data-gathering
- R for predictive advanced statistics, graphics and text
- Anaconda Python for:
  - Web scraping
  - Data extraction, formatting and transformation

It has published a Case Study on “Using Data Analyses to Identify Gender Disparities in Research Grant Awards”.

Potential Challenges

As with the adoption of any major emerging technology, the following broad challenges have to be addressed by SAIs looking to accelerate the adoption of Data Analytics at scale within their organizations:

- Resistance from audited entities in providing access to granular data
- Resistance from SAI personnel in upgrading their skills and incorporate techniques for Advanced Data Analytics into core Audit processes
- Lack of expertise/ skills to apply complex statistical techniques and analytical procedures correctly, by Auditors
- Lack of substantiation of leads/ insights generated by Data Analytics and absence of corroboration of results with other underlying documents/ sources
- Low incentives to allocate funds and high quality HR for Data Analytics function within the SAI, especially in work environments where there may be no/ low demand from the target audience for data driven and highly analytical SAI Reports.

Benefits and Costs

As with the adoption of any major emerging technology, the following potential benefits and costs have to be taken into account by SAIs looking to accelerate the adoption of Data Analytics at scale within their organizations.

i. Benefits

- Improved quality of risk assessment during Audit Planning, resulting in optimal allocation of resources
- Improved quality of monitoring during Audit Execution, resulting in timely interventions and real time decision making
- Improved quality of presentation and visualization during Audit Reporting, resulting in more interesting content and actionable pointers for stakeholders

ii. Costs

- Procurement of infrastructure, hardware and software
- Engagement of skilled external experts
- Interface with academia and the private sector
- Re-engineering workflows within the SAI due to adoption of Policy/ Guidelines on Data Analytics

Emerging technologies:
Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

Robotic Process Automation (RPA)

INTOSAI Working Group on Impact of Science and Technology (WGISTA)
Prepared by the Office of the Auditor General of Islamic Republic of Pakistan

Robotic Process Automation

Basic definition

In simple terms, Robotic Process Automation (RPA) is the process of automating routine human tasks like for example keyboard and mouse clicks, with the help of a robot by releasing humans from doing repetitive tasks, hence freeing them to work on more specialized work requiring creativity and human intelligence. In technical terms, RPA is an advanced software technology that facilitates the creation and management of software robots that imitate human interaction with digital systems and software to make them perform assigned tasks which are time consuming and complex.

Software robots are created in RPA which perform business processes as per requirement of the users. The users of RPA create bots in line with human digital actions which execute different tasks. The created bots work much quicker than humans and their precision is also up to the mark. Just like human beings, the software robots can do things as if they understand what is on a screen; complete the right keystrokes, navigate systems, identify and extract data and perform a wide range of defined actions. Moreover as already stated, software robots can do it much faster and with more consistency than human beings.

Today modern companies and other organizations have a priority in cost cutting, while the traditional ways require huge amount of labor. In such circumstances, RPA can play a key role in accomplishing their assignments in a much more efficient manner. RPA can help organizations in a number of ways in their daily routines e.g it can help running payroll processing, accurately calculate allowances, bonuses, deductions and can perform auditing tasks. In addition, it can create and update central databases of an organization and after configuration it can send e-mails to the clients as well. Similarly, in banking, it can automate process of disbursement of loans, credit card applications, and so on. Some popular software, tools of RPA which are used by private and public sector are UiPath, Blue Prism, Automation Anywhere, Kofax, Pega, Microsoft, NICE, Rocketbot, WorkFusion and others.

Pascal Bornet, Co-author of the book “Intelligent Automation” provides more than 500 cases for how RPA and AI and ML can tackle complicated societal issues like immigration, education, climate change, infrastructure, tax collection and staff morale, among other sensible ones.

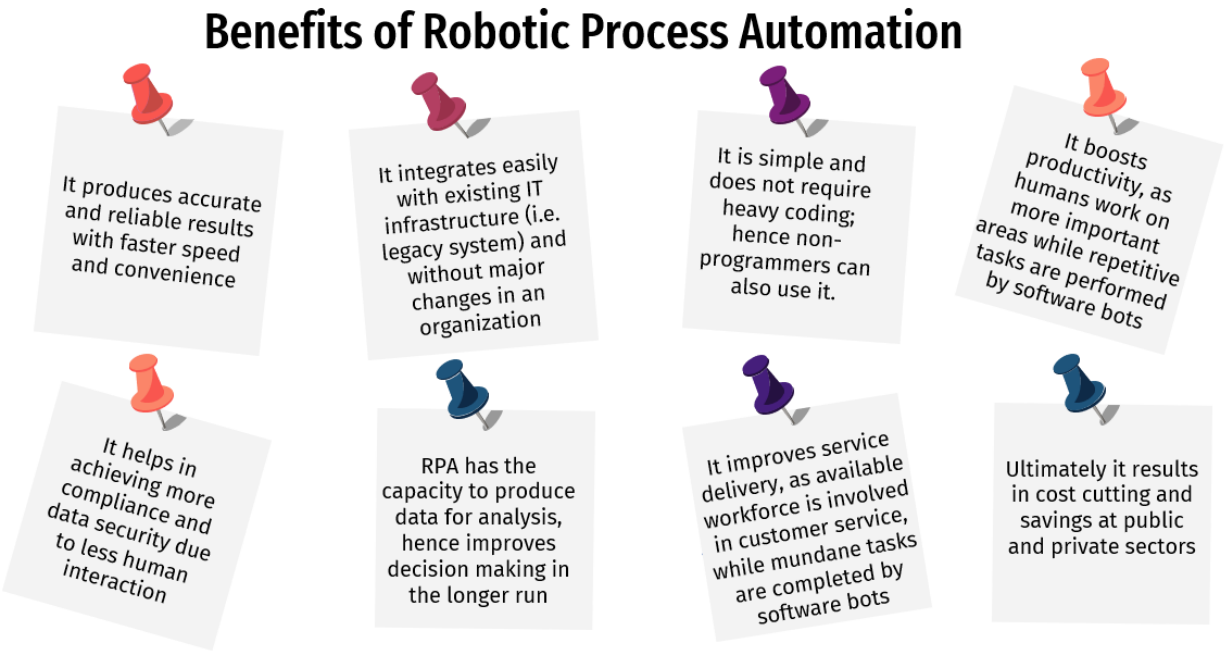
RPA use cases in Government

Key RPA Capabilities

UI data entry, rule based & validation	File creation & manipulation	System integration via system UI or APIs	Data import, export & reformatting across multiple systems	Queue processing	Screen scraping
HR, Finance and Service Management					
Customer 360	**Virtual integration**	**Virtual customization of legacy**	**Attended user augmentation**	**Reporting**	**Processing of unstructured data**
Generating a dynamic customer profile based on information across systems	Using RPA as a bridge between systems without any back end integration	Using RPA to virtually customize COTS legacy sustems	Using RPA to help users do their jobs	Using RPA to generate customized reports	Using RPA to sort & separate unstructured data enabling AI integration
*Single customer view *Meta search across systems *Auto processing of queries & applications *Next best action *Handling of incoming customer queries (email, letter) *Exceptions processing (rule based) Cross sell and upsell *ID verification, validation & credit checking	*Swivel chair data *Start my day *Wrap up *Aligning data across folders/systems *Integration into legacy systems *Pre-populating data in applications/forms *Data migration	*Shortcuts *Customized dashboards *Customized workflows *Auto customer fulfilment *Digital forms integration to back-end services *Virtual API *Data cleansing *Transferring data from one system to another *Service management	*Data validation *Auto customer prompts and follow-ups *Customized dashboards *Auto compliance checking *Auto data set-up *Pre-populating forms/screens *Knowledge base *Guided/contextual help *Training	*Reporting – actuals versus forecast *Monthly preparation of financial pack for business units *Customized dashboards *Automated scheduling and retrieval of reports and dashboards *Reconciliation	*Processing inbound semi-structure correspondence *PDF integration to back-end services *OCR of customer documents *Classification of data based on natural language processing (sentiment analysis, syntax analysis, entity recognition and content classification)

Adaptation from source: https://research.aimultiple.com/rpa-government/

Benefits of RPA



Source:(Benefits of RPA, 2022)

A comparison of computer assignments with and without RPA automation is as follows:

Without Automation		With RPA Automation	
120 Minutes in Total		08 Minutes in Total	
10 Min	Open 60 mails	Open 60 mails	01 Min
35 Min	Copy & Paste contents of 60 mails	Copy & Paste contents of 60 mails	02 Min
30 Min	Copy & Paste sender address of 60 mails	Copy & Paste sender address of 60 mails	02 Min
45 Min	Analysis of 60 mails & marketing status	Analysis of 60 mails & marketing status	03 Min

Source: (The History of Robotic Process Automation, 2022)

Evolution of Robotic Process Automation

RPA as a singular technology started in the year 2000, however, working on this technology can be traced back to the early 1990s. Relevant Machine Learning (ML) algorithms were developed in 1959 by Arthur Samuel which made software to do critical tasks like text summarization and translation. In the 1960s Artificial Intelligence (AI) established interactions between computers and human languages. Finally, this technology grew towards the founding of the RPA in the 1990s.

Robotic Process Automation has mainly three processes:

1. Screen Scrapping Software:

This technology is actually a leap towards development of RPA. It created a compatible bridge between new and old incompatible legacy systems. Screen scrapping allows extracting data from programs, documents, and webs on the presentation layer. Screen Scrapping had many advantages over manual working but had certain limitations like non availability of source codes, scarcity of programmers and reliance on the underlying HTML code of websites, making it difficult to comprehend by end users. For these reasons, businesses wanted to switch over to more friendly technologies.

2. Workflow Automation:

It is a process that helps minimizing human actions and tasks. However, these actions must be repetitive so that they become predictable. If this is the case then these actions can be computerized by using automated management tools. Workflow automation decides when a step is completed and when to start next action. In a nutshell, this type of software reduces requirement of manual data entry and enhances order completion rates with more speed and accuracy.

3. Artificial Intelligence (AI):

AI is the capability of software to perform tasks which require human intelligence, reasoning and human intervention. The tasks that are today done by AI Software were dependent on human judgment. It has replaced time consuming and mundane tasks to computers. The application of AI is possible in a huge number of areas like, speech and image recognition and several types of analyses. This area is discussed in detail in the “Artificial Intelligence” and “Machine Learning” section of this report.

All the above technologies developed Robotic Process Automation (RPA) to an effective and efficient family of programs which could result in having more advantages for the end users by investing less time and resources. RPA still relies on the above three technologies but it raises them to a new level with more improvements and advantages. It allows users to establish automation that is independent over coding knowledge.

Generally, there can be three types of Robotic Process Automation Bots which can be used by the government sector. Namely: Task bots, Metabots, and IQ bots, depending on the level of expertise required and needs of an organization. Task Bots are used as front-end-application to replicate rule-based tasks. They can process structured data. Early versions of OCR and ICR were a sort of Task Bots. MetaBots are independent, re-usable logic blocks which are used for common-user-interface operations as logging on to a system. The IQ bots have cognitive capabilities. With the help of AI they process semi-structured or unstructured data. They can detect patterns, and they have learning features as well.

Source: (The History of Robotic Process Automation, 2022). (The Evolution of RPA Past, Present and Future, 2022)

Resources needed

The use of RPA depends on what kind of RPA solutions are required. In back-office mode of operation a terminal server or a virtual machine or a cloud machine to receive automation requests are required. This processes the automation requests and returns required answers. On the server both robot and target application are run that one needs to automate. In front-office mode of automation or a desktop automation, there is no need for a special hardware and desktop of the agent is enough. In a nutshell, hardware requirements depend on the type of solution someone requires.

For public sector and SAIs, the first and foremost requirement is the will to create automation. SAIs can explore areas in which they can benefit from robots to do tedious tasks so that they can have their present work force to concentrate on better service delivery instead of performing repetitive tasks.

After finding out areas for Robotic Process Automation, SAIs need to appoint a dedicated team for that purpose. They need to have proper training and hardware infrastructure. As already said, RPA does not need huge coding, so SAIs do not need to have expert programmers to implement this type of applications.

A very important aspect is to be taken into consideration about RPA is that it does not replace human beings altogether rather, it frees them from time consuming and boring tasks, ultimately leading to more productivity. To implement RPA, SAIs need to find those areas in which processes are repetitive for instance daily, monthly and yearly basis

transactions having a high volume which require a lot of time and are prone to human errors. If the processes are repetitive then RPA reduces the time for execution. The assignments that require many hours by a human being in automation and on-screen clicking can be completed within minutes. Moreover, another requirement of RPA is that if the processes are rule-based then they may not require lots of changes. Hence the process can be translated into a set of criteria or rules and the robots can follow them with a lot of ease. Lastly, the processes must be clear and structured so that automation can be easily done.

Privacy, ethics and confidentiality issues

Every technology and program have certain risks; RPA is no exception to it. Without meaningful security measures, sensitive data cannot be handed over to robots. Mr. Naved Rashid, Associate Principal Analyst at Gartner says that mainly there are two risks in involved with RPA: data leakage and fraud.

According to: the article “Steps to Ensure Process Automation Security, confidentiality & ethics, 2022, managers need to follow a four step action plan for mitigating these risks:

1. Assigning specific identification IDs to each robot and implementing more secure authentication like user names, passwords and two factor human to system authentication protocols.

2. Restriction of RPA access for each robot as per its assigned task only, e.g. a bot that copies certain values from a database should not have the “write access” but only “read access”.

3. Ensuring that system generated logs are maintained to check any deviation in an extreme case.

4. Periodical review of controls and bringing them in line with changing circumstances.

Apart from the above, there are safety issues involved in RPA in terms of data leakage as well. Moreover, RPA should be built to uphold social standards of a society or an organization. For example RPA in a healthcare system should not favor one patient over another, rather it should be equitable. Issues like inequality, unemployment, errors, data theft and so on are also serious societal and ethical issues with reference to RPA.

Robotic Process Automation Applied for Auditing

As established by Marc Eulerich (July, 2021) the role of auditors is critical in enhancing the protection of the worth of an organization. However, evidences show that lack of resources can significantly hinder the effectiveness in audit as pointed out by (Ettredge, Fuerherm, and Li 2014; Christensen, Glover, Omer, and Shelley 2016). RPA presents auditors the opportunity to reduce costs. It also expands the scope of auditing by being more effective and efficient with limited resources (Ernst&Young 2018; Klynveld Peat Marwick Goerdeler 'KPMG' 2018; Pricewaterhouse Coopers 2018; Deloitte 2018).

Like in any other field in the government sector, auditors can also take advantage of RPA. Data collection is a crucial step in conducting audits which not only takes significant time but is also error prone. Data collection becomes even more difficult when the collected data is to be transported from various applications having several layers. RPA not only can collect data from multiple sources but can also organize it in easy-to-use formats too, thereby reducing chances of errors.

During the sampling phase in auditing, RPA can be used quite effectively as large population of data which require huge computational resources for processing and analyzing can be done with minimum possible time without errors. Similarly, RPA can also prepare reports, send e-mails, update records, set meetings, send reminders and highlight deadlines ahead of time, freeing up auditors to work on more important tasks and save time.

RPA has a wide range of applications in continuous auditing, especially for official government acts published in official gazettes. These acts, such as bidding notices, contracts, and management reports tend to have a typical structure, with their own usual vocabulary of the business of the entity that publishes it. Much of the information published in these acts is not explicit in the structured databases, or if they are, access to this data by the audit teams is not immediate, and when irregularity is detected, it may be too late to reverse it. By means of regular expressions and rules describing the types of irregularities sought by the audit, it is possible to continuously monitor the activity of public entities directly in the published acts and immediately issue notices of possible irregularities to competent auditors and even to the entity being audited.

Another possible application of RPA is helping auditors prepare official documents and reports during their work. By means of regular expressions, it is possible to identify structured elements in the text typed by the auditor, such as the names or identification codes of people, companies, places, or entities. With these elements identified, the robot can query databases or the Internet and suggest corrections or additions to the text. Based on text similarity, it is also possible to suggest that the auditor read complementary documents that have already been produced on the subject.

The timeliness of audit reports can also be improved through RPA, as it provides the auditors with real time feedback in identifying potential risk areas where they can concentrate and save time. Risk assessment, therefore, can be improved by using RPA technology. It can help the auditors in better decision making, such as whether or not to pursue any specific case, being a red flag or otherwise.

Similarly, RPA can detect frauds as well. It identifies patterns in data and auditors can take lead from unusual patterns of data. For example, RPA can compare data across various systems to look for discrepancies. Moreover, Reconciliation is one of the most important requirements in accounting and auditing. This can be left to a robot, which can help in the

reconciliation process and raise alarms in the case of non-reconciliation. Thus, RPA can streamline the process of auditing which ultimately results in better service delivery.

The uses of RPA are not limited to the above outlined areas only; rather it can be used in much more areas of concern as well. It depends on SAIs how they use this technology in their given scenario.

International Applications of Robotic Process Automation (RPA)

Some Instances of Use of RPA in USA

- NASA installed a bot in 2017 which makes procurement requests for the agency without human operators.

- The General Services Administration (GSA) Office of the Chief Financial Officer is another pioneer in using RPA in the government sector by redesigning processes to accomplish its goals. GSA has created many RPAs, from which an impactful bot has been a Public Building Service (PBS) leasing robot. It manages leases for the federal government nationwide and processes around $6 billion in payments per year. Moreover, GSA has also automated Credit Card processing through RPA for saving time. It creates an audit trail for improving compliance with laws.

- The Defense Logistics Agency (DLA) at the Department of Defense uses RPA since 2018. By 2021, it completed a total of 111 automations, while 92 were bots at the finalization stages. They process data, help in reconciliation, update sales orders, help in data extraction and audit support. Moreover, RPA with AI is in use at the Pentagon.

- The Internal Revenue Service (IRS) has successfully employed RPA bots to handle routine reporting processes.
- Arizona's Comptroller's Office uses RPA to make routine updates in the accounting system.

Whenever there is a change such as a name in the state's human resources and payroll systems, the RPA performs these updates just like a human operator.

- In Suffolk County, New York, CIO Scott Mastellon freed up the county's nurses from spending time doing paperwork and adopted RPA so the nurses could spend time caring for patients.

- The Minnesota Pollution Control Agency collects real-time weather data by using RPA. This can analyze data making air quality forecasts for citizens with respiratory problems. It can also send alerts in case of storms.

- During the COVID-19 outbreak, RPA helped in expediting applications for emergency loans distributed to Americans.

Some RPA Cases from other countries:

- In Ireland, the Health Services Executive established an RPA Centre of Excellence. By downloading the lab results, the automations have obtained 80% reduction of the

manual workload, reduced human errors and enabled rapid analysis. Nurses saved three hours per day of administrative work.

- Two RPA applications developed by TCU, the SAI Brazil. They will also be mentioned at Artificial Intelligence section:

Alice is an acronym for Bidding and Public Notice Analysis. The RPA reads daily bid notices and price registration minutes published not only by federal administration but also by states and public agencies. It collects information from the Official Gazette and from *Comprasnet,* a system that registers public procurement. From there, it prepares a preview of the document and indicates signs of irregularities to the auditors.

A second RPA, Sofia, an acronym for the Guidance System on Facts and Indications for the Auditor, also developed by TCU, points out errors in auditors' texts, suggests correlations of information, and indicates other sources of reference. For example, a text that proposes punishment to a company can indicate if there are sanctions against the company or if it appears in court cases. *Alternatively*, even point out that the company has other contracts with public administration.

- A New Zealand higher education institution automated its processes regarding student transcript requests and reduced workload for the staff.

- The Norwegian and German postal services are using RPA bots successfully for last mile mail delivery.

- Sweden uses RPA to speed up its welfare payments.

- Belgium is using RPA bots for job matching employment opportunities and hiring.

- Denmark has built automations to complement their resource shortage and delivering better services to its growing population demands.

Source: (Dr. David K. Rehr, June, 2022)

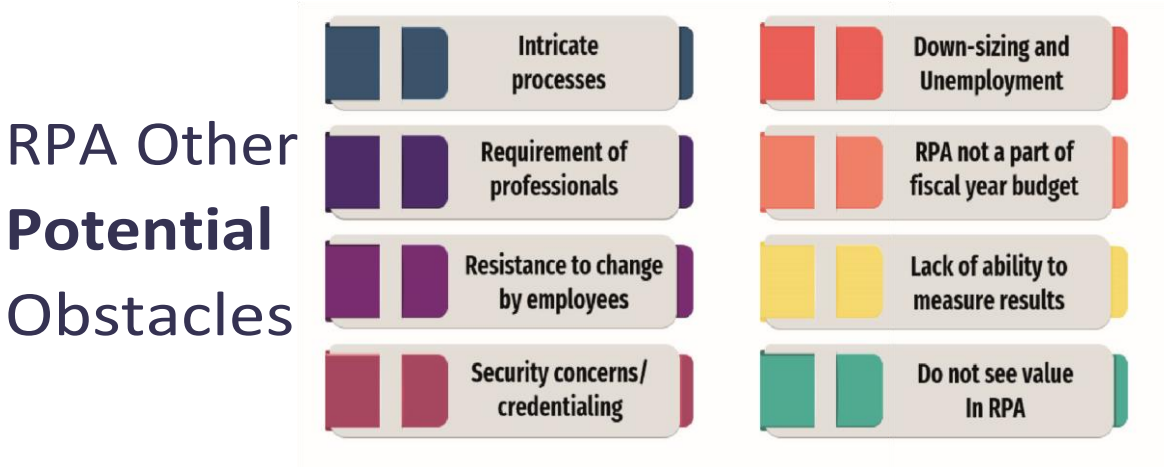
Potential Obstacles

Despite having many advantages, there are potential obstacles to adoption of RPA in both the private and the public sectors, including SAIs. In the public sector, there is always a concern about giving sensitive information to bots as there is a possibility of data leakage or theft. Similarly, due to lack of expertise in RPA in the public sector, a third party is required, which could also expose confidential matters to unwanted entities.

Lack of understanding of RPA is also a major obstacle towards its implementation. When managers do not know what RPA is, and what can it do for their business processes then deciding whether or not to implement it becomes a bottleneck. Similarly, Implementation cost of RPA is also significant. After implementation, there are operating costs for its maintenance while its benefits come in longer terms. Even if cots are reduced still expenses on its implementation discourage managers from employing RPA. In the same way, being a

complex technology, a professional trained team is required for its maintenance, which in some cases is not easy to find. Source: (Robotic Process Automation - Challenges, 2022)

Some other potential obstacles for SAIs and businesses could be:



Source: Prepared by the author

Organizational Changes needed

A major reason behind failure of RPA is having a lack of effective change management. RPA will tend to fail if it is taken in its technological perspective only. Users may oppose RPA in the first instance, but it is the change management that makes it a successful endeavor through a mix of people, the process execution and the new technology.

RPA has many advantages but only when right and capable teams are put in place. Organizations whether public or private, that benefit from RPA have to take into account their own business demands and the needs of the individuals. By assuring personnel that technology will help making their tasks less routine and will free them for more important work, they can be convinced of the benefits the organization will obtain in the longer run.

In the public sector, a broad policy may be required for switch over to RPA for the first time having clear objectives. Moreover, rules and regulations will also be necessary for its operation and maintenance to keep its accountability. For this, the institutions that intend to employ RPA need to convince their executives and their personnel for the changes needed in the organization.

Expected Benefits and Costs

As already discussed, RPA has benefits almost in any field of interest, ranging from Science & Technology to social services. The users of RPA have only to explore areas where RPA can help. One of the important uses of RPA in government sector is savings in work hours through automation of repetitive and time-consuming tasks. A US State of Federal RPA Report from November 2020 says “the annualized hours saved by automation deployed increased by 195%.” Meanwhile, an updated report in December 2021 showed the reduction of over 1.4 million hours (and counting) of low-value work across the US government.

Source: (RPA in the Government Sector, 2022)

- **Savings in Cost:**

Operational efficiency can lead to considerable cost savings for the public and private sectors including SAIs. According to Deloitte LLP, a mid-tier Fortune 1000 Company which has revenue of $20 billion with 50,000 workers, will be able to save $30 million per year with automating just 20% of its tasks. Source: (RPA in the Government Sector, 2022)

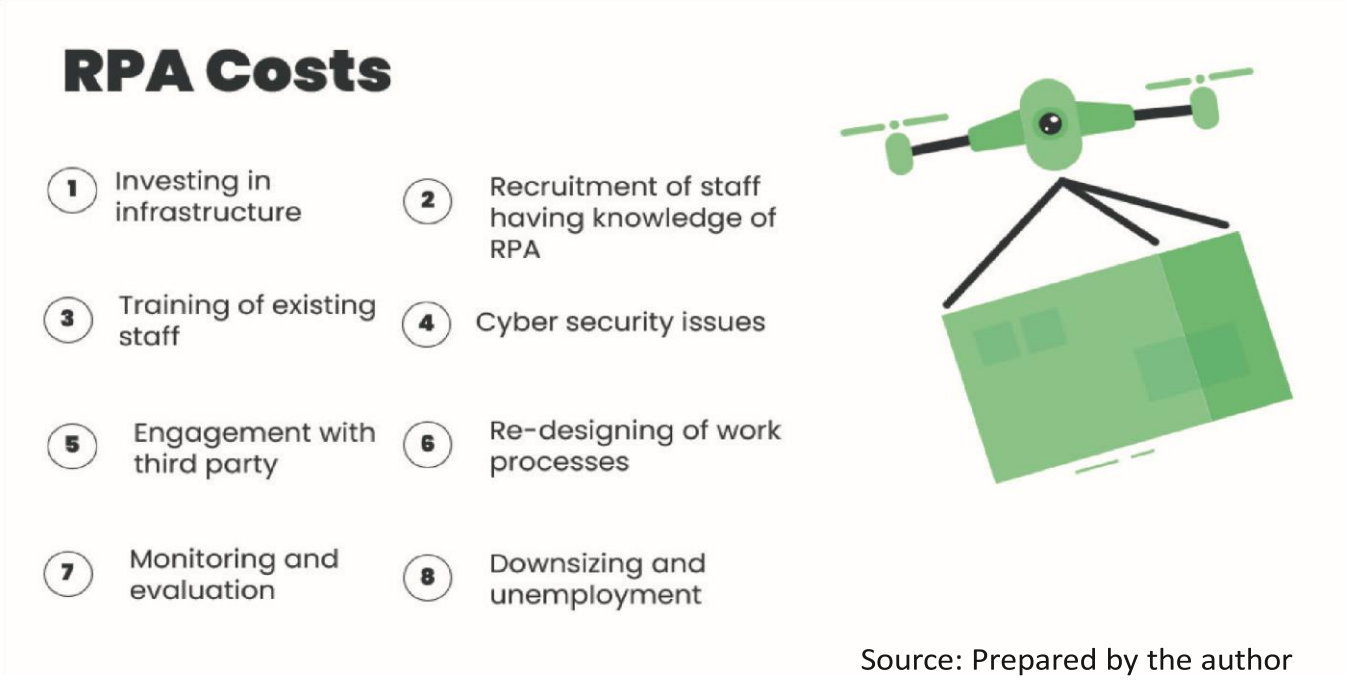
- **Improvement in efficiency:**

Survey by Governing Magazine reported that around 50% of government employees are over burdened with paperwork affecting their efficiency. Moreover, a human being is likely to make 10 errors in every 100 steps when performing redundant work. RPA can be a solution for this.

- **Service delivery:** RPA can help Government organizations in improvement in service delivery due to its accuracy, speed and reliability, resulting in enhancement of public trust.

- **Improved decision making:** Due to real time data analysis and generation of reports, RPA can help policy makers and policy executioners.

From the above considerations, it is evident that RPA has many benefits; however, the following concern areas and costs are to be considered by SAIs before incorporating this technology.



Source: Prepared by the author

Emerging technologies: Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

Artificial Intelligence

INTOSAI Working Group on Impact of Science and Technology (WGISTA)
Prepared by State Audit Office of the Kingdom of Thailand

Artificial Intelligence

Basic Definition

The science and technology revolution could improve auditing methodologies, shift the audit paradigm, and create value & benefits for citizens. Nowadays, AI has an influence in public sector auditing, especially SAIs could implement AI technologies like image recognition, speech recognition, and machine learning to integrate their operations. First, however, we should understand the basic concept and definition of AI, which was mentioned by Professor John McCarthy who coined the original term "Artificial Intelligence or AI" in 1955. He described the science and engineering of making intelligent machines, especially intelligent computer programs. He shows that AI is related to the similar task of using computers to mimic human intelligence, but it does not have to confine itself to methods that are biologically observable.

Professor John McCarthy (2007) established the branches of AI as in Table 1. In the meantime, he outlined several potential AI applications, as shown on figure 1.

Table 1: Branches of AI

AI Branches	Brief explanation
logical AI	The program decides what to do by inferring that certain actions are appropriate for achieving its goals.
Search	AI programs often examine many possibilities, e.g., moves in a chess game or inferences by a theorem-proving program. As a result, discoveries are continually made about how to do this more efficiently in various domains.
Pattern recognition	When a program makes observations, it is often programmed to compare what it sees with a pattern.
Representation	Facts about the world have to be represented in some way. Usually, languages of mathematical logic are used.
Inference	The simplest non-monotonic reasoning is default reasoning, in which a conclusion is inferred by default. Still, the conclusion can be withdrawn if there is evidence to the contrary.
Common sense knowledge and reasoning	This is where AI is farthest from the human level, even though it has been an active research area since the 1950s.
Learning from experience	The approaches to AI based on connectionism and neural nets specialize in that.
Planning	Planning programs start with general facts about the world (especially the effects of actions), facts about the particular situation, and a goal statement. From these, they generate a strategy for achieving the goal.
Epistemology	This is a study of the kinds of knowledge that are required for solving problems in the world.
Ontology	This is the study of the kinds of things that exist. For example, in AI, the programs and sentences deal with various kinds of objects, and we study what these kinds are and what their basic properties are.
Heuristic	It is a way of trying to discover something or an idea embedded in a program.
Genetic programming	Genetic programming is a technique for getting programs to solve a task by mating random Lisp programs and selecting the fittest in millions of generations.

Source: Summary from John McCarthy (2007: 8-10)

Artificial Intelligence applications

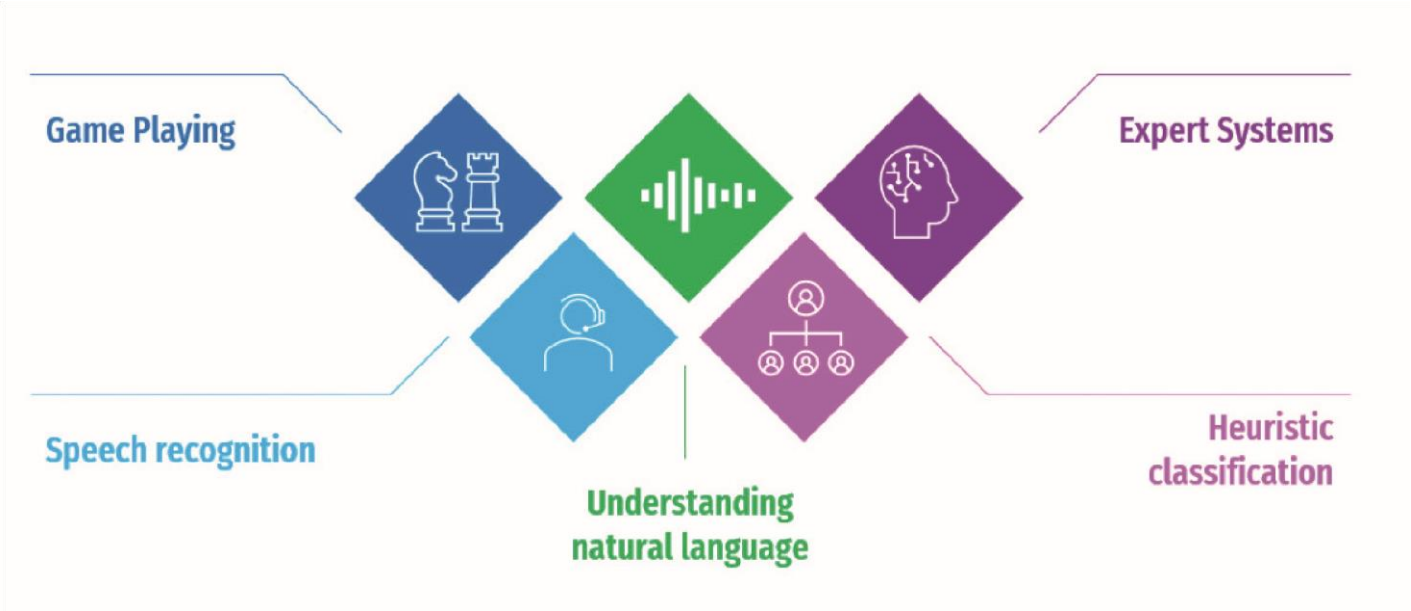


Figure 1 AI Application. Source: Summary from John McCarthy (2007: 10-11)

Evolution of AI

The evolution of artificial intelligence (AI) has significantly impacted various industries and sectors, including the Supreme Audit Institutions and the public sector auditing landscape. As AI technology advances, addressing aspects such as responsible AI, generative AI, text mining, big data, and technologies is essential to enhance the auditing process and ensure accountability and transparency in the public sector.

Responsible AI: As AI systems become more integrated into auditing, ensuring they operate responsibly and ethically is crucial. This includes addressing bias, fairness, transparency, and accountability in AI algorithms. SAIs need to adopt AI ethics guidelines and frameworks to ensure that AI systems are used to improve audit quality and are in compliance with relevant regulations and ethical standards.

Generative AI: Generative AI models, especially Large Language Models (LLMs), such as Chat GPT-4 from OpenAI, Google's PaLM 2 model with their chatbot BARD, and Microsoft's copilot systems with integrated LLMs, can help auditors by automating the analysis of complex documents, identifying patterns, and generating insights from vast amounts of data. It can significantly reduce the time and effort required in auditing, allowing auditors to focus on more strategic tasks. However, generative AI's potential misuse, such as generating fake documents or misleading information, highlights the importance of proper controls and guidelines for its application in auditing.

Text Mining: Text mining techniques can help auditors analyze unstructured data, such as emails, contracts, and reports, to identify potential risks, anomalies, or non-compliance issues. By employing natural language processing (NLP) and machine learning algorithms, auditors can efficiently process large volumes of text data and extract valuable insights, thus enhancing the overall audit quality.

Big Data: The growing availability of big data in the public sector presents new opportunities and challenges for auditors. By leveraging big data analytics, auditors can better detect fraud, waste, and abuse and identify trends and anomalies in financial data.

Additionally, big data can help auditors assess the effectiveness of public policies and programs. However, the management and analysis of big data also require advanced technical skills and robust data governance frameworks.

Geotechnologies: Geospatial technologies, such as geographic information systems (GIS) and remote sensing, can help auditors conduct more efficient and accurate audits. By integrating geospatial data into audit processes, auditors can visually represent and analyze data to identify patterns, trends, and discrepancies. Geotechnologies can also be used to assess the impact of public policies and programs on different geographic areas.

Integrating these technologies into the auditing landscape can significantly improve the efficiency and effectiveness of SAIs and public sector auditing. First, however, organizations must address AI adoption's ethical and practical challenges to ensure these technologies are used responsibly and in the public's best interests.

Finally, the article of Madhurjya Chowdury (2021) provides a good picture of AI evolution. The development of AI technologies could boost productivity from workflow management solutions to trend forecasts. AI can gather and organize vast data to draw interferences and estimates with ability better than human. Similarly, AI improves organizational efficiency while lowering the risk of mistakes, and it identifies unusual patterns, such as spam and fraud, instantaneously to alert organizations about suspicious behavior, among other things.

AI in the future will relate to smart technologies, the Internet of Things (IoT), exponential growing dataset, and innovative algorithms.

Resources needed

In today's rapidly changing public sector landscape, Supreme Audit Institutions must embrace digital transformation to enhance efficiency, effectiveness, and responsiveness. Therefore, the essential resources for SAIs in digital infrastructure, software, human ware, and knowledge ware are to implement AI and other digital technologies in their processes successfully.

1. Building a Robust Digital Infrastructure

A strong digital infrastructure is the foundation of any successful digital transformation. Therefore, SAIs must invest in the following:

a. High-speed internet connectivity: Stable and fast internet connections are crucial for accessing cloud-based services, remote collaboration, and communication tools.

b. Data storage and management solutions: Secure and efficient data storage systems (both on-premise and cloud-based) are necessary to handle large volumes of data and facilitate data analysis.

c. Cybersecurity measures: Implementing robust cybersecurity solutions, such as firewalls, intrusion detection systems, and secure access protocols, is critical for protecting sensitive audit data and maintaining privacy.

2. Adopting the Right Software Solutions

SAIs must choose the right software tools to support their audit processes:

a. AI and data analytics tools: Platforms like TensorFlow, PyTorch, or H2O.ai can be used for developing and deploying AI models for various auditing tasks.

b. NLP and LLM solutions: ChatGPT, IBM Watson, or Google Cloud Natural Language can help analyze unstructured text data and extract insights.

c. Data visualization tools: Software like Tableau, Microsoft Power BI, or QlikView can facilitate the visualization and analysis of audit data. d. Audit-specific tools: Specialized auditing software, such as ACL, IDEA, or TeamMate, can assist auditors in managing and automating audit processes.

3. Developing Humanware for Digital Transformation

Skilled personnel and continuous learning are key to the successful integration of digital technologies:

a. Skilled personnel: Hiring and retaining professionals with expertise in AI, data analytics, NLP, and other relevant areas is crucial for implementing and managing digital technologies in SAIs.

b. Training and development programs: Staff should be provided with continuous learning and development opportunities to keep them up-to-date with the latest technologies, tools, and methodologies.

4. Leveraging Knowledge Ware for Best Practices and Collaboration

Knowledge ware helps SAIs stay informed and connected with best practices and industry trends:

a. Best practices and guidelines: Resources like INTOSAI's guidance documents, the AI4G initiative, or the World Economic Forum's AI in Government project can provide valuable insights into best practices and guidelines for implementing AI and digital technologies.

b. Professional networks and communities: Engaging with professional networks, such as the Institute of Internal Auditors (IIA) or the Information Systems Audit and Control Association (ISACA), can facilitate knowledge sharing and collaboration with other SAIs and industry experts.

c. Conferences and workshops: Attending conferences and workshops focused on AI, digital transformation, and public sector auditing can offer insights into the latest trends and developments in the field.

In conclusion, by ensuring the availability of robust digital infrastructure, software, human ware, and knowledge ware resources, SAIs can effectively integrate digital technologies into their audit processes. This will enable them better to address the

challenges of an ever-changing public sector landscape, enhancing efficiency, effectiveness, and responsiveness to new risks and opportunities.

For the public sector, the first question of AI resources needed is how to start with AI in the organization. The OECD study by Jamie Berryhill et al. (2019) pointed out that AI is an area of research and technology application that can significantly impact public policies and services in many ways. Hence, governments can use AI to design better policies and make better decisions, improve communication and engagement with citizens and residents, and increase the speed and quality of public services.

Certainly, AI's potential benefits are significant, but attaining them is not easy. Government use of AI trails that of the private sector; the field is complex and has a steep learning curve; and the purpose of, and context within, the government are unique and present several challenges. Hence, the OECD (2019) suggested a framework for governments to develop AI strategies.

An AI strategy should include the components in figure 2 that follows:

Figure 2 AI Strategy for the public sector. Source: Summary from OECD (2019: 138-139)

Privacy, ethics, and confidentiality issues

As Supreme Audit Institutions increasingly adopt AI technologies to improve efficiency, accuracy, and risk identification, it becomes essential to recognize and address the potential risks associated with AI implementation—the risks related to the use of AI in auditing. However, we offer mitigation strategies to ensure responsible and ethical AI adoption.

Tackling Bias and Discrimination
Risk: Biases in training data may lead to biased audit outcomes and discriminatory practices, as AI algorithms could inadvertently perpetuate these biases.
Mitigation strategies:
a. Use diverse and representative training data to minimize biases.
b. Conduct regular audits of AI models to identify and correct biases.

c. Assemble interdisciplinary teams to develop and review AI algorithms, promoting diverse perspectives and reducing the risk of bias.

Ensuring Transparency and Explainability

Risk: Complex AI models can be challenging to understand and interpret, potentially resulting in a lack of transparency in audit findings and decision-making processes.

Mitigation strategies:

a. Employ explainable AI techniques to enhance the understandability and transparency of AI models.

b. Create clear documentation of AI algorithms, methodologies, and assumptions for better communication of audit outcomes.

c. Train auditors in AI and machine learning concepts to improve their ability to interpret and explain AI-driven findings.

Safeguarding Data Privacy and Security

Risk: Processing sensitive and confidential data in AI-driven auditing raises data privacy and security concerns.

Mitigation strategies:

a. Implement robust data protection measures like encryption, access control, and secure storage solutions.

b. Establish strict data handling and sharing policies and guidelines to ensure compliance with data protection regulations.

c. Regularly assess and update cybersecurity measures to protect against evolving threats.

Avoiding Overreliance on AI

Risk: Overreliance on AI tools can reduce human oversight and critical thinking, potentially resulting in undetected errors or misinterpretations.

Mitigation strategies:

a. Promote a human-in-the-loop approach, where auditors actively engage with AI-driven insights and provide expertise to validate findings.

b. Develop training programs to help auditors understand AI tools' limitations and potential pitfalls.

c. Cultivate a culture of continuous learning and skepticism to ensure AI is used as a complementary tool rather than a replacement for human judgment.

Addressing Ethical and Legal Considerations

Risk: Ethical and legal concerns may arise from using AI in auditing, such as the responsibility for AI-driven decisions and the potential misuse of AI-generated insights.

Mitigation strategies:

a. Create and implement ethical guidelines for AI adoption in auditing, including fairness, accountability, and transparency.

b. Set clear policies for AI-driven decision-making and ensure compliance with relevant laws and regulations.

c. Engage in ongoing discussions with stakeholders, including regulators and the public, to address ethical and legal concerns and build trust in using AI in auditing.

In summary, to harness the full potential of AI in auditing, it is crucial to implement responsible and ethical practices that address potential risks. By understanding these risks and adopting appropriate mitigation strategies, SAIs can capitalize on the benefits of AI while maintaining a strong commitment to fairness, transparency, and accountability.

The issues of AI privacy, ethics, and confidentiality might be explained under the concept of responsible AI. Katharina Koerner's (2021) essay raised the question: How can AI/ML systems be used responsibly and ethically that deserve the trust of users and society?. In fact, we have several AI governance frameworks.

However, Katharina observed that most AI governance frameworks overlap in their definition of basic principles, which include privacy and data governance. Also overlapping are concepts of accountability and auditability, robustness, security, transparency, explainability, fairness, non-discrimination, human oversight, and promotion of human values.

In 2020, The Singaporean government launched the "Model AI Governance Framework". This framework is another good practice that reflects how to protect privacy and confidentiality and support ethics for AI implementation.

The Model Framework comprises guidance on measures promoting the responsible use of AI that organizations should adopt in four key areas, as in following figure 3.

Figure 3 AI Governance
Source: Summary from Model AI Governance Framework (2nd edition) (2020: 20)

From figure 3, the Singaporean government clarified the AI governance framework based on four main areas. The first is the internal governance structures and measures. It represents adapting existing or setting up internal Governance structure and measures to incorporate values, risks, and responsibilities relating to algorithmic decision-making. The second consists on determining the level of human involvement in AI-augmented decision-making.

A methodology to aid organizations in setting their risk appetite for AI, i.e., determining acceptable risks and identifying an appropriate level of human involvement in AI-augmented decision-making. The third area is operations management with issues to be considered when developing, selecting and maintaining AI models, including data management. And finally, Stakeholder interaction and communication Strategies for communicating with an organization's stakeholders and managing relationships with them.

GAO's AI's Accountability Framework for Federal Agencies and Other Entities

The Government Accountability Office (GAO) is an independent, nonpartisan agency that provides audit, evaluation, and investigative services for the U.S. Congress. In June 2021, GAO released a report titled **"Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities."** The report outlines a comprehensive framework for federal agencies and other entities to use in their efforts to develop and implement responsible artificial intelligence (AI) systems.

The framework includes four key principles: (1) Governance, (2) Data (3) Performance, (4) Monitoring. The framework is intended to help federal agencies and other entities ensure that their AI systems are designed and used in a way that is consistent with ethical and legal principles, and that they are held accountable for their actions.

The report emphasizes the importance of governance in ensuring accountability and transparency for AI systems. It provides recommendations for federal agencies to establish governance structures and processes that can help ensure that AI systems are used in a responsible and ethical manner.

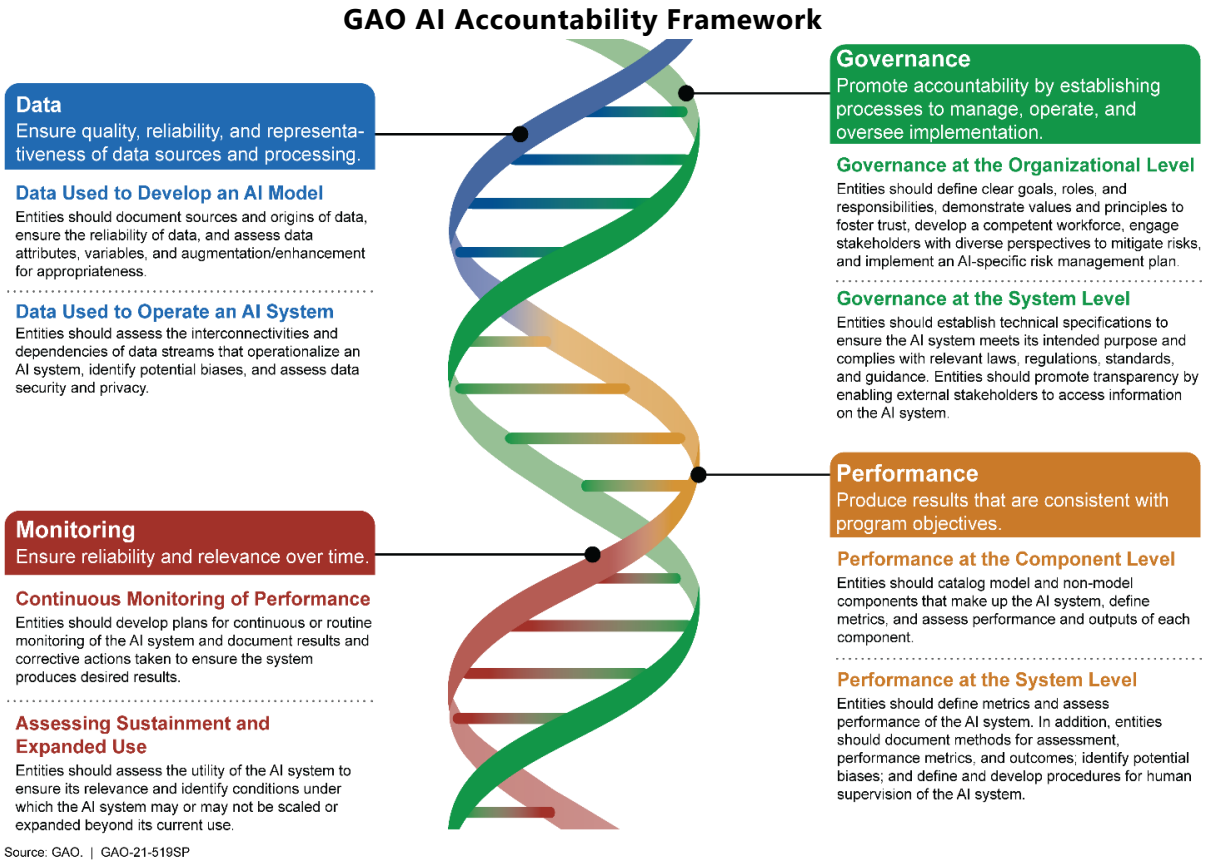


Figure 4. GAO AI Accountability Framework.
Source: Artificial Intelligence (AI) Accountability Framework. GAO-21-519SP, June 2021

Artificial Intelligence technology applied for auditing

Yves Genest (2019) from Canadian Audit & Accountability Foundation (CCAF) mentioned using AI in auditing for three areas that are fuelling the most promising technology for auditors: image recognition, speech recognition, and machine learning.

By their side, Ramu Prasad Dotel (2020), Deputy Auditor General of Nepal, shared their conceptual pathway to faceless or remote auditing; SAI Nepal is currently planning to implement AI tools to assist in audit work, including (a) Robotic Process Automation (RPA), (b) Search Optimization Tools, (c) Artificial Neutral Networks, (d) Information Extraction and data mining and also (e) Natural Language Processing (see figure 4).

Dotel (2020) concluded that AI significantly helps perform oversight work using available resources to produce high-quality results. Through various analyses, AI tools identify patterns and exceptions for further investigation by human auditors and increase remote auditing possibilities. Nevertheless, Dotel noticed that AI cannot replace human auditors' professionalism. Even though AI systems can indicate risk, auditors need to further analyse actual conditions, causes and effects. Therefore, Dotel summarized that AI must be employed as an assistive technology to augment the audit process, and equally important is that SAIs cultivate skilled manpower to harness AI technology.

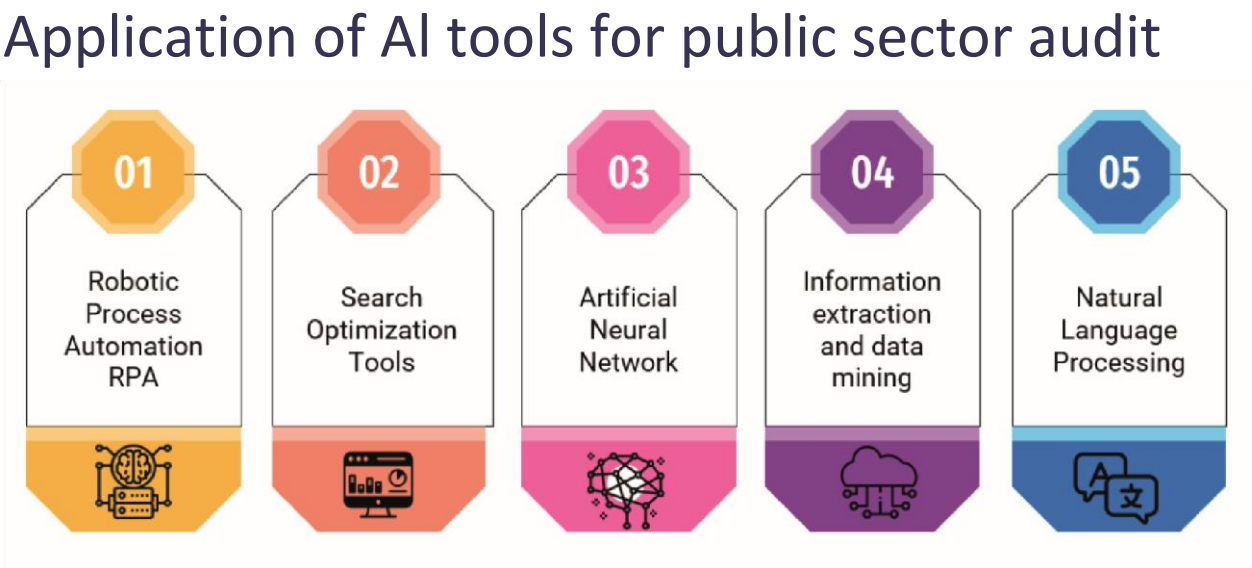


Figure 5 Application of AI tools for public sector. Source: Modified from Ramu Dotel (2020)

From the figure, the public sector auditing landscape is undergoing a digital transformation with the adoption of advanced technologies such as Robotic Process Automation (RPA), Search Optimization Tools, Artificial Neural Networks (ANN), Information Extraction, Data Mining, and Natural Language Processing (NLP). These application tools in public-sector auditing discuss their potential benefits, challenges, and prospects.

Rapid digital technology advancements have significantly impacted the public sector auditing landscape. By leveraging these technologies, auditors can enhance their processes' efficiency, accuracy, and effectiveness.

Robotic Process Automation (RPA)

RPA enables auditors to automate repetitive and time-consuming tasks, such as data entry, reconciliation, and report generation. By automating these tasks, RPA can help improve audit efficiency, reduce human error, and free up resources for more strategic tasks.

Benefits:

a. Increased efficiency and reduced human error
b. Enhanced scalability of audit processes

c. Time and cost savings

Challenges:
a. Initial investment in RPA software and infrastructure
b. Ensuring proper integration with existing systems
c. Keeping pace with evolving regulatory requirements

Search Optimization Tools

Search optimization tools facilitate effective and efficient data retrieval, allowing auditors to access relevant information and documents quickly. These tools employ advanced search algorithms and indexing techniques to optimize search results and minimize the time spent on manual data retrieval.

Benefits:
a. Accelerated access to relevant information
b. Reduced time spent on manual data retrieval
c. Improved audit quality through more comprehensive data analysis

Challenges:
a. Ensuring compatibility with various data sources and formats
b. Balancing data privacy and accessibility concerns
c. Maintaining up-to-date search algorithms and indexing techniques

Artificial Neural Networks (ANN)

ANNs are advanced computational models inspired by the human brain's neural networks. These models can identify patterns and relationships within large and complex datasets, enabling auditors to detect anomalies, fraud, and other risks more effectively.

Benefits:
a. Enhanced risk identification and fraud detection
b. Improved predictive capabilities in audit planning
c. Streamlined data analysis processes

Challenges:
a. Acquiring the necessary expertise to develop and maintain ANN models
b. Ensuring the quality and representativeness of training data
c. Managing the complexity and interpretability of ANN models

Information Extraction and Data Mining

Information extraction and data mining techniques can help auditors analyze structured and unstructured data to identify patterns, trends, and relationships. This enables auditors to gain valuable insights, better understand risk factors, and make more informed decisions during the audit process.

Benefits:
a. Improved insights and decision-making capabilities
b. More comprehensive and in-depth data analysis
c. Enhanced risk assessment and management

Challenges:
a. Managing large volumes of data from diverse sources
b. Addressing data quality and consistency issues
c. Ensuring data privacy and security

Natural Language Processing (NLP)
NLP enables computers to understand, analyze, and generate human language. By applying NLP techniques, auditors can efficiently process and analyze unstructured textual data, such as contracts, policies, and emails, to uncover insights and detect anomalies.

Benefits:
a. Accelerated analysis of unstructured textual data
b. Enhanced detection of anomalies and risks in textual data
c. an Improved understanding of complex regulatory requirements and policies

Challenges:
a. Handling ambiguities and nuances in human language
b. Ensuring compatibility with various languages and dialects
c. Managing the complexity and interpretability of NLP models

Hence, applying advanced technologies like RPA, Search Optimization Tools, ANN, Information Extraction, Data Mining, and NLP can significantly improve public sector auditing processes. However, addressing the challenges and risks associated with these tools is essential to harness their full potential. By investing in the right technologies, infrastructure, and expertise, auditors can enhance their processes' efficiency, accuracy, and effectiveness, leading to better outcomes for public sector organizations and their communities.

Meanwhile, the study of Ghanom and Folasade Alaba (2020) had the research question: How is AI enhancing the effectiveness of audit processes? Alaba (2020:21) viewed AI-based systems in auditing as those tools adopted in the auditing process for ease of the assignment that still ensures compliance with all required standards, thereby enhancing the effectiveness of such process.

Ghanom and Alaba (2020: 59) concluded that AI enhances the effectiveness of the audit process by the reduction in errors that formerly caused auditors to repeat the work. For instance, AI systems can collect and peruse financial records coherently and effectively. Moreover, AI reduces the time needed for classifying and comparing transactions, more so in the first entries in the journal.

Ghanom and Alaba (2020: 59) pointed out that using AI systems increases professionalism and compliance with international standards. As a result, the study uniformly agrees that using AI systems will continuously increase auditing effectiveness.

Another study by Nora Azima Noordin et al. (2020) explored the external auditor’s perception of using AI in the United Arab Emirates (UAE). The result evidenced the positive perception among external auditors towards the contribution of AI to audit quality.

The Rio Declaration 2022, adopted at the XXIV Congress of the International Organization of Supreme Audit Institutions (INTOSAI) in Rio DE Janeiro, Brazil, sets forth principles that guide the evolution of Supreme Audit Institutions towards more responsive, agile, and flexible entities. The key takeaways from the Rio Declaration emphasize the importance of agility and flexibility for SAIs in rapidly changing environments and emerging challenges.

Embracing Agility in SAIs

Adopting a proactive approach: SAIs must transition from reactive to proactive entities by anticipating and preparing for future risks and challenges. It involves continually monitoring the public sector landscape, identifying trends and issues, and adjusting audit priorities accordingly. By being proactive, SAIs can address potential problems before they escalate and ensure the effective allocation of resources.

Leveraging technology: The Rio Declaration highlights the importance of harnessing technology to enhance the efficiency and effectiveness of SAIs. It includes adopting AI, data analytics, and other digital tools to streamline audit processes, detect anomalies, and improve decision-making. In addition, by staying abreast of technological advancements, SAIs can remain agile and adapt their audit methodologies to address emerging risks better.

Building a culture of innovation: Encouraging a culture of innovation within SAIs can foster the development and implementation of new audit approaches, tools, and techniques. By embracing experimentation and learning from successes and failures, SAIs can continually refine their methods and stay agile in the face of evolving challenges.

Promoting Flexibility in SAIs

Encouraging collaboration and knowledge sharing: The Rio Declaration emphasizes the need for SAIs to collaborate and share knowledge, experiences, and best practices. By collaborating with other SAIs, international organizations, and the private sector, SAIs can benefit from diverse perspectives, learn from each other's experiences, and adopt more flexible and effective audit approaches.

Embracing a risk-based approach: Adopting a risk-based approach to auditing allows SAIs to prioritize audit activities based on the potential impact and likelihood of risks. It ensures that limited resources are allocated to the areas with the highest risk, enabling SAIs to remain flexible and responsive in addressing emerging challenges.

Investing in continuous learning and development: To remain flexible and adapt to the changing environment, SAIs must invest in their staff's continuous learning and development. It includes regular training, professional development opportunities, and access to the latest tools and methodologies. As a result, a well-equipped and skilled workforce can better adapt to new challenges and maintain the agility and flexibility of the organization.

Therefore, The Rio Declaration 2022 highlights the need for SAIs to embrace agility and flexibility to address the rapidly changing public sector landscape effectively. By

adopting a proactive approach, leveraging technology, fostering a culture of innovation, encouraging collaboration, and investing in continuous learning and development, SAIs can become more responsive entities capable of ensuring accountability, transparency, and efficient use of public resources in an ever-evolving world.

The Rio Declaration and the Role of Natural Language Processing and Large Language Models in Supreme Audit Institutions

The Rio Declaration 2022 underscores the importance of agility, flexibility, and technology adoption for Supreme Audit Institutions to address the challenges of an ever-changing public sector landscape. *Natural Language Processing (NLP) and Large Language Models (LLMs) like ChatGPT can significantly impact the auditing process, enabling SAIs to become more responsive and efficient.* The question is how the principles of the Rio Declaration can be related to using NLP and LLMs in the context of SAIs.

Enhancing Audit Efficiency through NLP and LLMs

One of the core principles of the Rio Declaration is leveraging technology to enhance the efficiency and effectiveness of SAIs. *NLP and LLMs can help auditors analyze unstructured data*, such as emails, contracts, and reports, to identify potential risks, anomalies, or non-compliance issues. By employing these advanced AI models, auditors can efficiently process large volumes of text data and extract valuable insights, thus enhancing the overall audit quality and aligning with the Declaration's call for technology adoption.

Fostering a Culture of Innovation with AI-based Solutions

The Rio Declaration emphasizes the importance of cultivating a culture of innovation within SAIs. *Integrating NLP and LLMs into the auditing process is an innovative approach that can help SAIs stay ahead of emerging risks and challenges.* By embracing these advanced technologies, SAIs demonstrate their commitment to innovation and can continually refine their methodologies to stay agile in the face of evolving challenges.

Encouraging Collaboration and Knowledge Sharing through AI-powered Tools

The Rio Declaration highlights the need for SAIs to collaborate and share knowledge, experiences, and best practices. AI-powered tools like ChatGPT can facilitate collaboration by acting as an information hub, enabling auditors to access relevant information and share insights with their colleagues easily. Additionally, LLMs can be used to analyze data from multiple sources, providing a more comprehensive view of risks and trends in the public sector and promoting cross-institutional knowledge sharing.

Investing in Continuous Learning and Development for AI Integration

The Rio Declaration's principle of investing in continuous learning and development is critical to ensure the effective adoption of NLP and LLMs. Therefore, SAIs must provide regular training, professional development opportunities, and access to the latest AI tools and methodologies to equip their staff with the skills needed to utilize these technologies. This will help SAIs maintain agility and flexibility while integrating advanced AI models into their audit processes.

In conclusion, *The Rio Declaration 2022 and its principles provide a roadmap for SAIs to embrace NLP and LLMs, such as ChatGPT, to enhance their audit processes.* By leveraging these advanced AI models, fostering a culture of innovation, encouraging collaboration, and investing in continuous learning and development, SAIs can become more agile and responsive entities capable of ensuring accountability, transparency, and efficient use of public resources rapidly changing world.

International Applications

Currently, there are several SAIs plan to integrate AI into the auditing process. For example, following the 2019 Moscow Declaration, SAIs could respond effectively to opportunities brought by technological advancement. Likewise, the 2021 Bangkok Declaration in Chapter 3 promotes SAIs and leveraging by using advanced technologies for public sector auditing. In the next normal era, SAIs could promote the principle of availability and open data, source code, and audit algorithms. Meanwhile, SAIs can implement data science in audits depending on their mandate and practices and develop future auditors who can employ data analytics, AI tools, and advanced qualitative methods.

Figure 6 The International Best Practice based on the 2019 Moscow Declaration and the 2021 Bangkok Declaration.

The Moscow Declaration was adopted during the XXIII International Congress of Supreme Audit Institutions (INCOSAI) held in Moscow, Russia, in September 2019. The declaration emphasizes the importance of leveraging technology to enhance the work of Supreme Audit Institutions and address global challenges.

Key aspects of the Moscow Declaration related to leveraging technology for SAIs include:

- **Digital transformation:** The declaration recognizes the potential of digital transformation to improve public administration and calls on SAIs to actively participate in implementing digital technologies.
- **Strengthening SAI capabilities:** The declaration encourages SAIs to invest in developing their technical and human resources to harness information technologies' power effectively. It includes promoting the digital skills of auditors, as well as supporting research, innovation, and knowledge-sharing initiatives.
- **Data analytics**: The Moscow Declaration acknowledges the growing importance of data analytics in public sector auditing. It encourages SAIs to develop data-driven audit approaches and adopt new analytical tools to enhance the effectiveness of their work.
- **Cybersecurity and data protection**: The declaration highlights the need for SAIs to address the risks associated with digital technologies, such as cybersecurity

threats and data privacy concerns. It calls on SAIs to develop robust policies and procedures to protect sensitive data and ensure the resilience of their digital infrastructure.

- **International cooperation**: The Moscow Declaration highlights the importance of international cooperation in addressing global challenges related to the digital transformation of public administration. SAIs should collaborate with international organizations, share knowledge and experiences, and develop joint initiatives to promote the use of information technologies in public sector auditing.
- **Fostering transparency and accountability:** The declaration recognizes that leveraging technology can enhance transparency and accountability in public administration. SAIs use digital tools to improve their communication with stakeholders, share audit findings, and promote the principles of good governance.

Meanwhile, the Bangkok Declaration 2021 was the ASOSAI document that followed the Moscow Declaration 2019. The third chapter of the Bangkok Declaration focuses on digital transformation as the smart SAI. The Bangkok Declaration 2021, adopted during the 15th Assembly of the Asian Organization of Supreme Audit Institutions (ASOSAI), builds on the Moscow Declaration 2019 and further emphasizes the importance of digital transformation for Supreme Audit Institutions. The third chapter of the Bangkok Declaration specifically focuses on digital transformation to develop "smart SAIs."

Key aspects of the third chapter of the Bangkok Declaration, focusing on digital transformation for smart SAIs, include:

- **Digital transformation strategies:** The declaration encourages SAIs to develop and implement comprehensive digital transformation strategies to improve their performance and better respond to the evolving needs of public sector auditing.
- **Capacity building:** The Bangkok Declaration highlights the importance of capacity building in digital technologies, urging SAIs to invest in the training and development of their staff, enabling them to adapt to new tools and techniques.
- **Technological innovation:** The declaration identifies the importance of adopting innovative technologies such as data analytics, artificial intelligence, and robotic process automation to enhance the efficiency and effectiveness of audit processes.
- **Collaboration and knowledge-sharing:** The Bangkok Declaration calls for increased collaboration and knowledge-sharing among SAIs and other stakeholders to learn from each other's experiences and promote adopting best practices in digital transformation.
- **Strengthening IT infrastructure:** The declaration underlines the need for SAIs to strengthen their IT infrastructure to support the successful implementation of digital transformation initiatives and ensure the security and reliability of their systems.
- **Cybersecurity and data protection:** In line with the Moscow Declaration, the Bangkok Declaration also highlights the significance of addressing cybersecurity and data protection concerns to ensure the integrity and confidentiality of audit information.
- **Performance measurement and monitoring:** The Bangkok Declaration encourages SAIs to establish performance measurement and monitoring mechanisms to assess the impact of digital transformation initiatives on their operations and identify areas for improvement.

The Relationship Between the Moscow and Bangkok Declarations: Uniting Supreme Audit Institutions in Digital Transformation

The Moscow Declaration 2019 and the Bangkok Declaration 2021 are key documents highlighting digital transformation's importance in Supreme Audit Institutions. The relationship between these declarations and their collective impact on promoting technological advancements in public sector auditing, fostering collaboration, and addressing global challenges.

The Moscow Declaration, adopted during the XXIII International Congress of Supreme Audit Institutions (INCOSAI) in 2019, emphasized the importance of leveraging technology to enhance SAI performance. The Bangkok Declaration, adopted during the 15th Assembly of the Asian Organization of Supreme Audit Institutions (ASOSAI) in 2021, builds on the Moscow Declaration's principles and focuses on digital transformation for smart SAIs.

Both declarations recognize the potential of digital transformation to improve public administration and SAI performance. They encourage SAIs to adopt innovative technologies such as data analytics, artificial intelligence, and robotic process automation to enhance audit efficiency, accuracy, and effectiveness.

The Moscow and Bangkok Declarations emphasize the importance of capacity building and human resource development. Both documents urge SAIs to invest in training and development to equip their staff with the necessary skills and knowledge to leverage digital technologies in their work effectively.

Both declarations highlight the significance of addressing cybersecurity threats and data privacy concerns in the digital era. They call on SAIs to develop robust policies and procedures to protect sensitive data, ensure the resilience of their digital infrastructure, and comply with relevant data protection regulations.

The Moscow and Bangkok Declarations underscore the importance of international cooperation and knowledge-sharing among SAIs. They encourage SAIs to collaborate with other stakeholders, share experiences, and develop joint initiatives to promote the use of information technologies in public sector auditing.

Both declarations acknowledge that leveraging technology can enhance transparency and accountability in public administration. They urge SAIs to use digital tools to improve their communication with stakeholders, share audit findings, and promote the principles of good governance.

While the Moscow Declaration provides a global perspective on the role of technology in SAIs, the Bangkok Declaration focuses on the specific needs and challenges of SAIs in the Asian region. This regional focus enables the Bangkok Declaration to address unique concerns and opportunities for digital transformation in Asia, complementing the broader vision of the Moscow Declaration.

In conclusion, The Moscow and Bangkok Declarations aim to promote digital transformation in public sector auditing. By uniting SAIs under shared principles and objectives, these declarations foster collaboration, knowledge-sharing, and innovation in digital transformation. Through their collective impact, the Moscow and Bangkok

Declarations support SAIs in addressing global challenges and contributing to achieving the United Nations' Sustainable Development Goals.

Fabrício Ramos Neves et al. (2019) studied the four AI systems of the Brazilian Supreme Audit Institution (TCU) to fight against corruption. Currently, ALICE, ADELE, MONICA, and SOFIA are Artificial Intelligence (AI) systems proposed to aid auditing processes in the public sector. Since 2015 TCU has integrated these four AI systems into the auditing workflow (see figure 7).

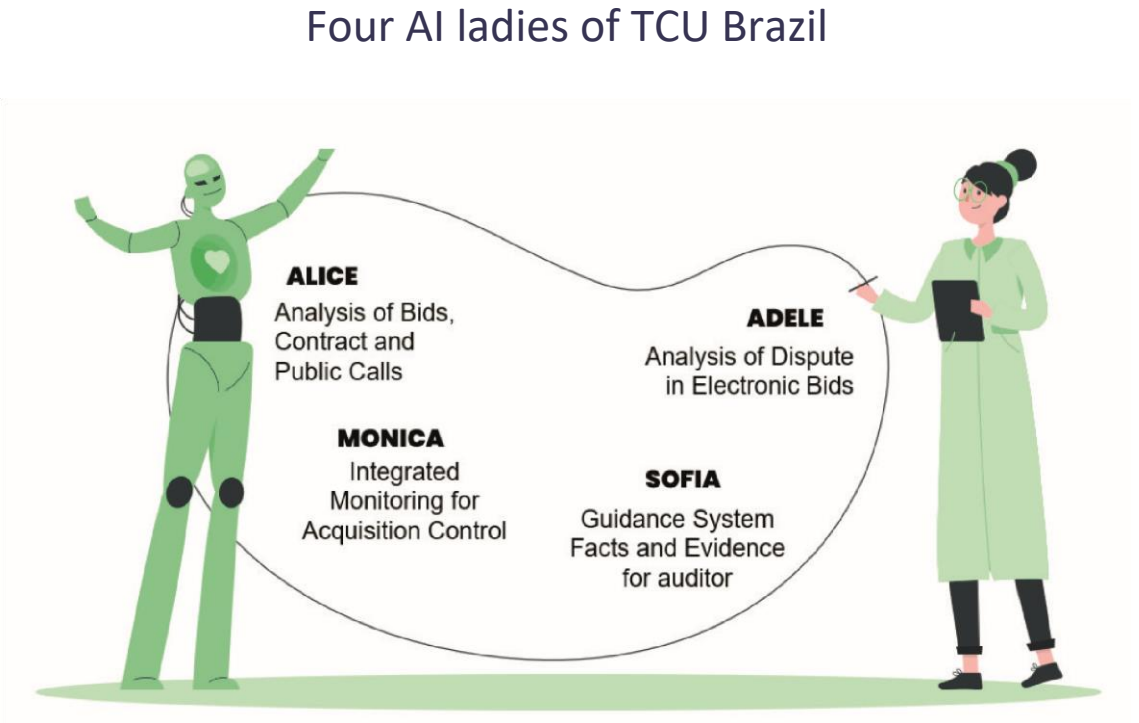


Figure 7 Four AI ladies of TCU Brazil

From figure 7, the TCU has used ALICE as the tender analysis platform to oversee government procurement processes. The recent report of FAPESP Innovative R&D showed that in 2021, it avoided more than BRL 504 million in losses to public coffers. In addition, TCU analysed evidence in the 2,000 new complaints and similar cases, mostly relating to public accounts, that come before the court every year.

Using AI for auditing could reflect the auditing development by the audit laboratory. For example, in 2019 National Audit Office of Finland (NAOF) proposed the Risk Detector AI pilot project. This project could help identify risky procurement, ensure the quality of audit work, and give the overall audit picture. The Risk Detector is the tool that guides the auditors in planning and targeting their work. In addition, it could identify potential risk cases: what procurement auditors should focus on. For example, AI could show the network of relations between purchasers and suppliers constitutes a bipartite network similar to Netflix or Tinder platforms. Also, risk detectors use data visualization.

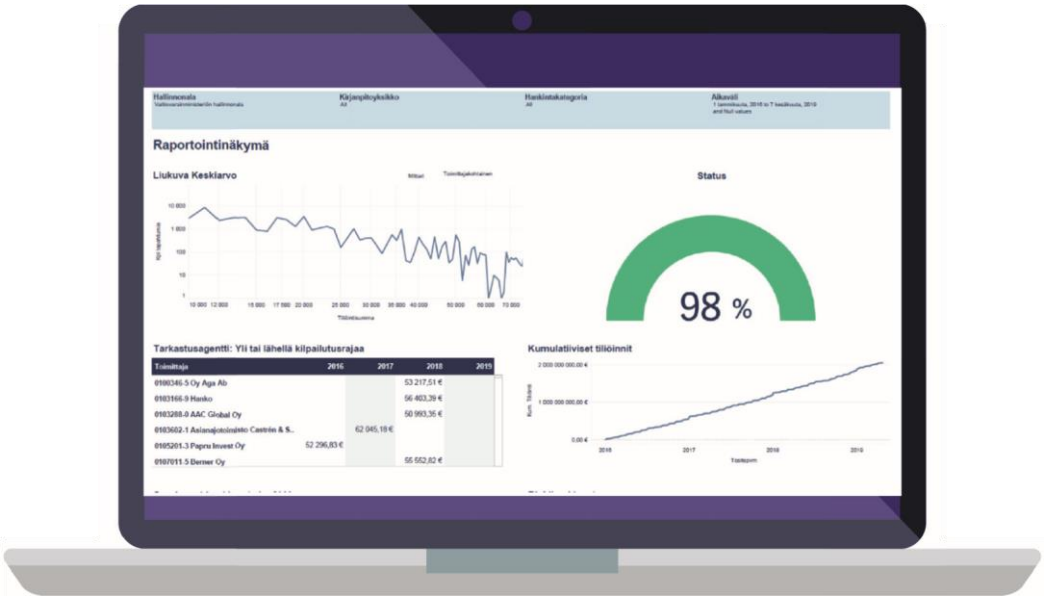


Figure 8 Risk Detector of National Audit Office of Finland

Source: PPT of Ines Gullichsen (SAI Finland) in ECA conference on Big and Open Data for European Union Supreme Audit Institutions.

Potential Obstacles

Even though SAIs recognize the benefits of AI for public sector auditing, we still face potential obstacles to adopting AI in the audit process. The article by Julian Torres Santeli and Sabine Gadon in World Economic Forum indicated five barriers to AI adoption in government and public entities (see figure 9).

Figure 9 Five Barriers to AI adoption in government and public entities
Source: Julian Torres Santeli and Sabine Gadon (2019)

From figure 9, the effective use of data shows the first potential obstacle. The public entities need to develop their dataset, which could reflect data reliability and

governance. Meanwhile, the second obstacle is low data literacy. Santeli and Gadon (2019) explained that government personnel in non-technical roles, such as department directors, policy-makers, and procurement officials, do not always have enough understanding of data and AI. This includes technical knowledge and, most importantly, knowledge of the legal and ethical implications of using vast amounts of data where the main concern is privacy. This makes it difficult for them to feel comfortable investing in the technology or be aware of existing laws that directly affect AI projects, such as data and privacy legislation.

The AI ecosystem and creating legacy culture are potential obstacles that could be barriers to AI implementation. Therefore, Santeli and Gadon (2019) suggested that governments need to involve newer players to utilize their considerable expertise and foster the growth of AI industry hubs that can contribute significantly to the local economy. This is another approach to creating the AI landscape in the future. Likewise, creating a legacy culture related to the agile approach. Comparing the private sector, a strong culture of experimentation encourages employees to innovate, and positive performance is rewarded. However, in government, there can be less encouragement for employees to take risks.

Santeli and Gadon (2019) raised the procurement mechanism as another potential barrier. They viewed that AI presents challenges that current procurement mechanisms do not address. The paper of CAHAI-PDG (2021) clarified that in case the AI system is not built in-house, it should be contemplated how to procure the technology. Since AI is an emerging technology, it can be difficult to define a route to market for requirements. Yves Ganest (2019:5) discussed the challenge that most organizations outsource their AI solutions. The paper of Yves Ganest mentioned the main challenge regarding auditors' skills. The required skill is data analytics.

The last potential challenge is related to AI biases. Yves Ganest (2019:5) explained that these biases are magnified by the limitations of neural network technology underpinning deep learning. As a result, some AI programs produce unexplained decisions and actions. These biases, called the "Black Box effect," has been recognized by the audit profession, and will be further explained in the "Machine Learning" section.

Organizational Changes Needed

The recent article by Carlos Santiso (2022) gave a comprehensive concept of organizational changes needed to prepare for the integration of AI in the public sector. Santiso explained the "three Ps" are fundamental for governments in pursuing AI: People, Partnerships, and Procurement.

Modified Three Ps of Carlos Santiso to integrate AI into public entities

The recent article by Carlos Santiso (2022) gave a comprehensive concept of organizational changes needed to prepare for the integration of AI in the public sector. Santiso explained the "three Ps" are fundamental for governments in pursuing AI: People, partnerships, and procurement.

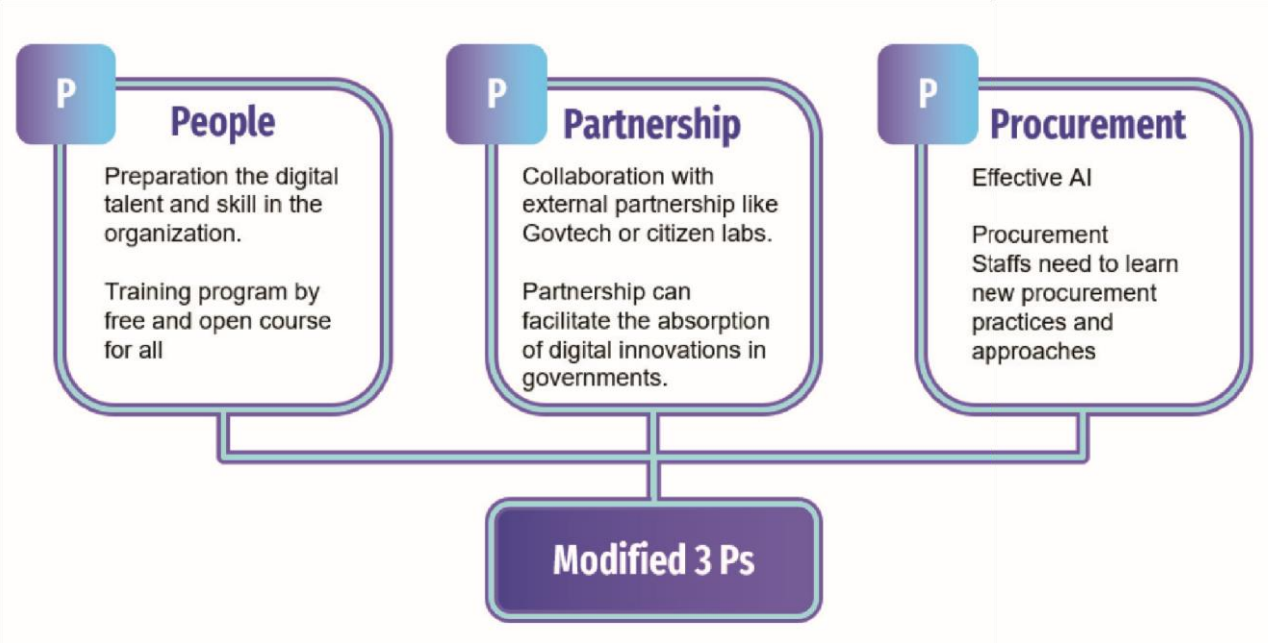


Figure 10 Modified Three Ps of Carlos Santiso to integrate AI into public entities. Source: Carlos Santiso (2022)

Emerging technologies make the increasing wealth of available data and are re-thinking traditional public accountability and the roles of these actors. Therefore, the paradigm shift of SAIs will lead to algorithm accountability in the future. According to the rapid growth of AI, SAIs needs to ensure AI is used responsibly, trustworthy, and ethically. Santiso (2022) borrowed the definition of algorithm accountability from the Ada Lovelace Institute, AI Now Institute, and Open Government Partnership. He concluded that algorithm accountability represents ensuring those that build, procure, and use algorithms are eventually answerable for their impacts.

Expected Benefits and Costs

In conclusion, three main benefits are expected from integrating AI in the audit process. First, AI could improve audit efficiency, lowering the cost of audit products. Second, AI could improve audit quality. And third, AI could reduce the audit workforce, especially entry-level employees. However, SAIs should concern about the expected costs of integrating AI in audit workflow. The main costs have consisted of:

(a) investing in AI infrastructure (digital infrastructure),
(b) costs of cloud computing and open source,
(c) preparing an agile approach to AI procurement,
(d) enhancing cybersecurity capabilities,
(e) developing collaboration with external partnerships,
(f) engaging with AI experts,
(g) redesigning workflows to improve efficiency,
(h) monitoring systems to identify unintended consequences.

Pros and Cons

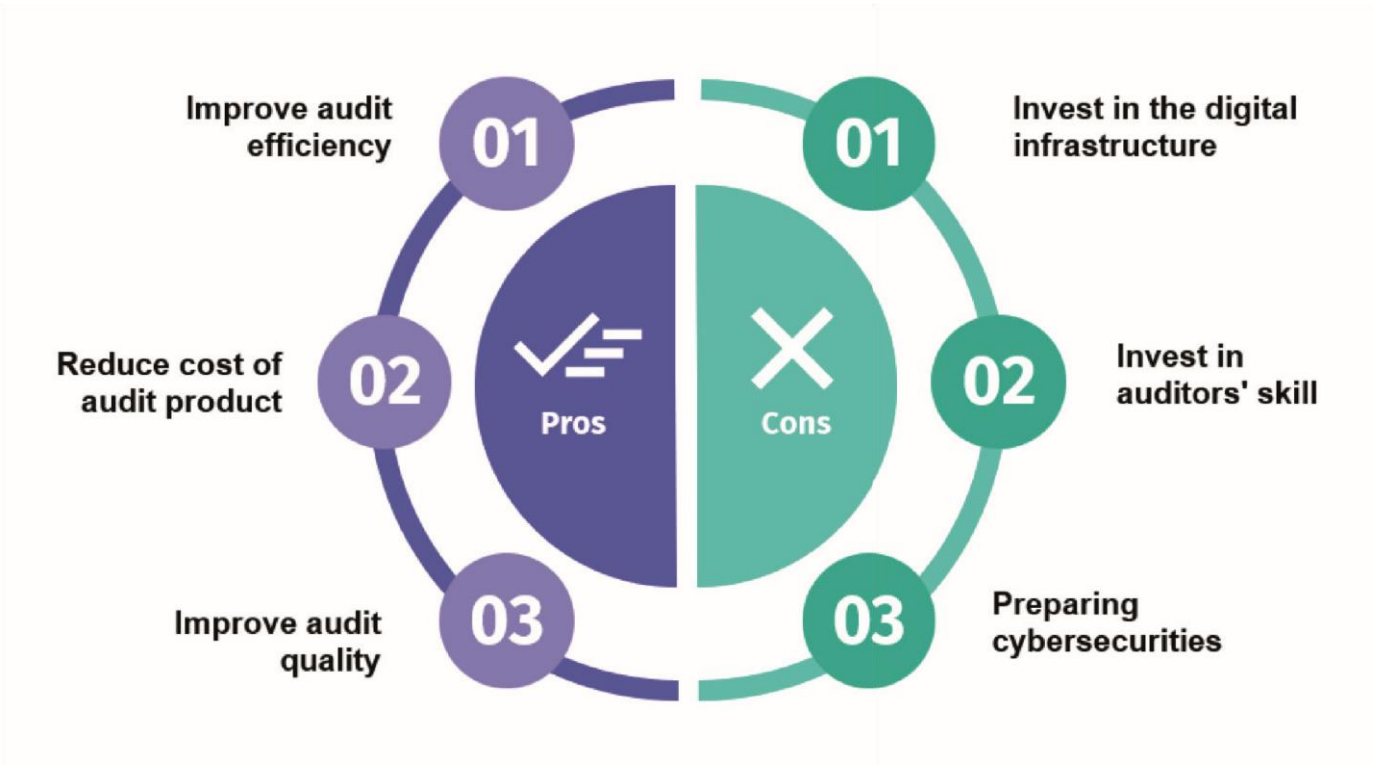


Figure 11: Expected Benefits and Costs for integrating AI for SAI

Cybersecurity

To create and maintain robust cybersecurity, SAIs can take the following steps:

- **Develop a cybersecurity strategy:** SAIs should create a comprehensive cybersecurity strategy that outlines their approach to identifying, protecting, detecting, responding, and recovering from cyber threats. This strategy should be aligned with the organization's overall objectives and risk management framework.
- **Establish a dedicated cybersecurity team:** SAIs should establish a dedicated team of cybersecurity professionals responsible for implementing, monitoring, and maintaining the organization's cybersecurity measures. In addition, this team should work closely with other departments to ensure a coordinated approach to cybersecurity.
- **Implement cybersecurity policies and procedures:** SAIs should develop and enforce robust cybersecurity policies and procedures that govern information systems, networks, and data use. These policies should cover access control, data protection, incident management, and user awareness training.
- **Invest in cybersecurity training and awareness:** SAIs should provide regular cybersecurity training and awareness programs for their staff to ensure they understand the risks and their responsibilities in maintaining the organization's cybersecurity posture. This training should be tailored to different roles and responsibilities within the organization.
- **Conduct regular risk assessments:** SAIs should perform regular risk assessments to identify, analyze, and prioritize potential cyber threats and vulnerabilities. This process should inform the organization's risk management activities and help prioritize cybersecurity controls and measures investments.
- **Implement technical controls:** SAIs should deploy a range of technical controls to protect their information systems and data. These controls may include firewalls,

intrusion detection and prevention systems, encryption technologies, and secure configurations for hardware and software.

- **Monitor and respond to incidents:** SAIs should establish processes for monitoring their information systems and networks for potential cybersecurity incidents. When incidents are detected, they should have a clearly defined incident response plan to manage and effectively contain the situation.
- **Collaborate with external partners:** SAIs should collaborate with other government entities, private sector organizations, and international partners to share cybersecurity best practices, threat intelligence, and resources. This collaboration can help SAIs stay informed about emerging threats and improve their overall cybersecurity posture.
- **Regularly review and update cybersecurity measures:** Cyber threats and technologies evolve rapidly, and SAIs should continuously review and update their cybersecurity strategies, policies, and controls to ensure they remain effective and aligned with the organization's objectives.
- By taking these steps, SAIs can create and maintain a strong cybersecurity posture that protects their information systems, data, and work integrity. This, in turn, helps them to fulfill their mandate of ensuring the effective and transparent use of public resources.

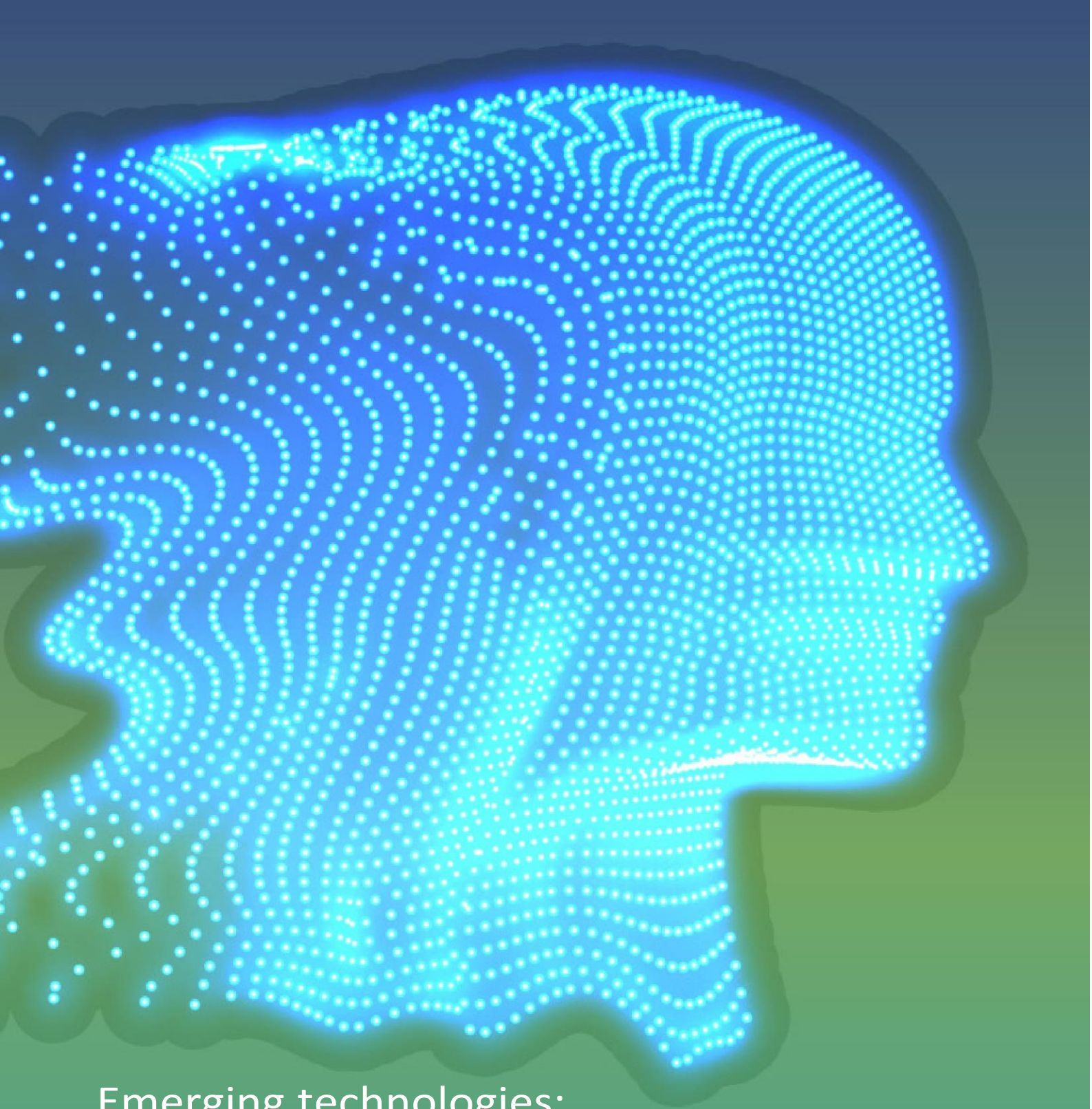
Challenges of Science and Technology in the audit process

SAIs can take to prepare auditors for the challenges of science and technology in the audit process:

- **Training programs:** SAIs should invest in comprehensive training programs that cover relevant scientific and technological topics. These programs should be tailored to the needs of auditors and can include workshops, seminars, and e-learning courses. By offering continuous training and development opportunities, SAIs can ensure that their auditors stay up-to-date with the latest advancements and can incorporate them into their work.
- **Collaboration with experts:** SAIs should collaborate with subject matter experts from academia, research institutions, or the private sector to gain insights into the latest scientific and technological developments. These experts can provide valuable guidance and support to auditors during the audit process, ensuring they understand and accurately assess the impact of scientific and technological factors on the entities they audit.
- **Interdisciplinary teams:** SAIs should consider creating interdisciplinary audit teams that include auditors with specialized knowledge in science and technology. These teams can work together to address complex audit issues that involve the intersection of technology, science, and public administration.
- **Knowledge-sharing platforms:** SAIs should establish knowledge-sharing platforms, such as internal databases, forums, or newsletters, to facilitate the exchange of information and best practices related to science and technology among auditors. This can help build a culture of continuous learning and foster innovation within the organization.
- **Participation in conferences and seminars:** Encourage auditors to attend relevant conferences and seminars in their fields of interest. It allows them to stay informed about the latest developments in science and technology and network with professionals and experts in their areas of expertise.
- **Partnerships with other SAIs:** SAIs should foster partnerships and collaborations with other SAIs with experience or expertise in specific scientific and technological domains. These partnerships can lead to joint audits, knowledge-sharing initiatives, or capacity-building programs that benefit both parties.
- **Certification and accreditation programs:** SAIs can encourage auditors to pursue certification and accreditation programs in relevant fields of science and technology.

These programs can help auditors build their expertise and demonstrate their commitment to staying current with the latest developments.

- **Monitoring and evaluation:** SAIs should establish mechanisms to monitor and evaluate the effectiveness of their efforts to familiarize auditors with science and technology. This can help identify areas for improvement and ensure that auditors are well-prepared to address the challenges posed by scientific and technological advancements in their work.
- By taking these activities, SAIs can prepare their auditors to navigate the complexities of science and technology in the audit process, ensuring they continue to provide high-quality, relevant, and effective audits in the face of rapid technological change.



Emerging technologies: Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

Machine Learning

INTOSAI Working Group on Impact of Science and Technology (WGISTA)
Prepared by the Office of the Comptroller General of the Republic of Chile

Machine Learning

Basic Definition

Artificial Intelligence and Machine Learning are fast growing Data Analytics technologies with great actual and potential use for the SAI´s on their mission of preventing and controlling corruption and fraud in the public sector.

There is no consensual definition of "Human Intelligence", consequently "Artificial "Intelligence", understood as the attempt to artificially reproduce that attribute on a non-human entity, is not precisely defined either.

But, as a work definition, we will understand Artificial Intelligence as technologies that try to provide intelligence-like behavior to machines (or machine-like systems).

While the notion of thinking machines may be much earlier, we can say that the concept of artificial intelligence was developed by science fiction writers in the first half of the 20th century, as a capability of robots.

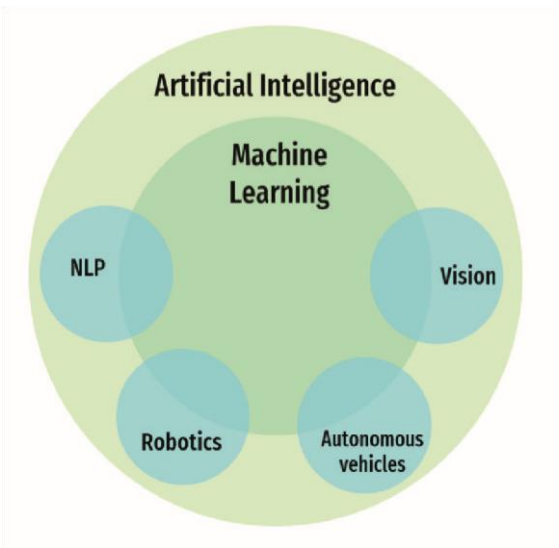
An alternative and more formal definition of AI could be: "a system's ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation".

Machine Learning in this context, is one way of implementation of Artificial Intelligence. It was defined in the 50's as "the field of study that gives computers the ability to learn without explicitly being programmed.".

Given these general definitions, we understand Machine Learning as a subset of AI technologies that specifically focus on obtaining the expected intelligence-like behavior through learning, which is, by itself, an intelligent-like behavior.

Thus, Machine Learning implies that the machine has the ability to remember and modify its behavior from experience. Machine Learning relates with other AI technologies to realize even wider goals, as represented in the figure below, for example assisting human-machine communication through Natural Language Processing (NLP), manufacturing (through Robotics), transportation (through Autonomous Vehicles) and computer Vision.

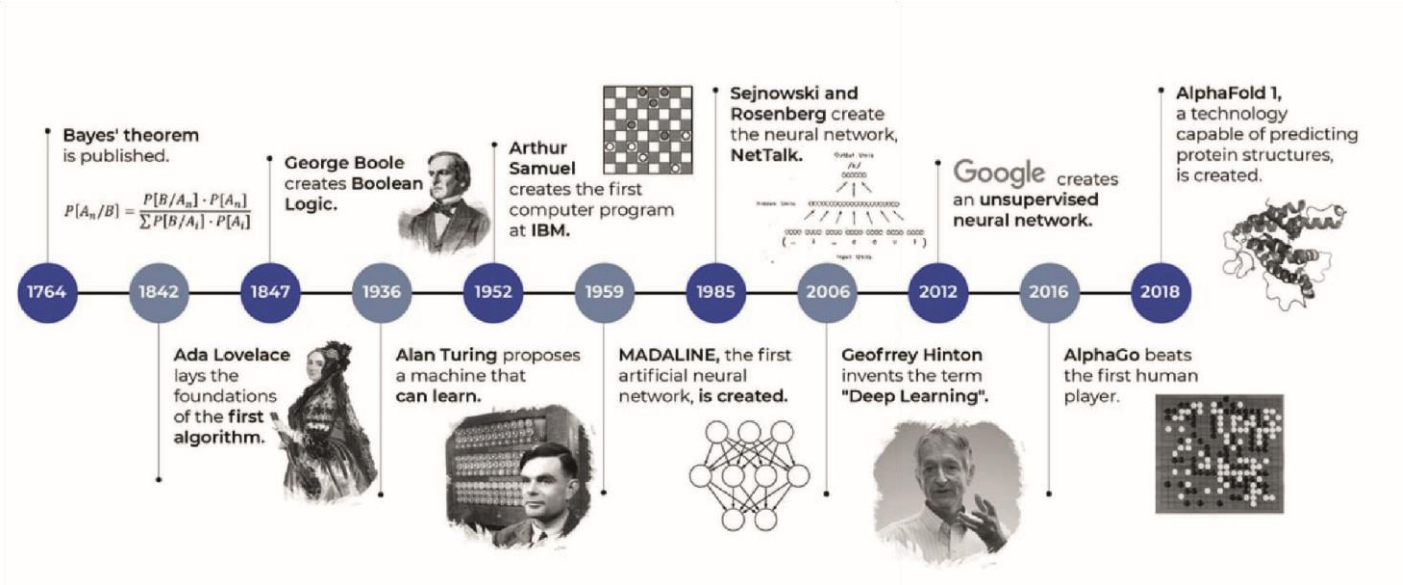
Use of emerging technologies



state of the art in the use of emerging technologies in the public sector. OECD, 2019

Evolution of Machine Learning

Machine learning timeline



Source: https://www.algotive.ai/

Although ML development really took off starting in the 20th century, it's only fair to acknowledge the crucial contribution made by inventors and mathematicians in earlier centuries, including Wilhelm Schickard, Thomas Bayes, Charles Babbage, and Ada Lovelace.

About 1643 Schickard, besides devising machines for other purposes, invented a mechanical calculator and a machine for learning Hebrew grammar.

Around 1760, Thomas Bayes, laid the statistical foundations required to develop Machine Learning.

In 1822 Charles Babbage conceived and partially built an analytical machine capable of running a computation program.

By 1830 Ada Lovelace, a British mathematician, developed the first algorithm, together with Charles Babbage. She also introduced the concept of a universal machine that could be programmed and reprogrammed to process symbols, words and even music.

Time later, by 1936, the English mathematician Alan Turing -later recognized as the father of AI- worked professionally on the same concept and in 1941 developed a code breaking machine called The Bombe for the British government, with the purpose of deciphering the Enigma code used by the German army in the Second World War.

The powerful way in which The Bombe was able to break the Enigma code, a task previously impossible to even the best human mathematicians, made Turing wonder about the intelligence of such machines.

Turing suggested that, as humans do, machines can use available information as well as reason (or logic) to solve problems and make decisions.

He also devised a test to identify intelligence of an artificial system: if a human is interacting with another human and a machine and unable to distinguish the machine from the human, then the machine is said to be intelligent.

From then on, AI was established as an academic discipline but remained an area of relative scientific obscurity and limited practical interest for over half a century, despite experts predicting that in a few years an intelligent machine would be produced.

One limitation for further progress was computing machinery, which needed a fundamental change. Before 1949 computers lacked a key prerequisite for intelligence: they couldn't store commands, only execute them, so they couldn't remember what they did. Second, computing was extremely expensive. In the early 1950s, only prestigious universities and big technology companies could afford the big computers required to research AI.

Another problem was the approach that had been used in earlier attempts: Writing precise instructions on how to process information and make decisions to carry out specific tasks. In other words, teaching computers to reason abstractly. But this proved too complex, and progress was stagnant.

Research at this point then began to pursue algorithms that could teach themselves how to execute the tasks, relying on statistics. This approach is what we specifically recognize as Machine Learning (ML) and requires increasingly powerful computers. Only in the past few decades computers with enough storage and processing power for the approach to work became available. The rise of cloud computing and customized chips has powered an exponential progress that produces breakthroughs at astounding rates.

Many ML algorithms are based on a technique called artificial neural networks (ANNs). These are biologically inspired networks of artificial neurons, or brain cells, developed by neurophysiologist Warren McCulloch and psychologists Walter Pitts and Frank Rosenblatt in the 40's and 50's to classify, explain and model pattern recognition skills in images.

The concept was extended in the 70's giving rise to the development of Deep Learning, understood as a subset of Machine Learning, dealing with large-scale processing of ANNs in many levels whose performance is scalable.

During the 1960s and 1970s, increasingly advanced algorithms and procedures were developed to set up learning, until the 1980s when more and more ambitious specific applications began to appear, like autonomous vehicles and speech recognition.

Since the 2000s with the advent of cloud computing, coupled with collaborative open-source concepts and huge investments by corporations and countries, more and more advanced applications have been pushed at a constantly accelerating pace, without anticipated limits.

Resources required for Machine Learning

Human resources requirements for Machine Learning

To implement successful machine learning projects, a team of qualified professionals must be assembled.

Many organizations wonder about leveraging non-specialist data scientists – analysts who have been trained in some specific AI/ML techniques – to power their ML transformations. But based on experience and given the significant challenges involved in applying AI/ML algorithms – including challenges with framing the problem, correlation vs. causality, bias in datasets, and information leakage – it is essential for an institution to achieve its AI/ML transformation assembling a strong, core, technical AI/ML team. This technical team will be central to unlocking the greater value expected from the most complex applications. It can be said that the science of AI is still too early in its development cycle to be entrusted to a non-technical team of nonspecialist data scientists and developers.

Nonetheless, there is a strong need for non-specialist data scientists to produce significant value from a long tail of less complex AI problems. But these personnel must be complemented and supported by a core, seasoned technical team.

Hardware Requirements for Machine Learning

Choosing the right hardware to train and operate machine learning programs will greatly impact the performance and quality of a machine learning model. Most modern institutions have transitioned data storage and compute workloads to cloud services. Many institutions operate hybrid cloud environments, combining cloud and on-premise infrastructure. Others continue to operate entirely on-premise, usually driven by safety and confidentiality considerations.

Cloud-based infrastructure provides flexibility for machine learning practitioners to easily select the appropriate compute resources required to train and operate machine learning models.
The processor is a critical consideration in machine learning operations. The processor operates the computer program to execute arithmetic, logic, and input and output commands. This is the central nervous system that carries out machine learning model training and predictions. A faster processor will greatly reduce the time it takes to train a machine learning model and to generate predictions.

In addition to processor requirements, memory and storage are other key considerations for the AI/ML pipeline.
To train or operate a machine learning model, programs usually have data and code to be stored in local memory to be executed by the processor. Some models, like deep neural networks, may require faster local memory because the algorithms are larger. Others, like decision trees, may be trained with less memory because the algorithms are smaller.

However, cloud storage in a distributed file system can remove any storage limitations that were imposed historically by local capacities. Nonetheless, AI/ML pipelines operating in the cloud still need careful design of both data and model stores.

Software Requirements for Machine Learning

Machine learning software is any dedicated tool used for artificial intelligence, self-iteration based on data, unsupervised or supervised learning, and other ML classifiers. Much software at work today has elements of machine learning, like in email filtering and computer vision.

There is also machine learning specialty software for things like simulation, recruitment, architecture, and accounting. Some ML toolkits, can be custom-built to adapt to the unique data sets and workflow needs of a specific project.

There are several machine learning software applications available on the market, a list that has grown daily in recent months. Each project or institution will choose its particular mix of ML and general supporting software for its medium-term needs, with the expectation that new and better applications will soon appear on the market, so that reinvestment in some of them will be necessary.

Privacy, ethics, and confidentiality issues

Machine Learning, as a subset of Artificial Intelligence and in the context of the public sector, presents three major areas of concern for society:

- Ethical issues, as for instance, bias and discrimination
- Legal issues, including privacy and surveillance
- Governance issues, the existing governance and compliance structures within the audit institutions.

All these concerns are circumscribed within an environment dependent on human judgment. Using Machine Learning (ML) in auditing, to fight against corruption and fraud, raises a wide range of challenges regarding ethical, legal and governance issues.

One of the biggest challenges is figuring out how to convert broad ethical principles such as fairness, equity, privacy, transparency, accountability, and human safety to specific deployments. These principles sometimes even conflict with one another, and SAIs need to define their meaning in the context of the relevant system and specify how to judge Machine Learning algorithms accordingly.

Codes of ethics are essential in public institutions around the world, and those codes are being expanded to address the development and use of machine learning.

Thus, there is already momentum in some quarters for government regulation of ML that address ethical concerns. By 2016 the EU established a regulation for Data Protection (GDPR) and in October 2020, the European Parliament adopted a legislative initiative urging the European Commission “to present a new legal framework outlining the ethical principles and legal obligations to be followed when developing, deploying and using artificial intelligence, expanded to address the development and use of Machine Learning. robotics and related technologies in the EU including software, algorithms and data”.

In 2021 the US GAO published “Artificial Intelligence- An Accountability Framework for Federal Agencies and Other Entities”, with the purpose “to identify key practices to help ensure accountability and responsible AI use by federal agencies and other entities involved in the design, development, deployment, and continuous monitoring of AI systems”.

Other AI frameworks by public organizations have been issued by UNESCO, the OECD and China's government, among others. They usually cover privacy and data governance, accountability and auditability, robustness and security, transparency and explainability, fairness and nondiscrimination, human oversight, and promotion of human values.

Given the above developments, any audit institution that is considering using anti-corruption machine learning should review its relevant codes of ethics to see whether and how those codes address the ethical dimensions of machine learning, with reference to the principal categories of ethics-related issues.

The main ethical issues that need to be considered in relation with ML applications are schematized in the picture below:

Source: Prepared by the author

There is general agreement that ethics should be built into the design and development process of machine learning applications from the outset.

The design of any ML system must be performed in a responsible, safe and secure way. Its use shall comply with the same quality standards along all its life cycle.

An ongoing risk Management program must be implemented in which potential risks that ML systems pose are continually assessed, addressed, and managed, commensurate with their expected impact. Audit Institutions need to plan for such a program for any ML application that it deploys, including appropriate training for risk and compliance officers.

Additionally, having an evidence-based assessment built into the process is key for responsible ML. It is vital to collect evidence on how the app affects people. Effective evaluation must go hand in hand with good product design. Having clear data analysis and policy evaluation will inform ML design and implementation, leading to products that are safer, fairer, and more effective in achieving their goals.

The issue of transparency concerns the responsible disclosure around ML systems, to ensure that people understand ML-based outcomes and can challenge them.

To maximize algorithmic transparency and accountability, audit institutions should:

- Be aware of the possible biases involved in ML solutions' design, implementation, and use.
- Seek to have their systems using algorithmic decision-making produce explanations regarding both the procedures that the algorithm follows and the specific decisions that the solution makes. This is usually called "explainable AI"
- Have the builders of the algorithm maintain a description of the way in which the institution collected the training data and an exploration of the solution's potential biases.
- Record models, algorithms, data and decisions for auditability purposes.
- Use rigorous methods to validate their models and document those methods and results.

Data Privacy pertains to the need for the collection, processing, use, and transfer of personally identifiable data by ML systems. They should comply with relevant data privacy laws and regulations.

The European Union General Data Protection Regulation (GDPR) can be considered a relevant reference in this area. It covers seven key principles regarding personal data:

Source: Prepared by the author

Many other nations across the world have adopted or are considering legislation similar to GDPR. Legislation on data privacy is also gaining support in the United States both at the Federal and the State levels.

Virtually every system today confronts the cybersecurity threat and the systems architect need to ensure that the use of machine learning on auditing "should include effective cyber and physical security to mitigate the risk of data theft and to promote trust".

In addition to the challenge of storing, moving and processing large datasets within the organization, public sector institutions using these technologies need to understand that machine learning can create new and different cybersecurity challenges that may not be obvious even to data scientists. One example is the phenomenon known as unintentional memorization where certain neural network models that classify or predict sequences of natural-language text have unintentionally "memorized" certain text sequences containing sensitive personal data in documents that were part of the training dataset.

Responsible use also includes considering legal constraints. Obviously, machine learning should not be used for dangerous purposes or activities that are otherwise illegal. Legal areas within the institution implementing ML solutions should evaluate legal risks that may arise. Legal risks can include machine learning solutions generating outputs that result in unjustifiably discriminating against individuals based on categories such as gender, race, and ethnicity.

Machine Learning technology applied for auditing

When talking about Machine Learning for auditing purposes, each SAI must think about two main issues: What type of audit is to be performed and what type of fraud risk assessment problem we wish to solve by using these algorithms.

Regarding the first question, according to the International Standards of Supreme Audit Institutions (ISSAI's), there are three main groups of audits:

Financial audits: Focuses on whether the financial statements of the audited institutions are true and fair.

Compliance audits: Check if the audited entity has followed the regulations and laws of their respective countries.

Performance audits: To assess the government undertakings, systems, operations, programs, activities or organizations operating in accordance with the principles of economy, efficiency and effectiveness.

Regarding the second question, there is a great variety of fraud schemes and methods, which requires dynamism in the detection and analysis of new cases. According to the Association of Certified Fraud Examiners (ACFE), Occupation fraud is the most costly and common type of fraud in the world. It is defined by ACFE as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets".

The three main categories of occupational fraud are Asset misappropriation with 86% of cases, (according to the ACFE 2022, of a study made to 133 countries with a total of 2.110 cases). However, it has the lowest cost of the three categories, with a loss of USD 100.000 per case.

On the other hand, financial statement fraud has the most significant median loss with USD 593.000 dollars, but the lowest percentage of schemes (only 9%). The third category, Corruption, has 50% of cases and a median loss of USD 150.000 per case.

Another aspect to consider for Machine Learning training algorithms are the electronic sources for their analysis. Some countries are still under their digital transformation and their

documents are physical. When it comes to electronic documents it can involve the creation or alteration of fraudulent documents or files.

An auditor has to differentiate between structured and unstructured data, to apply a Machine Learning algorithm. Structured data is well defined information stored in rows and columns that can be searched, sorted and analyzed. On the other hand, unstructured data can come to the form of images, audios or social media data. As a first stage for creating ML models, structured data is the most efficient resource to train algorithms.

Another important concept is the difference between Supervised Learning and Unsupervised Learning. Supervised Learning has information already labeled (E.g. Fraudulent or not fraudulent) that will help to learn and train the algorithm. Unsupervised Learning does not need that labeled guidance.

Parameter	Supervised Learning	Unsupervised Learning
Dataset	Labeled Dataset	Unlabeled Dataset
Method of Learning	Guided learning	The algorithm learns by itself using dataset
Complexity	Simpler method	Computationally complex
Accuracy	More Accurate	Less Accurate

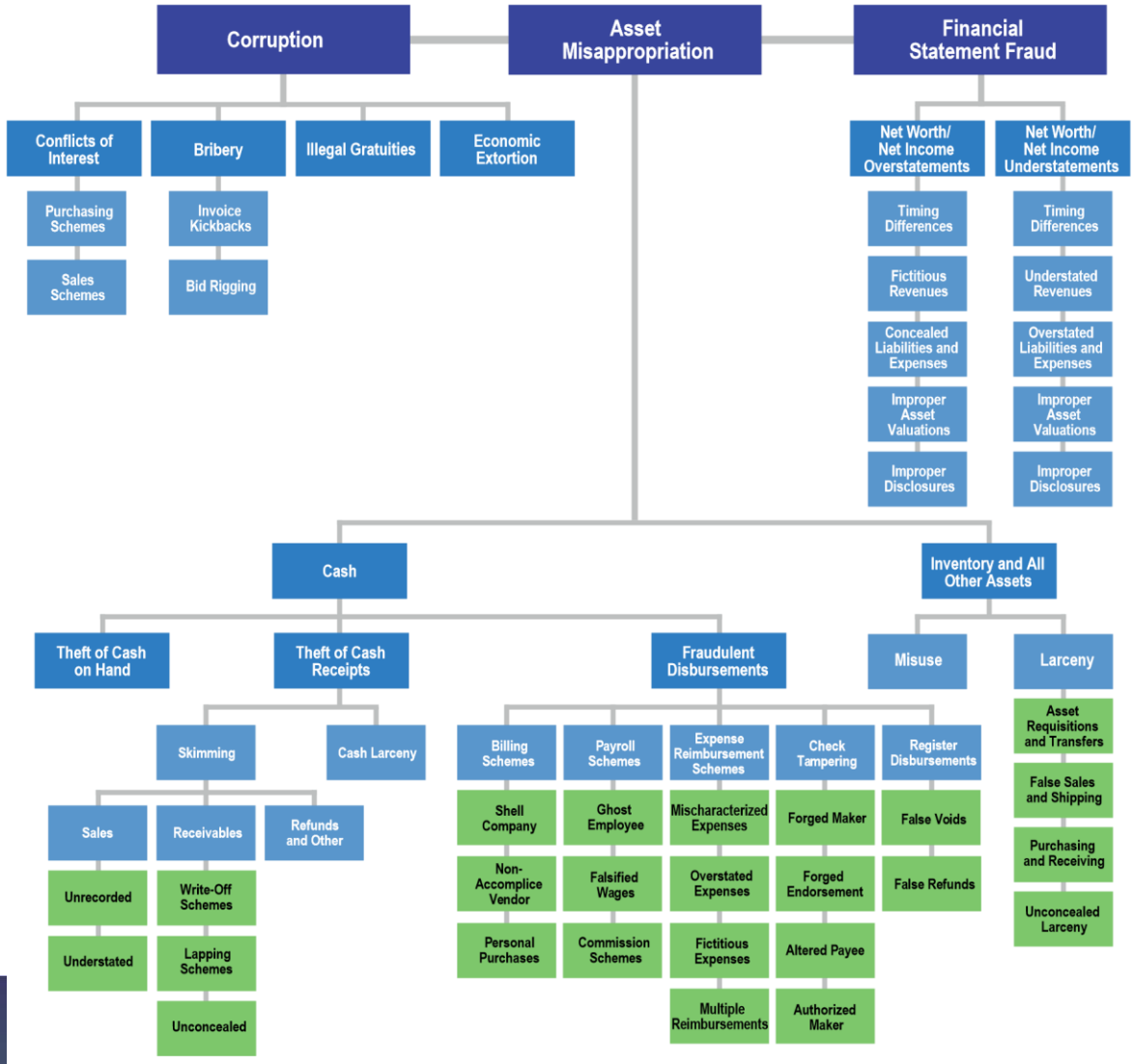
Source: https://www.edureka.co/blog/unsupervised-learning/

Fraud Schemes Analysis

Computational power can detect suspicious patterns faster than humans, reducing the manual review time. In the following fraud detection tree, there are three main types of schemes: Corruption, Asset misappropriation and Financial State Fraud. All these methods and behaviors have a potential use for machine learning algorithms.

THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM



Source: Association of Certified Fraud Examiners (ACFE)

Machine Learning most popular algorithms

From all the possible ML algorithms, a question arises at the moment to select the “right” algorithm. It will depend on the amount of data available and the audit purpose, as mentioned before.

Linear Regression (Supervised Learning - Regression)

There are many factors entailed in a fraud case, and the combination of several of those factors can lead to a fraudulent risk activity. Linear regression can help to understand individual variables and their impact on fraud.

Logistic Regression (Supervised Learning - Classification)

It will analyze a set of independent variables to determine an outcome. There will only be two possible outcomes (binary dependent variable). Some use cases are identifying risk factors, word classification.

Naive Bayes Classifier (Supervised Learning - Classification)

Mostly used for document classification, spam filters and sentiment analysis (texts with positive or negative impressions). This classification method is easy to build and accepts large data sets. It assumes the independence of all variables (even if they are dependent) so they all work in their own probability to get an outcome. The main disadvantage is their precision.

K-Nearest Neighbors (Supervised Learning)

This algorithm is used in image and video recognition, stock analysis and handwriting detection applications. It takes labeled points of data to label other points. The methodology is to make a voting system from its nearest neighbors. The "k" is the number of neighbors it checks. The advantages are the simplicity in implementation and it works well with noisy data. The main disadvantage is the elevated computer costs.

Decision trees (Supervised Learning - Classification/Regression)

It's a flow chart tree structure with nodes and branches that represents the different decisions taken and their outcomes. A model can be trained giving a set of rules to create a predictive model on frauds committed to an organization.

Artificial Neural Networks, ANN (Reinforcement Learning)

It is composed of a series of "units" or elements, interconnected by layers that work together to detect hidden relationships in data. It is based on the idea of biological systems, like the neurons of the human brain and are very helpful to solve non-lineal relationships or high dimensional data. It can also provide among fraud or non-fraud transactions.

Machine Learning most popular algorithms

	TYPE	NAME	DESCRIPTION	ADVANTAGES	DISADVANTAGES
Linear		**Linear Regression**	**The "best fit" line** through all data points. Predictions are numerical.	Easy to understand — you clearly see what the biggest drivers of the model are.	Sometimes too simple to capture complex relationships between variables. Does poorly with correlated features.
		**Logistic Regression**	The adaptation of **linear regression** to problems of classification (e.g., yes/no questions, groups, etc.)	Also easy to understand.	Sometimes too simple to capture complex relationships between variables. Does poorly with correlated features.
Tree-Based		**Decision Tree**	**A series of yes/no rules based on the features**, forming a tree, to match all possible outcomes of a decision.	Easy to understand.	Not often used on its own for prediction because it's also often too simple and not powerful enough for complex data.
		**Random Forest**	Takes advantage of many decision trees, with rules created from subsamples of features. Each tree is weaker than a full decision tree, but **by combining them we get better overall performance.**	A sort of "wisdom of the crowd". Tends to result in very high quality models. Fast to train.	Models can get very large. Not easy to understand predictions.
		**Gradient Boosting**	Uses even weaker decision trees, that are increasingly **focused on "hard" examples**.	High-performing.	A small change in the feature set or training set can create radical changes in the model. Not easy to understand predictions.
Neural Networks		**Neural Networks**	Interconnected "neurons" that pass messages to each other. Deep learning uses several **layers of neural networks stacked on top of one another.**	Can handle extremely complex tasks — no other algorithm comes close in image recognition.	Very slow to train, because they often have a very complex architecture. Almost impossible to understand predictions.

Source: Machine Learning Basics: An Illustrated Guide for Non-Technical Readers. (2021). Dataiku.

International Applications

Public procurement

There have been historical efforts for the fight against corruption and one of the main concerns are public procurement markets, which are vulnerable to political connections (Titl & Geys, 2019; Titl et al., 2021), and collusion (Kawai & Nakabayashi, 2021; Baranek et al. 2021).

Attempts have been made with Machine Learning algorithms to identify procurement contracts misallocated due to corruption, potential conflicts of interest, or political connections. Decarolis & Giorgiantonio (2020) has used new indicators coming from Italian police investigations, in addition to judiciary cases or other indicators inferred from economic outcomes. They take information from the owners or top executives of winning contracts to see if they have been part of police investigations for corruption cases. Some machine learning algorithms applied were LASSO, Ridge regression, random forest and ordinary least squares (OLS) for comparison.

Corruption

Mazrekaj, Titl, and Schiltz (2021) trained a model to identify politically connected firms, by using all firms in Czechia in 2018. Some variables included members of boards who ran a political office, political donations made by the firm or their managerial boards. Five Machine Learning algorithms were used: Logit, Boosting, Random Forest, Ridge regression and LASSO. Results indicate that Boosting gave an 84,1% of accuracy in predicting which firms were politically connected, followed by a random forest algorithm.

In the field of Neural Networks, López-Iturriaga and Pastor (2018), used both economic and political factors to predict public corruption in Spanish provinces. They gathered information about criminal cases taken by their main newspaper “El Mundo”, and used a technique called SOM (self-organizing maps) to find patterns without a total understanding of the internal relationships.

In the area of Artificial Intelligence and Machine Learning, SAI Chile has executed some pioneering projects that form the basis of the strategic development in this area, two examples are shown:

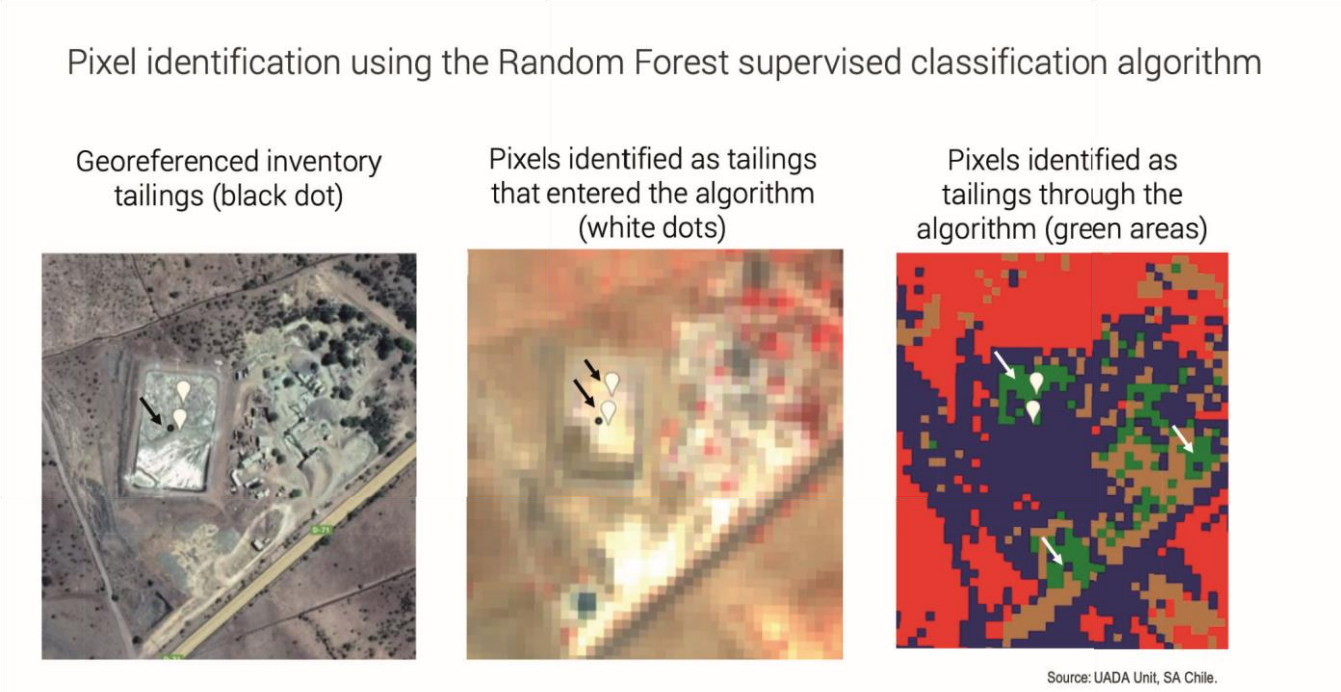
Mine tailings detection

This application consisted on using satellite images with machine learning techniques.

In coordination with the Regional Comptroller’s Office, an analysis work was carried out to identify possible tailings that were not part of the “Registry of Tailings Deposits in Chile” obtained from the website of the National Service of Geology and Mining (Sernageomin), dated updated August 10, 2020.

The platform used for the analysis was Google Earth Engine, in which a mosaic of images was configured between January 1 and December 31, 2021.

The Machine Learning technique used for pixel classification was the supervised classification algorithm called RandomForest, and the samples were defined from the georeferencing of the 389 tailings identified in the Sernageomin cadastral database.



Pixel identification using random forest supervised classification algorithm
Source: UADA Unit, SAI Chile 2022

As a result, 114 possible tailings were identified that are not inventoried in the 2020 Cadastre. It is currently in the field validation phase.

Natural language processing (NLP)

Another recent project used a Natural Language Processing algorithm to read and analyze SAI Chile´s webpage results from citizens reporting their allegations (GAO's FraudNet equivalent). The data to be analyzed was a sample of 15,157 observations, from an original file of approximately 40,000 observations, from January 1 to July 2, 2020.

The object was to identify if all allegations were derived correctly to their auditing departments.

Inconsistencies were detected by using this methodology. Five recommendations were sent to improve the website to receive quality data for the future.

Potential obstacles

As stated by Darrell West in "Using AI and Machine Learning to reduce government fraud" (2022), while ML tools exist for fraud detection and financial oversight, it is not always easy to implement them operationally, introduce new digital tools, or integrate them into Audit Institutions. There are several barriers to AI and machine learning innovation in SAIs and government agencies. For example, the procurement process is complicated and difficult for many agencies to supervise and expedite. Rules often require a lengthy and detailed sequence of activities that include defining the scope of the job, an analysis of task alternatives, requests for proposals, formal analysis of competing bids, and appeals process if losing competitors object to the way things were handled, among other things.

Many SAIs lack a procurement workforce with the skills necessary to purchase and assess ML algorithms. They have problems figuring out the best way to procure advanced technology products and services. One of the crucial decisions is whether to develop their

own software that is personalized to their own particular needs, buy proprietary software off the shelf, or rely on third-party developers. But in any of those alternatives, Audit Institutions need people who understand algorithms to make prudent decisions that yield actionable and scalable information.

In a 2020 publication (Engstrom, D. F., Ho, D. E., Sharkey, C. M., & Cuéllar, M. F. (2020)), the Administrative Conference of the United States reports that about half of government agencies' current ML applications were developed by in-house personnel customized to support their particular needs; the rest relied upon third-party or commercially available products. However, a number of the in-house solutions were not fully implemented, and it is not clear whether they were able to achieve stated objectives.

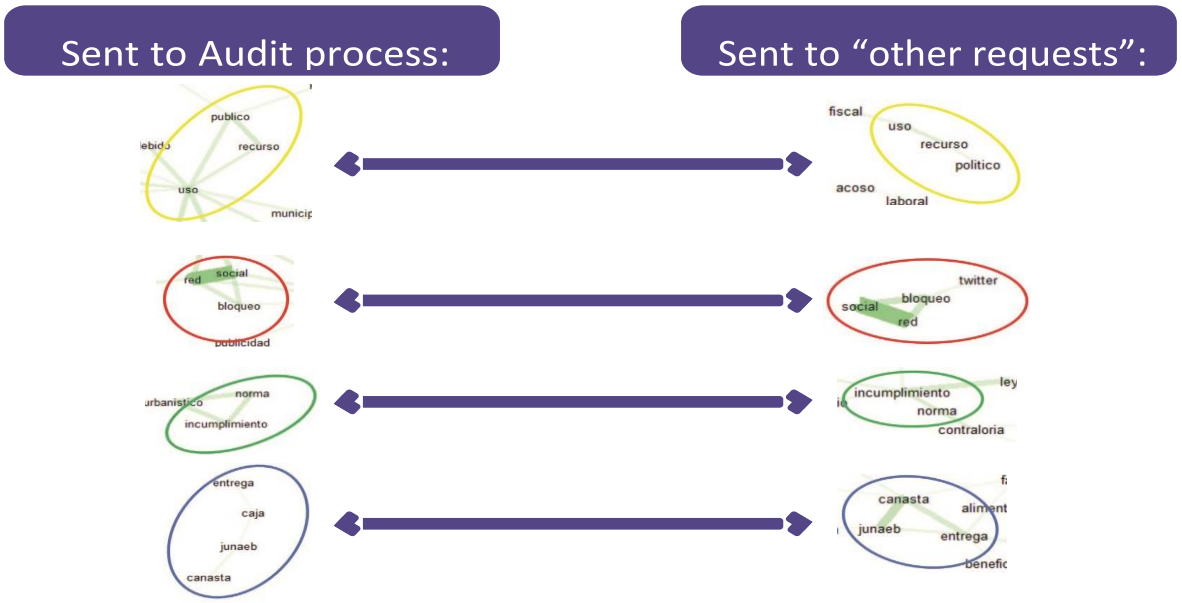
Within many agencies, there are cultural and structural barriers to change. These include a reluctance to innovate, preference for the status quo, fear of failure, being overly siloed so that different divisions handle various data and parts of essential missions, and not having leaders and managers who are skilled at facilitating change. In many organizations, the barriers to change are not just about the technology, but about the structure, operations, management, and culture of the agencies. Unless leaders are committed to building an innovation culture, the adoption of new technologies almost always will fall short of their intended benefits.

Organizational changes needed

Creating a culture of innovation

Creating a culture of innovation is one of the most challenging steps that government officials can undertake to break through bureaucratic inertia and encourage responsible ML adoption. They need to instill in their structures, operations, and management styles the idea that change is helpful, and experimentation is desirable. Pilot projects should be established for small-scale ML applications that do not compromise standard procedures but provide agency experience in algorithm development and deployment. Projects that prove successful can be scaled up and deployed more broadly.

It is difficult to know how to build these kinds of organizational cultures, but management leadership plays a key role. Government officials need to create "sandboxes" for experimentation that provide low-risk chances to design new products and services and test them in a limited way. This will help refine the products and reduce the problems when large-scale deployment takes place. It inculcates a culture of change that, in the long run, will improve agency operations and lead to a workforce that is willing to experiment, take acceptable risks, and learn how to deploy digital products more effectively.



Naturallanguageprocessinganalysisfor citizen'sreportingwebsite Source:UADAUnit,SAIChile

Scaling up innovation

It is crucial for institutional leaders to figure out how to safely scale up innovation. Private companies often develop new products and test them on pilot samples before extending them more broadly throughout the community. That helps them evaluate the deployment and learn how people are using and being affected by the new applications. It is a way to safeguard the innovation process and provide guardrails for product rollouts.

Audit Institutions need to develop similar processes. It is almost never a good idea to launch new software on millions of people simultaneously; there always are going to be bugs, defects, and unanticipated outcomes that inflict possible harms. Having processes that start small, identify problems, and mitigate them before large-scale deployment helps institutions avoid embarrassing failures.

SAIs need some permanent means of learning from one another. Right now, each country is reinventing the wheel and wasting valuable time on moving up the learning curve. They should share their best practices and take advantage of the successes and failures that each entity experiences. There is no reason for Audit Institutions to repeat the same mistakes in different settings when better communications and coordination could avoid particular problems.

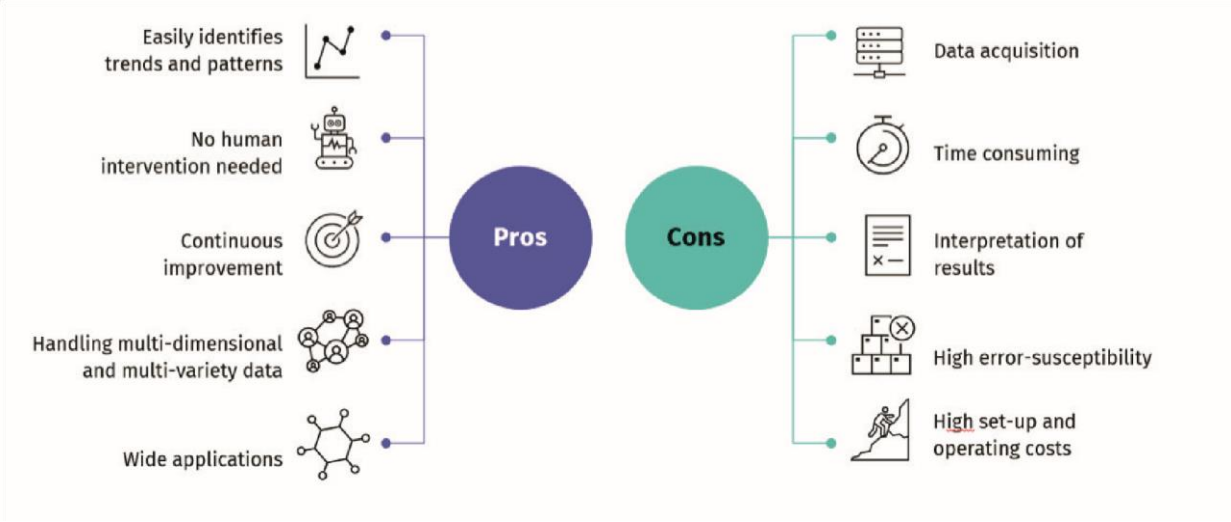
Expected benefits and costs

The general benefits offered by Machine Learning for any Institution, are the easy identification of trends and patterns when processing large volumes of data, that it does not need human intervention to set the logic of the solutions, that it improves continuously and that it can easily handle very complex data, like images and speech.

Initial versions of Artificial Intelligence were rule-based, on which the logic for system operation is set at the beginning and couldn´t easily be adapted to changes in the rules. Human knowledge is encoded in those rules through standard programming statements (like if-the else and loops). This approach is still in use, as it suits many applications, but for others it has been superseded by Machine Learning, where instead of a programmer the algorithm is created by

selecting an appropriate model or library and submitting it to a very large dataset. The algorithm then analyses the dataset and determines relationships within that data; logic is thus embedded in the algorithm without human coding. True to its name, the model trains itself and learns from the data, creating a cohesive relationship between data inferences and useful data outputs.

Pros and Cons of Machine Learning



Source https://data-flair.training/blogs/advantages-and-disadvantages-of-machine-learning/

Audit institutions from different countries should take full advantage of the benefits that have led corporations and private companies along the world to invest large resources in the development and use of IA technologies, particularly Machine Learning.

Given the general benefits offered by this technology, as outlined above, the specific benefits for audit institutions include the possibility of broadening the scope of audit processes, as well as speeding them up and increasing the quality of the results obtained.

Ultimately, the application of advanced technologies such as ML is an indispensable link to achieve the ultimate goal, which is to keep under control and aim at eliminating corruption and fraud in the public sector processes of countries.

The ability of ML applications to work with datasets too large for manual handling make it possible to reveal or even predict corruption or fraud that previously was nearly or completely impossible to detect.

Moreover, useful correction orientation can be derived from the experience to be gained, as AI assisted procedures can replace previously corruption-prone processes.
Despite its advantages, Machine Learning also has its drawbacks and limitations, the following being some frequently mentioned:

Data acquisition is very complex, since ML requires massive data to train the system. Moreover, this data should be unbiased, inclusive and of good quality possibly requiring a big effort and time for preparation.

The learning process can take a lot of time to achieve the desired level of relevance and accuracy. Great computer capacity must be put into action for real-life applications.

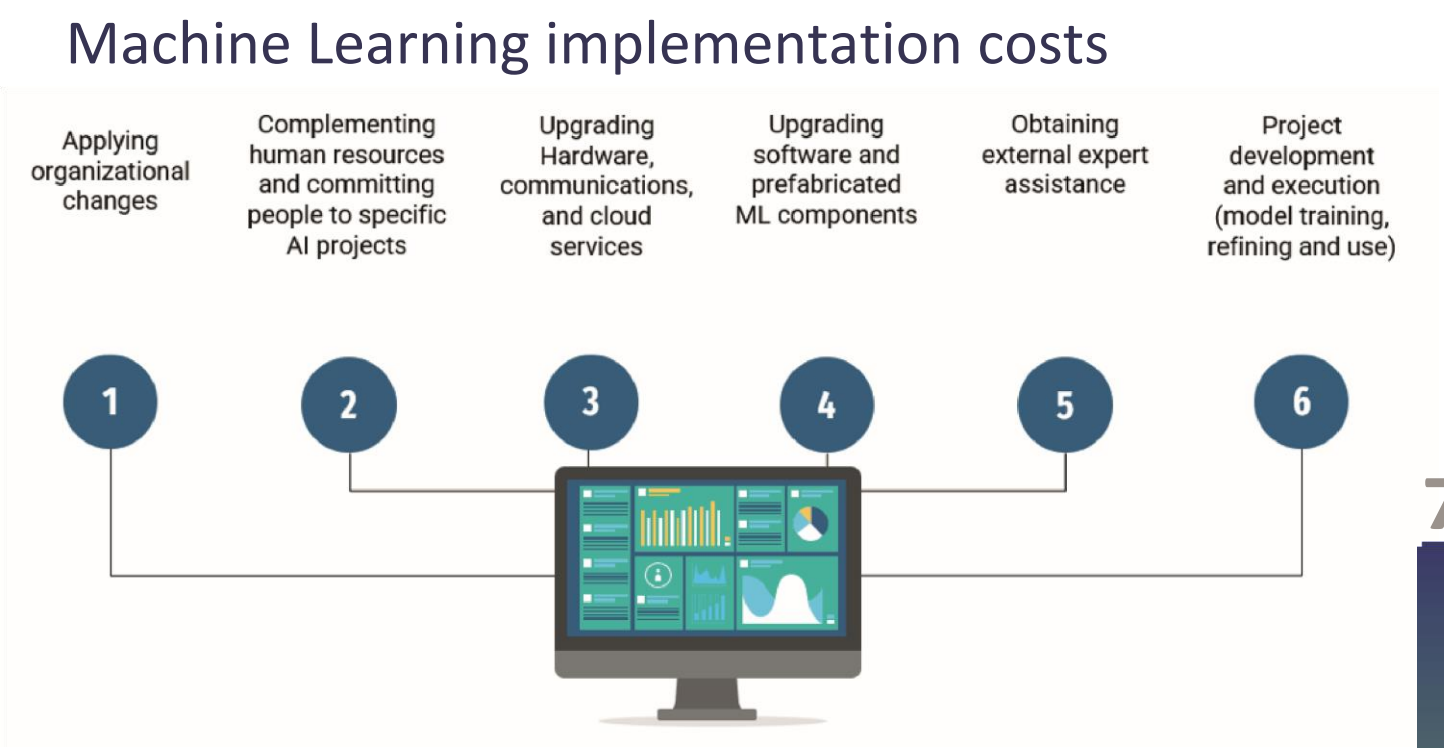
Results can be very sensible to the algorithm that are put in place, and its proper interpretation can be difficult.

Despite its autonomous functioning, ML is highly susceptible to errors or hidden bias in the training datasets.

Considering that much of the technology for IA/ML has been developed (and continues to grow) by corporations, with limited participation and funding from countries, development costs are not a major obstacle for Audit Institutions to apply it.

However, implementation and operation costs, depending on each country, can be significant and each SAI will need to make its own justification in terms of the speed and economic resources it will allocate to this type of application.

Implementation costs, as discussed in previous articles, are composed of:



Source: Prepared by the author

Emerging technologies:
Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

5G

INTOSAI Working Group on Impact of Science and Technology (WGISTA)
Prepared by the Commission on Audit of Philippines

5G

Basic Definition

By definition, 5G refers to fifth-generation cellular network technology, which has been evolving since 1980. In a white paper, the World Economic Forum (2020) mentions that 5G is expected to significantly enhance the mobile network, enabling more connections and interactions. It adds that this connectivity enhancement across networks will unlock significant potential for various industries to improve their bottom line.

According to Lin & Lee (2021), 5G is expected to deliver much higher data rates, lower latency, greater capacity, and more efficient spectrum utilization compared to the previous technology generation, 4G. Equipped with these more advanced capabilities, 5G can support diverse usage scenarios and applications. Compared to 4G, 5G will increase data rates by 10 times. Specifically, 5G is expected to offer a 20 Gbps peak data rate in the downlink (DL) and a 10 Gbps peak data rate in the uplink (UL). In dense urban environments, 5G can support a user-experienced data rate (at the five percentile) of 100 Mbps in the DL and 50 Mbps in the UL. With dramatically increased data rates, 5G will deliver a much-enhanced mobile broadband experience.

The WEF (2020) paper summarized the societal impact of 5G technology across several industry sectors in the following table using the United Nations Sustainable Development Goals (SDGs) as a framework:

Industry sector	Key industry trends	Sample use cases	SDG impacted	Transformation enabled
Manufacturing	*Hypercompetition with no sustainable competitive advantages. *Increasing volatility from business cycles and product life cycles. *Smart factory advances due to developments in the internet of things and automation. *The need to securely connect systems on a common infrastructure. *Increasing consumer demand for customized and personalized products. *Demand for products that are more complex to build and deliver.	*Smart factory floor. *Human-to-robot collaboration. *Predictive maintenance *Digital twins *Augmented reality (AR) *Virtual reality (VR) *Digital performance management	SDG 7 SDG 8 SDG 9 SDG 12 SDG 13	*Advanced predictive maintenance can lead to enhanced equipment availability and throughput. *Remote maintenance can lead to lower operational costs. *Digital performance management and digital standard operating procedures result in enhanced operational efficiency. *Factories of the future have smart, automated manufacturing.

Industry sector	Key industry trends	Sample use cases	SDG impacted	Transformation enabled
Mobility	*Autonomous driving and a connected traveller with telematics. *Car sharing and changing commuter habits. *Electric mobility with the green agenda. *Digital vehicle ecosystem. *nfotainment on the Move. *Urbanization and intermodality. *Environmental awareness and public spaces. *Urban lifestyle and growing expectations on public transport.	*Digital twin (predictive maintenance). *High-density platooning and automation (C-V2X). *Smart traffic control with prioritization. *Remote vehicle health monitoring. *Massive media car infotainment. *Airborne taxis. *Vehicle-to-vehicle.	SDG 3 SDG 7 SDG 9 SDG 11	*Autonomous mobility as a reality lead to enhanced individual productivity (less time spent on driving). *Green and sustainable mobility reduces environmental impacts.
Healthcare	*Increasing consumer attention on well-being. *Increasing cost to meet socio-demographic changes. *Increasing demand on quality, patient safety and data storage. *Changing consumer behavior, freedom of choice and alternative service providers.	*Remote patient monitoring. *Internet of medical skills/remote surgery. *Image transfer. *AR/VR-enabled healthcare. *Disease management. *Wearables and ingestibles. *Drone-enabled medical service delivery.	SDG 3 SDG 4 SDG 5 SDG 8 SDG 9	*m-Health (mobile health) and the wider introduction of telemedicine result in increased accessibility to quality healthcare. *Preventive healthcare measures (wearables and ingestibles) lead to decreased longterm healthcare costs
Financial services	*Disruption from fintech (technology used to support financial services) due to online payments, e-wallets, etc. *Challenging customer relations with online/ mobile transactions and customized financial solutions. *Structural changes: state involvement, protectionism and fiscal measures.	*Mobile banking: centre of all banking transactions. *Wearables for payment. *Virtual personalized financial advisor. *Internet of moving things. *Digital deposits, payments and peer-to-peer lending. *Mobile as a digital wallet. *Remote teller.	SDG 4 SDG 5 SDG 8 SDG 9 SDG 13	*Shorter settlement cycles in capital markets lead to enhanced economic activity. *Virtual personalized services and all-in-one mobile wallets enhance the customer experience.

Industry sector	Key industry trends	Sample use cases	SDG impacted	Transformation enabled
Retail	*Omni-channel retail strategies. *Personalized retail experience. *Growing culture of immediacy. *Increasing relevance of digital mobile wallets. *Faster e-commerce shipping. *Rising subscription e-commerce.	*Consumer 3D calls/ holograms. *Consumer AR/MR. *Automated checkout. *Layout optimizations. *Smart customer relationship management. *In-store personalized promotions. *Inventory shrinking prevention.	SDG 2 SDG 3 SDG 8 SDG 12 SDG 13	*Try-before-you-buy using AR/ VR results in an enhanced consumer experience. *Customized in-store advertisements lead to increased sales.
Energy	*Electrification and renewable energy generation. *New decentralized business models. *Structural shifts with increasingly retiring assets. *Political and societal push for sustainable energy systems. *Production and transmission assets often located in remote locations. *Need for improved customer engagement.	*Smart grid. *Drone monitoring capabilities. *Smart energy management. *Hazard and maintenance sensing. *Electric vehicles. *Residential smart meters. *Smart street lighting.	SDG 7 SDG 8 SDG 9 SDG 13	*Smaller plants dependent on renewable energy and smart grids enhance reliability and availability. *Demand-side integration with suppliers unlocks commercial opportunities for suppliers. *The digitization of gas networks leads to faster decision making, minimizing potential losses.
Entertainment/ media	*Consumers of content acting as content cocreators. *Increasingly interactive and immersive forms of entertainment. *A new sensory dimension to entertainment. *Expansion of digital content through new platforms and market players. *Ecosystem complexity.	*Immersive media applications (ultrahigh-definition, AR, VR). *Live in-stadium experiences. *Connected haptic suites. *3D holographic displays. *Gaming (AR and cloud gaming). *Home entertainment subscription for car *In-venue media	SDG 3 SDG 4 SDG 5	*Content-fuelled interactions igniting emotional connections lead to increased customer expenditure. *The consumer as content cocreator results in increased consumer engagement. *Gamification is induced in other industries.

Evolution of these technologies

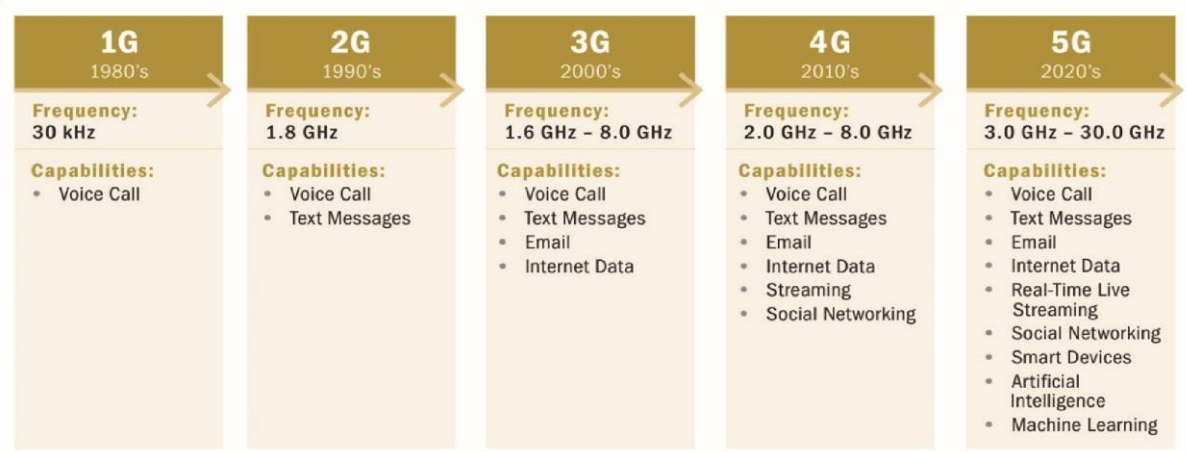


Figure 1: Evolution/ generations of mobile network (Source: Office of Auditor General of Ontario, Canada (2021))

5G Evolution

In Dahlman, Parkvall, & Skold's (2018) book, they elaborated on the history and evolution of mobile communication technology. The first generation of mobile communication, emerging around 1980, was based on analog transmission with the main technologies being the Advanced Mobile Phone System (AMPS) developed within North America, Nordic Mobile Telephony (NMT) jointly developed by the, at that time, government-controlled public-telephone-network operators of the Nordic countries, and Total Access Communication System (TACS) used in, for example, the United Kingdom. The mobile-communication systems based on first-generation technology were limited to voice services and, for the first time, made mobile telephony accessible to ordinary people.

The second generation of mobile communication, emerging in the early 1990s, saw the introduction of digital transmission on the radio link. Although the target service was still voice, the use of digital transmission allowed for second-generation mobile-communication systems to also provide limited data services. There were initially several different second-generation technologies, including Global System for Mobile (GSM) communication jointly developed by a large number of European countries, Digital AMPS (D-AMPS), Personal Digital Cellular (PDC) developed and solely used in Japan, and developed at a somewhat later stage, the CDMA-based IS 95 technology. As time went by, GSM spread from Europe to other parts of the world and eventually came to completely dominate among the second-generation technologies. Primarily due to the success of GSM, the second-generation systems also turned mobile telephony from something still being used by only a relatively small fraction of people to a communication tool being a necessary part of life for a large majority of the world's population. Even today there are many places in the world where GSM is the dominating, and in some cases, even the only available, technology for mobile communication, despite the latter introduction of both third- and fourth-generation technologies.

The third generation of mobile communication, often referred to as 3G was introduced in early 2000. With 3G the true step to high-quality mobile broadband was taken, enabling fast wireless internet access. This was especially enabled by the 3G evolution known as High-Speed Packet Access (HSPA). In addition, while earlier mobile-communication technologies had all been designed for operation in the paired spectrum (separate spectrum for network-

to-device and device-to-network links) based on the Frequency-Division Duplex (FDD), 3G also saw the first introduction of mobile communication in unpaired spectrum based on the China-developed TD-SCDMA technology based on Time Division Duplex (TDD).

The fourth generation (4G) era of mobile communication is represented by the LTE (Long-Term Evolution) technology. LTE has followed the steps of HSPA, providing higher efficiency and further enhanced mobile-broadband experience in terms of higher achievable end-user data rates. This is provided by means of OFDM-based transmission enabling wider transmission bandwidths and more advanced multi-antenna technologies. Furthermore, while 3G allowed for mobile communication in the unpaired spectrum by means of a specific radio-access technology (TD-SCDMA), LTE supports both FDD and TDD operation, that is operation in both paired and unpaired spectra, within one common radio-access technology. By means of LTE, the world has thus converged into a single global technology for mobile communication, used by essentially all mobile-network operators and applicable to both paired and unpaired spectra. The later evolution of LTE has also extended the operation of mobile-communication networks into unlicensed spectra (Dahlman, Parkvall, & Skold, 2018).

According to Yu, Lee, & Jeon (2017), research on 5G services and their technical requirements has been performed by the International Telecommunication Union-Radiocommunication Sector (ITU-R), the 3rd Generation Partnership Project (3GPP), and the Next Generation Mobile Networks (NGMN) Alliance. In the ITU-R Working Party (WP) 5D, 5G is defined by the name of International Mobile Telecommunications-2020 (IMT-2020), and various 5G services are presented in a vision document. The proposed usage scenarios are grouped into three categories:

- enhanced mobile broadband (eMBB);
- massive machine-type communications (mMTC); and
- ultra-reliable and low-latency communications (URLLC)

The peak data rate, area traffic capacity, network energy efficiency, connection density, latency, mobility, spectrum efficiency, and user-experienced data rate are selected as key performance indicators (KPIs), which can be regarded as technical requirements.

5G Services

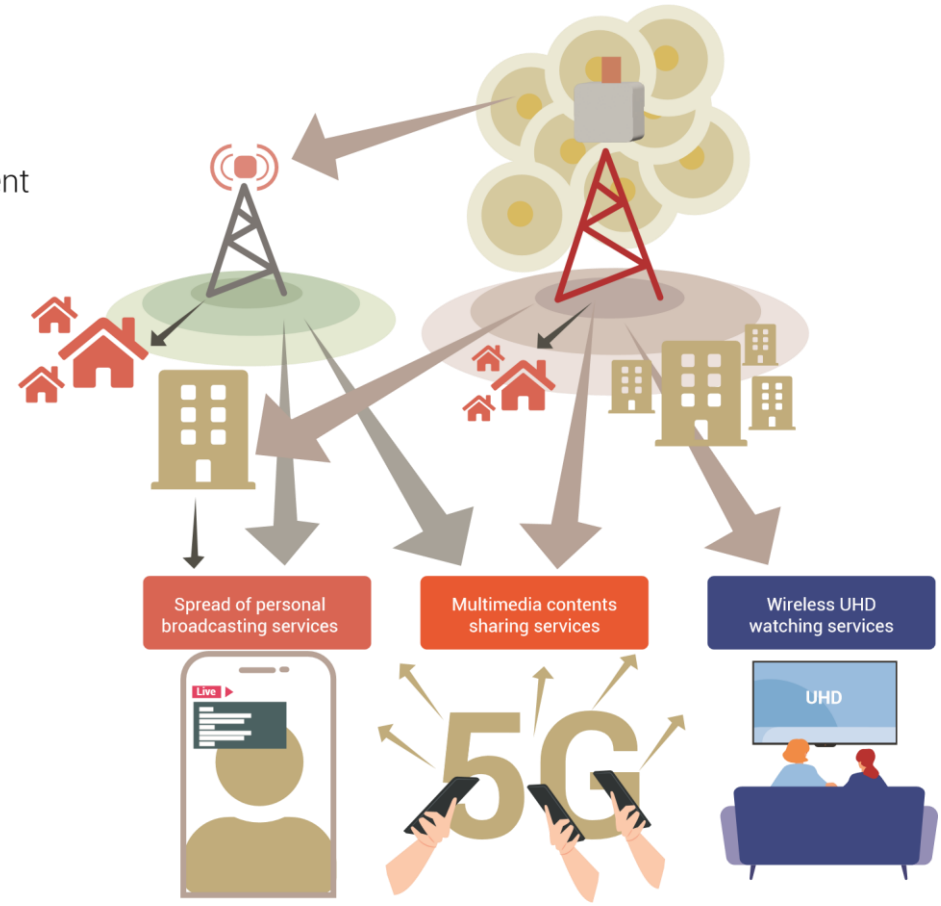
In their paper, Yu, Lee, & Jeon (2017) proposed five (5) categories of 5G services in terms of the end-user experience that is different from the categories presented by the ITU-R which is based on the technical viewpoint of network operators and service providers. These categories are as follows:

1. Immersive 5G Services

Figure 2: Real-time mixed reality with Augmented Reality (AR) and Virtual Reality (VR) services

1. Immersive 5G Services

Figure 3: Massive Content Streaming Services



2.Intelligent 5G Services

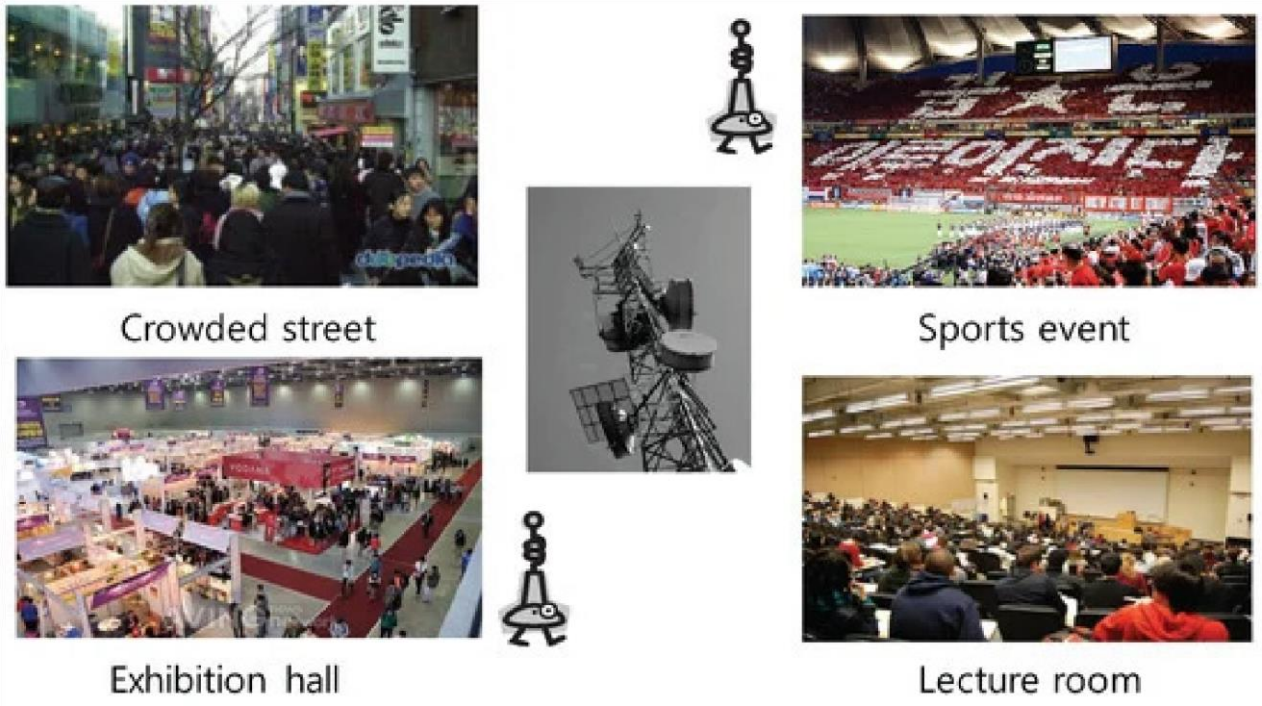
Figure 4: User-centric computing services

Mobile concierge services

User-centric knowledge services

3.Immersive 5G Services

Figure 5: Crowded area services



3. Omnipresent 5G Services

Figure 6: Smart personal, building and city services with Internet-of-Things (IoT)

Figure 7: Smart transportation services

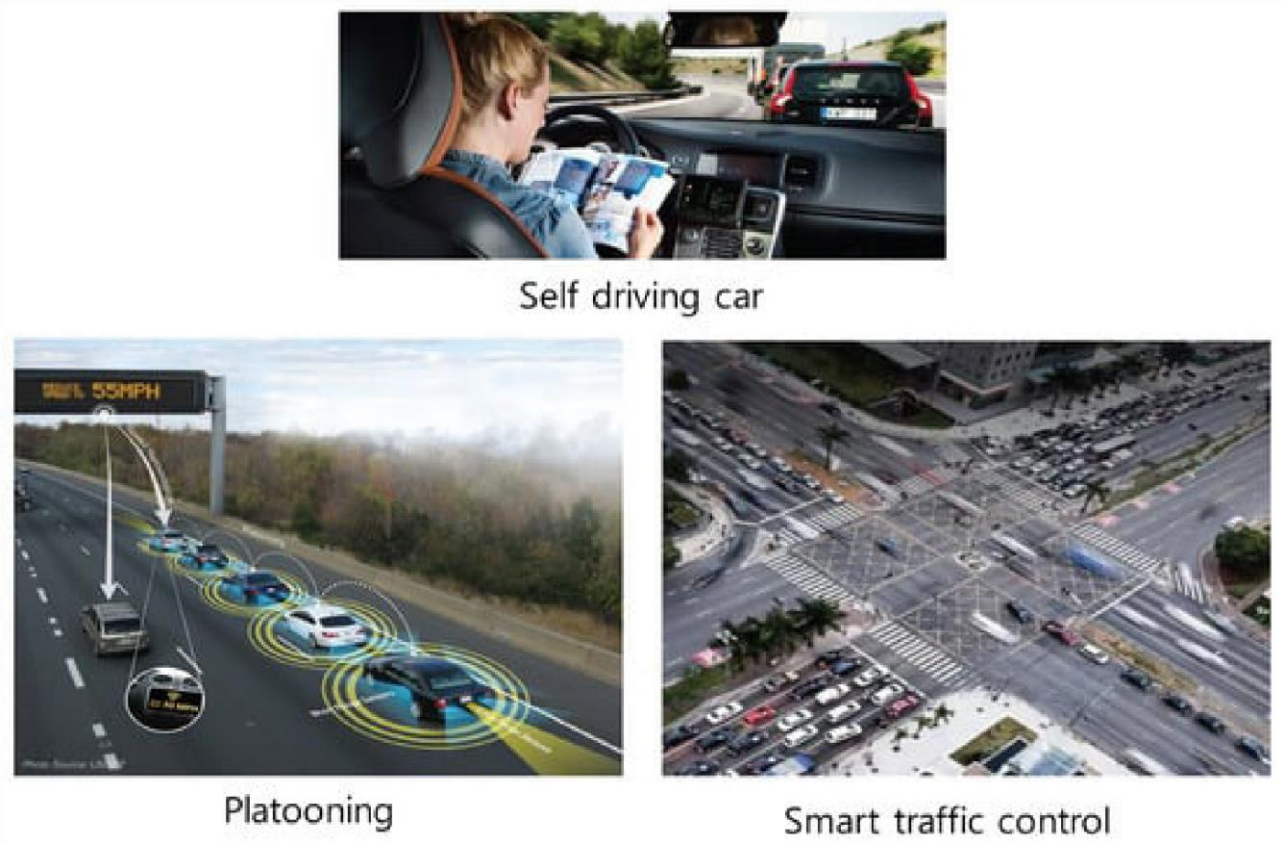


Figure 8: Remote surgery services with robots

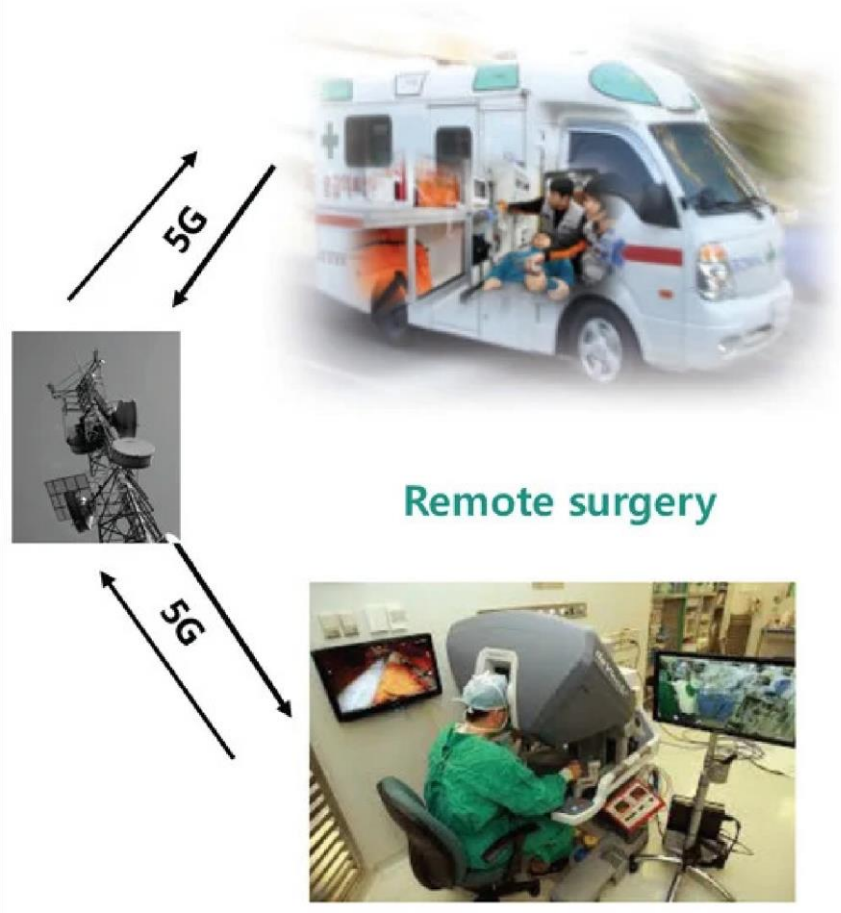
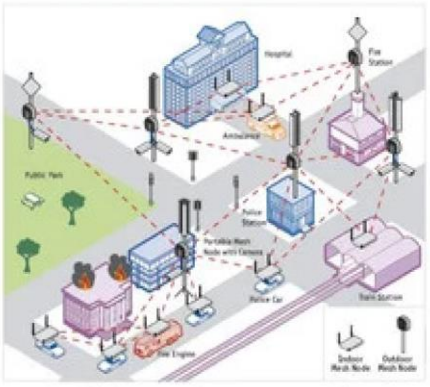


Figure 9: Private security and public safety services

Emergency services



Public safety services

Resources needed

CISCO (2019) published a white paper providing a high-level, technical, 5-step approach for deploying 5G, including the resources needed such as the infrastructure. As the information provided therein is too technical and more suited for telecommunications companies that build the infrastructure to make 5G possible, such information is no longer included here.

The global rollout of 5G is ongoing, spawning various 5G-enabled services like IoTs. From these new services, various industries will build new products and services that will also require different sets of resources. For SAIs, this could mean the following resource requirements in the future if they wish to adopt 5G technology:

a.) Procurement of 5G internet services from telecommunication companies;
b.) Investment in equipment that could receive and transmit 5G signals;
c.) Replacement of legacy equipment in favor of 5G-enabled IoT devices;
d.) Hiring and training personnel on the operation and maintenance of IoT devices that rely on 5G

Privacy, Ethics and Confidentiality issues

Wazid, et.al. (2021) of the Institute of Electrical and Electronics Engineers (IEEE) enumerated some of the security and privacy issues in 5G in their article, particularly on IoT communications where almost the entirety of the technology is expected to be used for:

a.) Lack of robust security schemes: IoT devices are connected to the system i.e., desktop or smartphone. In such an environment the lack of security mechanisms improves the threat of leakage of personal data. The collected and transmitted data of IoT devices may be disclosed (i.e., health data collected through smart healthcare devices).

b.) Openness of the network: It is necessary to connect IoT devices with a consumer network that has a connection with the other systems. It is also possible that IoT devices comprehend some security vulnerabilities, which may be harmful to the network of consumers. Because it may become the entry point for the attacker to get entry into the system.

c.) Privacy of sensitive data: IoT environment consists of different types of devices, which have various types of hardware and software. Some of them may be vulnerable to different attacks i.e., replay, Man-In-The-Middle, impersonation, password guessing, etc. Therefore, sensitive data may be leaked through unauthorized access and manipulations. Some of these devices transmit users' personal information such as name, address, contact number, date of birth, health data, and credit card. Hence it is always required to protect the communication of IoT against possible attacks.

The paper, however, also discussed existing security protocols in 5G-enabled IoT communications environments which they categorized into four as seen below.

1. Key management protocols	3. Access control/user access control protocols
2. User authentication/device authentication protocols	4. Intrusion detection protocols

Figure 10: Classification of security protocols in 5G-enabled IoT communications environment

5G applied for auditing

An article by Miolo & Lussu (2018) of Deloitte Switzerland presented some innovative audit practices and business models that the firm is planning to roll out in the years since its publication. In the article, they mentioned leveraging 5G's high bandwidth and support for minimal-time large data transfers to create various audit use cases for big data streaming in 5G-enabled mobile devices like laptops, tablets, and smartphones. Some examples they mentioned include:

a.) Use of the inventory observation solution, "iCount", to scan barcodes directly, capture pictures of inventory that is being counted, and use voice-to-text technology to record results and observation directly on mobile devices. This data is then transmitted to the audit team in real-time – aggregating and reconciling inventory records in multiple count locations
b.) Piloting the use of drones for remote sensing of large-scale infrastructure and construction sites: these will transfer data and observations to mobile devices based on the "iCount" technology

c.) Making changes to the working environment to leverage fully upcoming technological advances such as live big data analytics, Artificial Intelligence (AI), and blockchain for mobile, all based on the possibilities presented by 5G. This will enable audit teams to share their firsthand experiences and insights directly with their clients and deliver value at a faster pace.

International Applications

In many audit use cases, 5G as a technology, is mostly seen as an enabler that serves to power other audit tools and technologies. 5G technology is not directly involved in the development of audit findings nor in fraud detection but it is needed by other technologies like artificial intelligence and machine learning to harvest vast quantities of data from multiple devices and access points to perform advanced data analytics and produce high-quality audit reports. According to the Institute of Internal Auditors (IIA), 5G will drive greater use of big data, and that will boost demand for data analytics.

Hence, to make the most out of 5G technology, it would be best to have it complement other emerging technologies and existing audit tools to amplify their capabilities. For instance, 5G can be used to make it possible for auditors to perform interviews, record observations, document inspections, harvest data, conduct data analytics, and prepare audit reports, all while only carrying their smartphones. Through 5G technology, auditors can use powerful computers and servers for both computing and storage operations through remote connections via their smartphones, thereby allowing them to perform all major audit procedures with only one or a few devices.

The IIA's (2019) Global Perspectives and Insights publication provided some pathways for Chief Audit Executives (CAEs) for embracing technology including 5G:

- Recognize the need for self-assessment, and challenge how objectives are being accomplished
- Embrace technological advances
- Do not blame the failure of innovation on the lack of resources
- Develop and communicate the case for internal audit to actively pursue innovation

As mentioned before, 5G technology can be used to amplify the capabilities of data analytics. In this regard, Richard Cambers, president and CEO of the IIA, echoed 10 action items offered by the global consulting firm, Protiviti, in its 2018 publication entitled, "Analytics in Auditing is a Game Changer." These items are as follows:

1. Recognize that the demand for data analytics in auditing is growing across all organizations and industries and that the trend is certain to continue.
2. Seek out opportunities to expand auditors' knowledge of sophisticated data analytics capabilities so that the function has a more comprehensive and precise understanding of what is possible with analytics.
3. Recognize that resource constraints, along with business-as-usual workloads, can limit auditors' capabilities to optimize their data analytics efforts.
4. Consider the use of experts to lead the analytics effort and, when appropriate, create a dedicated analytics function.
5. Explore avenues to expand auditors' access to quality data, and implement protocols that govern the extraction of data used during the audit process.

6. Identify new data sources, both internal and external, that can enhance auditors' view of risk across the organization.

7. Increase the use and reach of continuous auditing and monitoring to perform activities such as monitoring fraud indicators, key risk indicators (KRIs) in operational processes, and information used in the leadership team's strategic decision-making activities

8. Leverage continuous auditing to develop real-time snapshots of the organization's risks and incorporate results into a risk-based audit approach that is adaptable and flexible enough to focus on the highest areas of risk at any point in time.

9. Seek ways to increase the level of input stakeholders provide when building and using continuous auditing tools and when determining what data should be monitored by these tools.

10. Implement steps to measure the success of data analytics efforts, and also consider the most effective ways to report success and value to management and other key stakeholders The IIA adds that practitioners must be forward-thinking to provide assurance and apply digital technologies to their own work and anticipate the issues and risks associated with 5G. Further, it is imperative that auditors anticipate stakeholders' moves (to the degree possible) toward new technology, strategies, and business models so they can be ready to provide valuable and visible assistance where needed and when needed.

Potential obstacles

A survey of 183 executives by the global consulting firm, Protiviti (2022), has shown some of the challenges for 5G adoption.

Cost and Integration Drive the Timeline of 5G adoption

The results of the survey suggest that about half of organizations surveyed are already adopting or planning to adopt 5G in the next two years, while the other half of respondents had no timeline. Less than 15% of organizations indicated they have already adopted 5G.

There are a number of reasons causing such hesitation. Cost and the ability to integrate with legacy systems and networks are clearly the most significant barriers to 5G adoption, followed closely by security concerns and the availability of products and technology with 5G. The cost of 5G modems is expected to decrease significantly over the next several years. However, it will likely be more than five years before 5G modems approach the cost of today's LTE cellular modules for IoT devices.

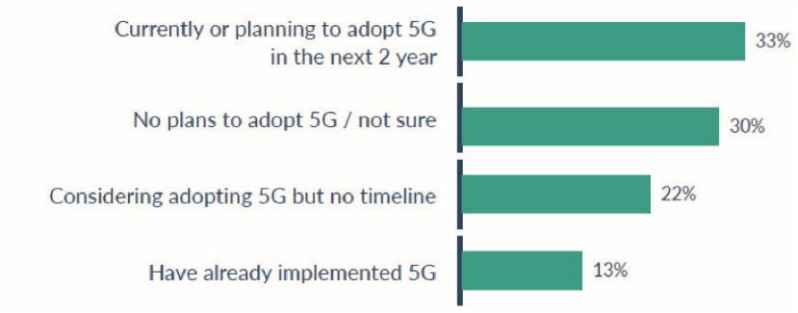


Figure 11: Result of Survey question: Where is Your Organization in Adopting 5G?

Cost and Legacy Technology Bring hallenges to 5G Adoption

Today's reality is that 5G is still very expensive and the devices that support 5G are currently limited. Over the next several years, new products are expected to address new use cases such as autonomous drones, remote cobots and robots, edge cloud computing, artificial intelligence and other augmented reality solutions. These products will rely on the speed and low latency of 5G to become a reality. Many IoT devices that use LTE today — and that do not require the speed and latency advancements of 5G — will continue to do so for the next five to 10 years until the costs of 5G are more aligned with LTE costs.

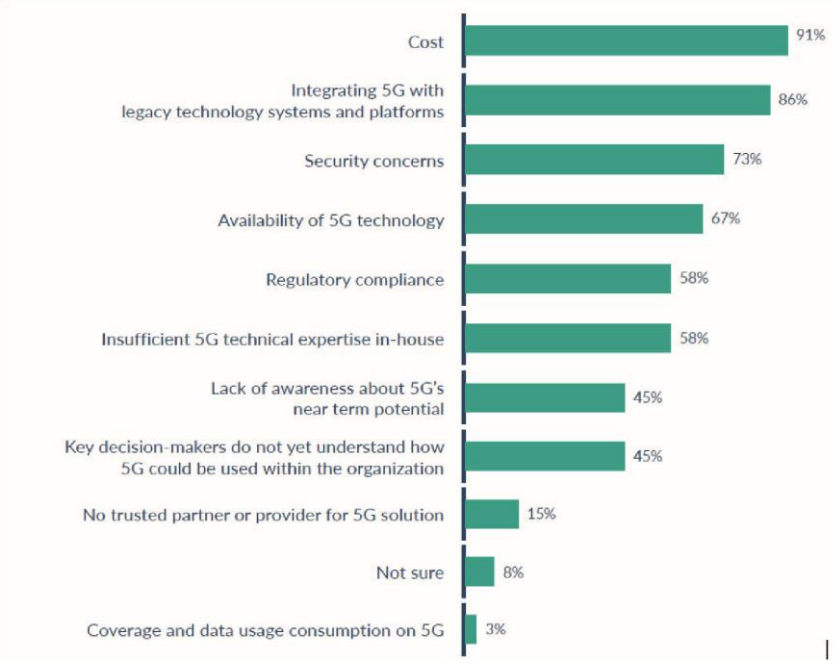
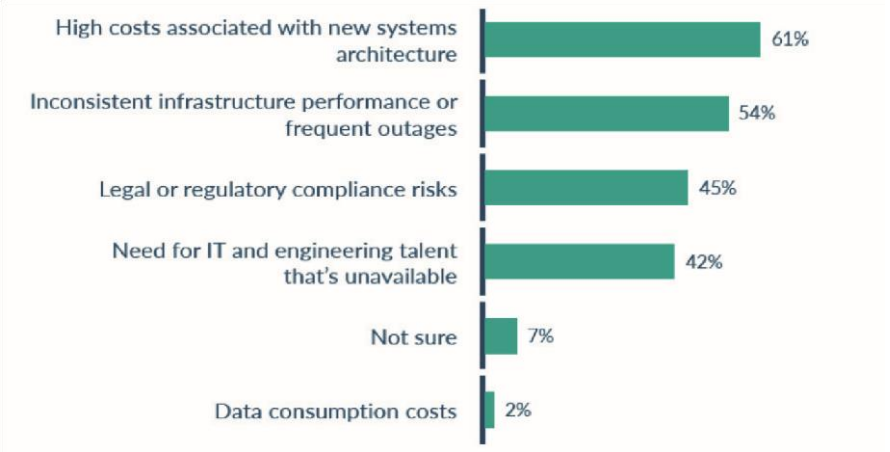


Figure 12: Most Significant Barriers to 5G Adoption

New System Architecture Costs Are a Risk Concern with 5G Adoption



Survey respondents view high costs inconsistent infrastructure performance as the most significant risks in adopting 5G. In addition, businesses must consider the potential regulatory and compliance implications on the horizon.

Figure 13: Most Significant Risks involved in 5G adoption

Organizational changes needed

Despite the perceived and technological advantages of 5G technology, its rollout is facing resistance in different parts of the world. In one study in Germany, Jenal,et.al. (2021) found that 53% of survey respondents are against 5G and that most of the arguments are health-related

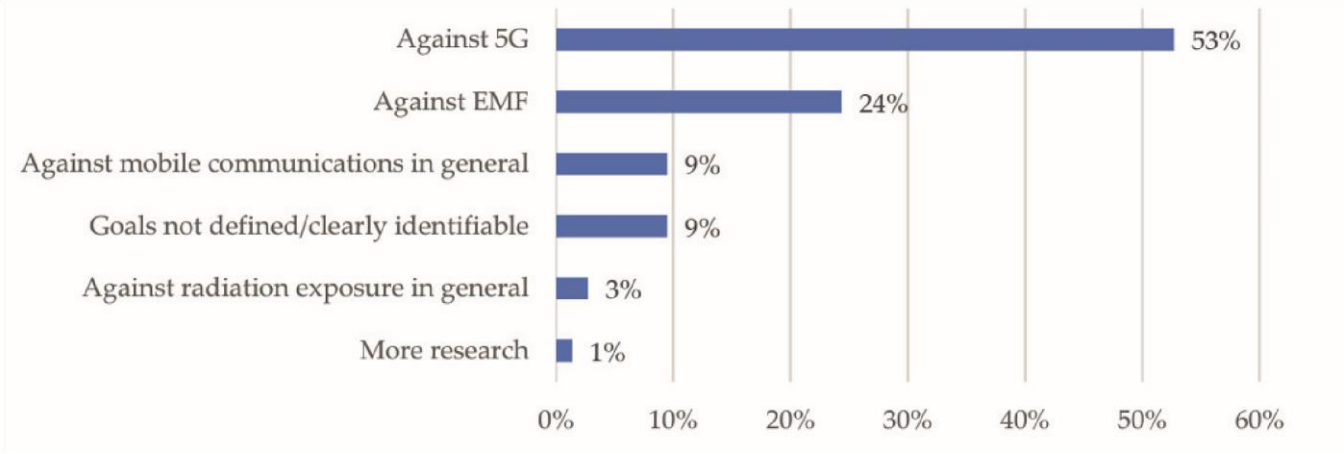


Figure 14: Goals of the citizens' initiatives against 5G (n=74)

New System Architecture Costs Are a Risk Concern with 5G Adoption

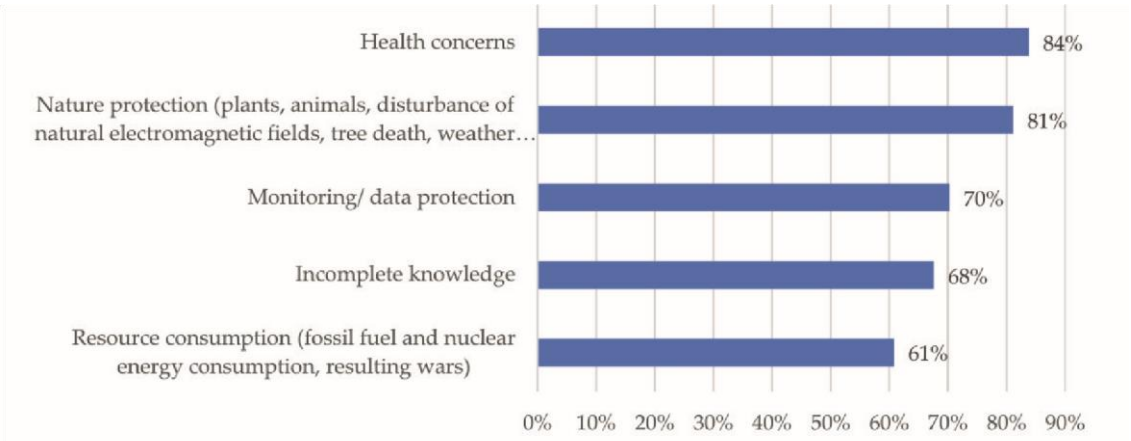


Figure 15: Arguments against 5G according to citizens' initiatives (n=74)

The study however concluded that the analysis of the online presence of 5G opponents shows that the initiatives involved have a high degree of organizational capacity and interconnectedness, which is generated and reinforced in particular by the closed exchange from within themselves. "This often hermetic closedness of the discourses in the organized conflict parties with an increasing external presence leads to a dichotomized structure, i.e., polarizes into a pro or con, which no longer allows for differentiations and thus makes regulation difficult", the study claims.

Expected benefits and costs

Benefits

5G technology has many advantages. It has superior bandwidth, latency, and speed compared not only to the previous generation, 4G, but also to fiber in some tests. Apart from its technical advantages, Curtis (2022) of the Information Systems Audit and Control

Association (ISACA) listed several other ways by which 5G will transform the way enterprises conduct business:

- Enhancing mobile broadband for services such as ultra high-definition (UHD) video, VR, and AR.
- Enabling communication for devices sending small amounts of information such as sensors for inventory management and smart cities.
- Introducing ultra-reliable and low latency communications for high availability and throughput for AVs, smart grids, e-health, industrial automation, and automated traffic control.
- Evolving e-health and telemedicine services by enabling healthcare providers to establish remote assistance and health monitoring services and leveraging drones to transport medicine and medical equipment.
- Providing longer battery life and increased bandwidth to support newer services such as the
- Industrial Internet of Things (IIoT), Avs, and unmanned aerial vehicles (UAVs).
- Integrating Industry 4.0 technologies to optimize factory operations such as the supply chain and IIoT.
- Improving environmental protection by optimizing radio access for smart grids, gas sensors, ozone sensors, and temperature sensors..
- Providing real-time administration for heavy machinery, inventory management, and product tracking via IoT sensors and ultra high-definition (UHD) camera.
- Collecting environmental data to improve workplace health; data management for smart cities; and remote access for power, water, and gas meters.
- Supporting environmental protection by allowing remote administration of UHD cameras for surveilling car plates and abandoned hazardous waste.
- Monitoring building structures in preparation for natural disasters such as earthquakes
- Enhancing agriculture, cultivation, irrigation, and fertilization systems.
- Equipping law enforcement with smart eyewear and remote-controlled drones fitted with UHD cameras.
- Embedding cellular-vehicle-to-everything (C-V2X) chipsets to implement vehicle-to-network (V2N) communications for increasing safety (e.g., by reducing collisions).

As far as the IoT use case of 5G is concerned, Wazid, et.al. (2021) listed the following advantages:

a.) **Easy remote access to information**: Using the IoT communication environment, data from smart devices which are located far from our location can be accessed in real-time using the Internet via a smartphone/ tablet. This makes it very convenient for everyone.

b.) **Provides better communication:** A network of interconnected devices in IoT provides a better communication environment. It increases efficiencies by making communication more transparent. Machine-to-machine communication makes the job more efficient and produces faster results.

c.) **Cost-effective**: Communication among electronic devices becomes easy because of the use of IoT. In such an environment, the transmission of data packets happens efficiently and saves money. Such type of fast transmission of data was not possible in the past.

d.) **Automation:** is the biggest need of the present as it virtually eliminates human involvement in tedious day-to-day activities. In business, it helps boost the quality of services.

Costs

There are still a lot of unknowns when it comes to the costs of 5G technology given that some of its components are still being developed to this date. The costs also vary by region and country, similar to how it was in the previous generations of the technology.

However, there are independent studies made that made multi-year projections as to the costs of 5G. A study by Statista (2022) shows that the total cost of 5G enhanced mobile broadband (eMBB) across all mobile networks and markets in Europe is expected to amount to around 150 billion euros from 2019 to 2040, with Germany and France expected to have some of the largest costs, at 25 billion euros and 19.3 billion euros respectively.

5G subscription costs per individual also vary per country. Data collected by one online source, GSMA Intelligence (2019), showed the difference in average cost between 5G and 4G unlimited plans varying from $5 to $72 per month depending on the operator. According to GSMA Intelligence, some of the variations can be explained by the various extras offered by each operator.

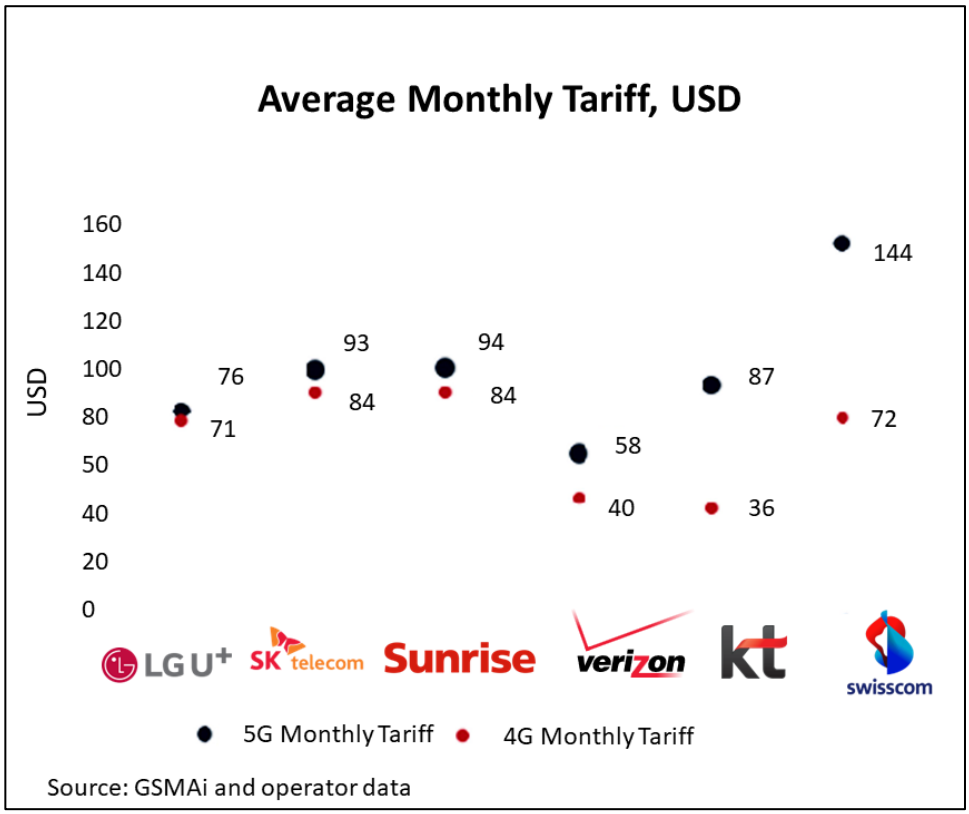
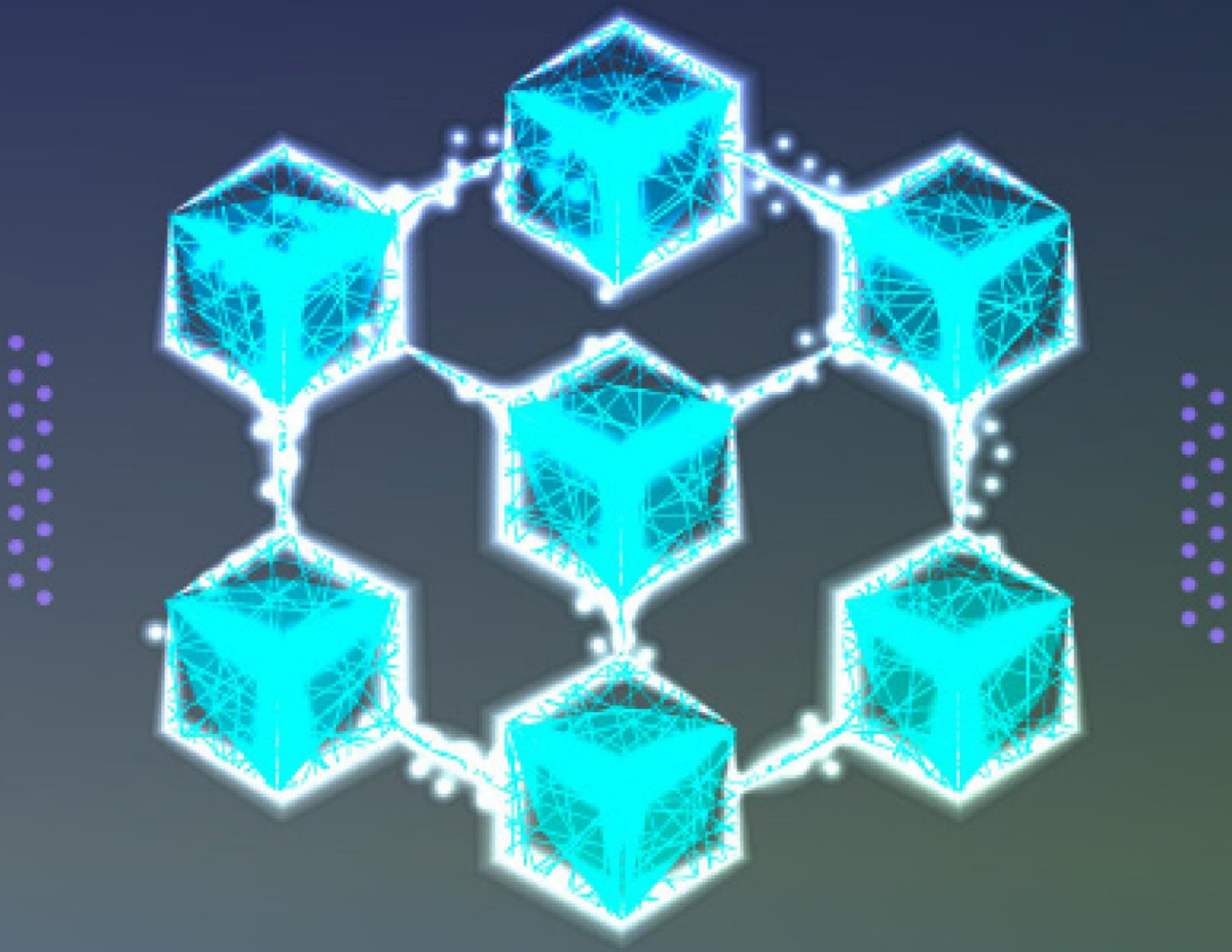


Figure 16: Average Monthly tariff per 4G/ 5G operator



Emerging technologies: Applications in developing and maintaining expertise within SAIs in the use of science and technology in auditing

Blockchain

INTOSAI Working Group on Impact of Science and Technology (WGISTA)
Prepared by State Audit Office of Vietnam

Blockchain context

Basic definition

Blockchain technology traces its roots to Satoshi Nakamoto's invention of Bitcoin in 2008, Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." and rapidly became an important tool for conducting various types of transactions and assets-related activities. At its core, blockchain represents an internet-based distributed ledger system that comprises multiple blocks linked together securely via cryptography in a peer-to-peer environment. Each block features a cryptographic hashcode referring to its predecessor along with evidence about the timing of its creation plus transaction information that's illustrated using Merkle trees (where data nodes correspond to leaves). The time stamp indicates whether or not transaction data indeed has existed at the same time or crypto-hash being coded during block creation serves as proof-of-work factor contributing towards chained sequence formation (similar to how linked list algorithm operates). Owing to this unique feature set-up thereof Blockchain infrastructure assurance basically revolves around attributes such as transparency; immutability underpinning decentralization principles without requiring any trusted third parties.

Main advantages and differences with current technologies

Security: All transactions are validated or executed are permanently stored in blocks that cannot be deleted or changed by anyone.

Decentralization: There is no need for a third party or intermediary to validate the transactions and information entered into the distributed database. In fact, a consensus mechanism shared and accepted by all nodes in the network is used to confirm transactions and blocks.

Distributed structure: Data is provided across all nodes of the network and geographically dispersed across the globe, the system is highly resistant to network attacks. Since each node has a copy of the entire database, there is no point of failure and any damage to a node in the network does not affect the overall operation of the system, unlike in centralized system, where a cyber attack or data center outage can occur, disrupting the service of the entire system. This redundancy gives the entire network high availability and reliability.

Efficiency: The system can effectively exchange the values of the network in real time.

Transparency: Data is published on a common platform and contained in the blockchain that is available in all nodes of the network. As a result, other interested parties and regulators accessing the network can easily get a real-time view of the platform.

Resilience: In Blockchain technology, even with the massive number of participants or individuals, the robustness of data is increased with longer life.

Trust: The majority of individuals or participants must agree on the data before adding it to the Blockchain network, which is different from the centralized network. Thus, trust is increased to write, change or even read any data.

Combine blockchain and 5G

As blockchain and 5G unite forces, they pave the way for cutting-edge mobile services. By connecting diverse devices and intricate networks with high data rates and low latencies via ultra-dense small cell networks within the infrastructure of the emerging technology standard; it is projected that over tens of billions of connections will be made by IoT & MMC by as early as next year - projecting an upwards trend towards over half a billion mobile interconnections in less than a decade from now. Considering these significant numbers; ensuring trustworthy interoperability amongst heterogeneous sub-networks presents itself as an essential challenge for the successful implementation of such advanced technologies like those on offer via blockchain-based architecture. Deploying blockchain's inherently decentralized structure enables distributed massive communication with no compromise on security or reliability - making advancements in D2D communications as well as other ground-breaking tech such as cloud/edge computing, SDN & NFV with network slicing key enablers for materializing future-proofed 5G networks and services, as stated by Dinh C. Nguyen et al. in their work “Blockchain for 5G and beyond networks: A state of the art survey”.

One pressing challenge facing present-day 5G platforms lies in establishing an open, transparent, and secure system amidst a massive number of resources and mobile users. Luckily though, there's a solution on the horizon with blockchain technology. By applying its decentralized operations to storage concerns for 5G heterogeneous data, blockchain offers commendable benefits such as increased data privacy, security transparency and immutability. As such experts predict that this technology will soon become indispensable in driving optimal performance levels for the 5G systems while minimizing associated costs and management overheads.

Evolution of Blockchain

According to Khizar Hameed et al. on their work: "A Taxonomy Study on Securing Blockchain-based Industrial Applications", Blockchain technology continues to evolve its underlying architecture through a sequence of phases or evolution for developing a variety of applications, as illustrated in Fig. 1.

Phase 1- Transactions 2008-2013: Blockchain 1.0 - Bitcoin Emergence

Bitcoin came into being in 2008 as the first application of Blockchain technology. Satoshi Nakamoto in his whitepaper detailed it as an electronic peer-to-peer system. Nakamoto formed the genesis block, from which other blocks were mined, interconnected resulting in one of the largest chains of blocks carrying different pieces of information and transactions.

Ever since Bitcoin, an application of blockchain, hit the airwaves, a number of applications have cropped all of which seek to leverage the principles and capabilities of the digital ledger technology. Consequently, blockchain history contains a long list of applications that have come into being with the evolution of the technology. However, in Blockchain 1.0, there are a few issues about computational cost, extended waiting times, lack of inter-operability and versatility which are recognised as major barriers to wider adoption.

Phase 2- Contracts 2013-2015: Blockchain 2.0 - Ethereum Development

Officially launched in 2015, Ethereum blockchain has evolved to become one of the biggest applications of blockchain technology given its ability to support smart contracts used to perform various functions. Ethereum blockchain platform has also succeeded in gathering an active developer community that has seen it establish a true ecosystem. The key features of such programs are that they execute automatically, based on defined logics and conditions in them, for example, time, performance, the decision and verification policies. It is equally important to describe here that these small programs (or contracts) run with the autonomous identities of users to protect personal information in the Blockchain network. The advantage of the smart contracts is that they can possibly reduce execution and verification times without requiring additional system resources to perform computation. Further, it can also allow the users to write smart contracts in a transparent way which prevents different fraud and hazard problems.

Ethereum blockchain processes the most number of daily transactions thanks to its ability to support smart contracts and decentralized applications. Its market cap has also increased significantly in the cryptocurrency space.

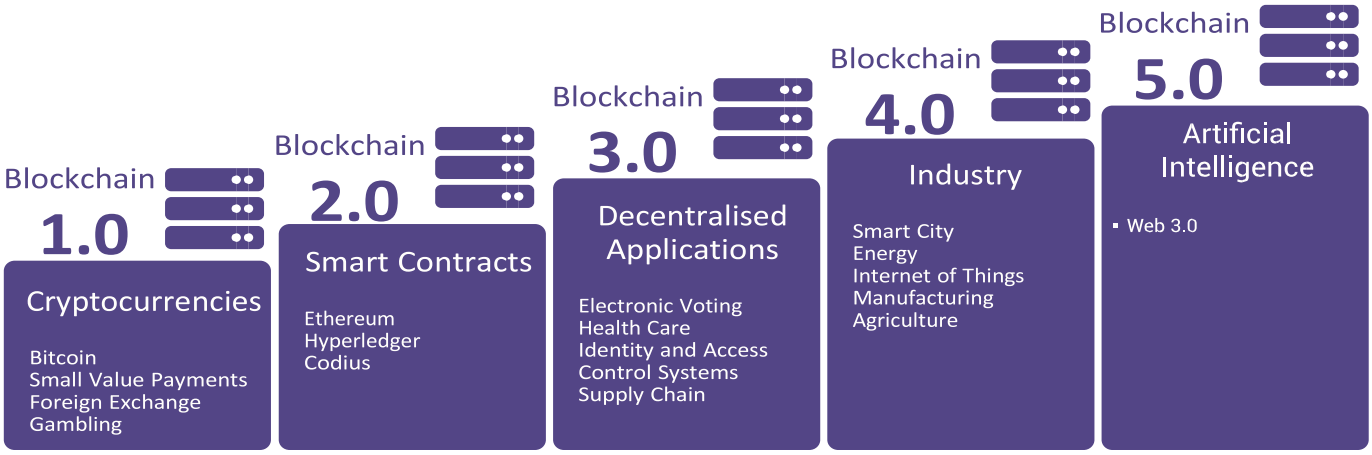


Figure 1 - Blockchain Evaluation. Source: "A Taxonomy Study on Securing Blockchain-based Industrial Applications: An Overview, Application Perspectives, Requirements, Attacks, Countermeasures, and Open Issues" by Khizar Hameed, Mutaz Barikaa, Saurabh Garga, Muhammad Bilal Amina, Byeong Kanga.

Phase 3- Decentralised Applications 2018 - now: Blockchain 3.0

In recent years, a number of projects have cropped up all leveraging blockchain technology capabilities. New projects have sought to address some of the deficiencies of Bitcoin and Ethereum in addition to coming up with new features leveraging blockchain capabilities. Bitcoin and Ethereum are open to everyone, and the data are produced and recorded on the Blockchain daily. Therefore, the primary need is to store a large amount of data in different storage places, such as data servers and clouds. For this purpose, a new version of the Blockchain has proposed a Blockchain 3.0 in which the decentralization concept is utilized to store a huge amount of data and to legally support a wide variety of communication mediums. Indeed, the code in decentralized applications supports multiple servers to run and compile it; whereas a single server with limited storage only runs limited applications The advantage of Blockchain 3.0 is that it allows the developer to write the code of applications in any language since it requires system calls to communicate with the decentralized system for the execution of the program. To illustrate the concept of Blockchain 3.0, the developers of smart contracts introduced Genaro, a first Turing machine based public Blockchain, which permits

the users to write and deploy native smart contracts in decentralized storage systems with the support of different network modules in the one place.

Blockchain 4.0 and Blockchain 5.0: Future

With the completion of a successful journey made by leading Blockchain versions (from 1.0 to 3.0), the new version of Blockchain 4.0 is presented to address the industrial challenges and limitations of real-world applications.

Blockchain 4.0 is a new generation or version of Blockchain technology that aims to introduce Blockchain into the industrial world and make it practical for developing and running real-world applications in a secure and decentralised way. The new version also enables us to propose new solutions and fills the gap between business and information technology industries.

Furthermore, Blockchain 4.0 enables the industry and business sectors to transition their entire structure and processes (or parts of them) transparently, to stable, self-recording applications built on a decentralised, distributed and immutable ledger. As Industry 4.0 is known as a revolutionary technological wave for the interconnectivity between people and machines, it provides substantial industry growth and productivity change that positively affects both the human quality of life and the environment.

Although Blockchain technology is relatively new, it has advanced dramatically. It is now used in a broad range of industrial sectors, including banking, healthcare, IoT and supply chain management. After achieving considerable success in earlier versions, Blockchain 5.0 is designed to serve the needs of the next generation 'business peoples' by formalising and standardising digital lifelines. Therefore, it is becoming extremely important to have Blockchain 5.0 in the today's world. The aim of Blockchain 5.0 is to concentrate on the integration of AI and DLT in order to develop the next generation of decentralised Web 3.0 applications to achieve data privacy, security, and interoperability.

Resources needed

Specialized infrastructure plays a central role in ensuring maximal effectiveness concerning blockchain technology usage. High-capacity storage combined with powerful hardware resources meeting computational demands required for storing blockchain constitute basic requirements for effective setup.

Underpinning blockchain storage is Distributed Ledger Technology (DLT), which brings several parties together via its shared database recording transactions concerning them immutably and indefinitely while steadily increasing block numbers over time.

Available estimates suggest Bitcoin saw a growth rate around 340GB between April 2019 to March 2021; however, this figure may fluctuate depending on the discovery rate concerning new blocks.

Mining blocks currently requires sophisticated hardware components that demand substantial computational power resulting from the growing numbers and sizes of Bitcoin miners.

Industrial settings seeking to introduce Blockchain technology must consider several cost scenarios, including (i) setting up and deploying Blockchain infrastructure, (ii) replacing

existing industry infrastructure, (iii) training employees to use Blockchain technology effectively and (iv) energy sources serving as backup resources. To properly regulate or audit Blockchain-based government systems or services from an SAI perspective it is imperative to explore in depth what skills and technical qualifications are required for these roles.

While cutting-edge hardware and computational abilities are integral components attention must also be given to human factors. Those undertaking such duties need a profound grasp not just of the technical intricacies of Blockchain but also of regulatory norms. Hence why is vital to foster talent pools comprised of individuals who possess both technological ingenuity, regulatory knowledge, and an aptitude for adapting to changes occurring in government-related applications utilizing Blockchain technology among our Supreme Audit Institutions.

Privacy, ethics, and confidentiality issues

Privacy and Trust

One of the most appealing features and benefits of Blockchain technology is to achieve anonymity of user identity and transactions, using pseudo-anonymity methods. However, the selection of public Blockchain type and the use of different pseudo-anonymous techniques in Blockchain applications may connect the identity of users to transactions such as public keys, thus increasing the chances of disclosing personal information to others. Therefore, there is a substantial need to implement pseudo-anonymity methods that must be fully anonymous and must achieve a higher level of privacy and trust among Blockchain users.

Ethics and Disruptive Technologies

Blockchain technology has gained praise for its transparent and immutable transaction capabilities. Nevertheless, critics argue that it also enables illicit activities such as funding illegal endeavors or money laundering because of its pseudonymous nature.

As such concerns arise about whether permitting anonymous usage of blockchain-based services should be viewed as a right or a privilege upheld by society?. Furthermore, investing in cryptocurrency such as Bitcoin comes with a significant toll on the environment as mining consumes vast amounts of energy which contributes negatively to carbon footprint raising an ethical concern between preserving the environment versus supporting technological advancements.

Adding on to this concern is wealth disparity; Blockchain technology can serve as a new financial paradigm empowering marginalized communities but implementing them haphazardly may widen socio-economic disparities if not regulated correctly ensuring proper distribution amongst all communities regardless of their level of knowledge towards this emerging technology will play an essential role in alleviating these growing concerns.

In summary, Blockchain technology reflects more extensive societal righteousness regarding equity justice privacy protection and how all these values relate together whilst maintaining our shared responsibility for our planet. Moving forward with exploring such disruptive technology requires digital ethics integration to ensure that the benefits of Blockchain do not cause more significant harm to societies.

Integrity and Transparency

Integrity and transparency are core values for delivering trust to prosperous markets. Blockchains can provide immutable land title records to improve property rights and growth in small economies, such as Honduras. In smart power grids, blockchain-enabled meters can replace inefficient centralized record-keeping systems for transparent energy trading. Businesses can keep transparent records for product provenance, production, distribution and sales. Forward-thinking governments are exploring use cases through which transparent, immutable blockchains could facilitate a lighter, more effective regulatory touch to holding industry accountable. However, trade secrets and personal information should not be published openly on blockchains. Blockchain miners may reorder transactions to increase fees or delay certain business processes at the expense of others. Architects must leaven accountability and transparency with confidentiality and privacy. Developers (or regulators) should sometimes add a human touch to smart contracts to avoid rigid systems operating without any consumer safeguards.

Blockchain technology applied for auditing

Blockchain is transforming not only the way of recording, processing and storing financial transactions and information, but also the way audit firms can practice their profession. Based on a qualitative study [cite] shows that Blockchain will allow an auditor to (1) save time and improve the efficiency of their audit, (2) favor an audit covering the whole population instead of an audit based on sampling techniques, (3) focus the audit on testing controls rather than testing transactions, (4) set up a continuous audit process, (5) play a more strategic audit role and (6) develop new advisory services.

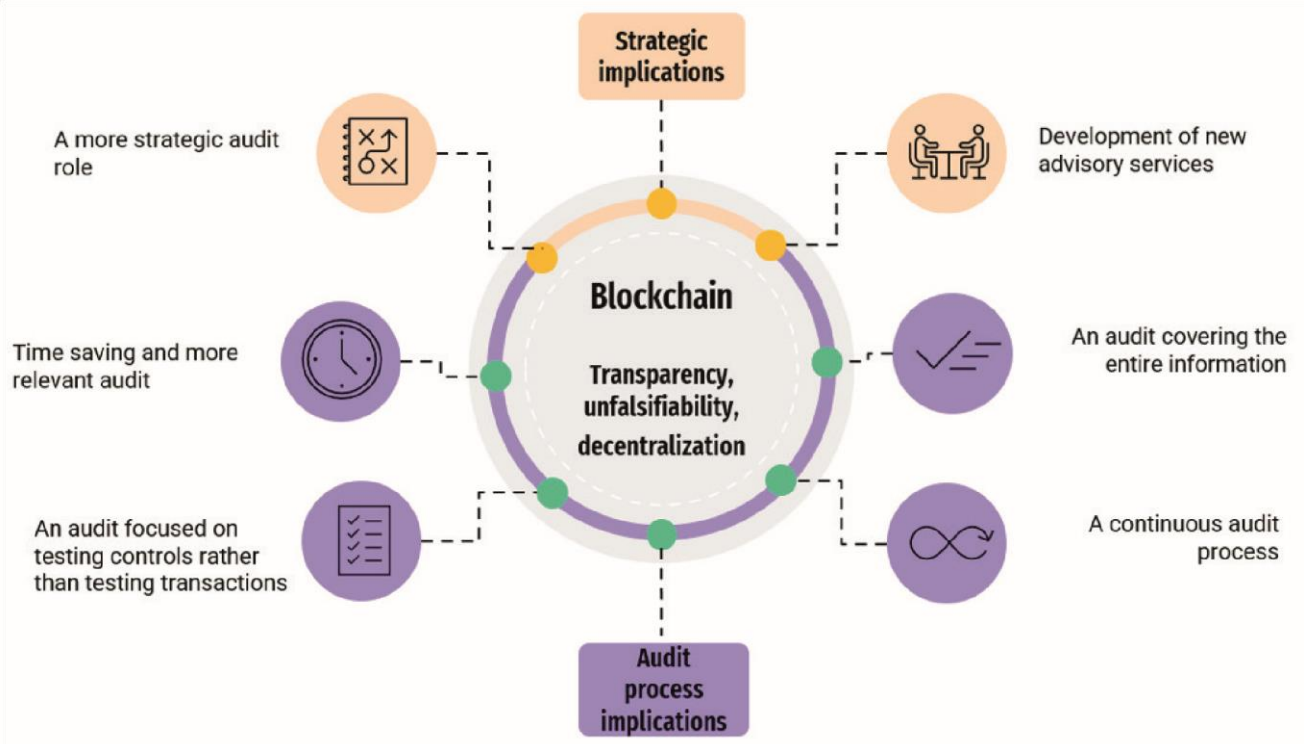


Figure 2 - Blockchain's implications for the auditing profession. Source: "How Blockchain Innovation Can Affect the Auditing Profession: A Qualitative Study" by Najoua Elommal and Riadh Manita.

Time Saving and More Relevant Audit

Blockchain technology has had a significant impact on accounting practices by helping to digitize all transactional and contractual processes, identity certificates, and validation procedures. It eliminates paper documents in exchange for electronic records that feature unique identification numbers ensuring their security from any tampering or breaches. This innovation replaces insular accounting systems with new shared platforms collectively certified across businesses.

With so many external entities involved across many industries regarding various financial matters, blockchain technology allows for joint ventures by providing an efficient mechanism for collaboration between different parties while remotely controlling costs associated with controlling hard copies or relying on traditional methods. Auditing procedures may soon be revolutionized thanks to private and authorized blockchains, which offer reliable information sharing capabilities that save significant time for auditors. This technology enables a secure method for businesses to provide unalterable documentation via a shared system with timestamps provided for transparency. Additionally, third-party entities like suppliers or clients can also upload their documents onto this network which assists in bolstering an auditor's understanding of a client's activity without relying on time-intensive traditional methods.

The potential savings for auditors utilizing these new systems include shorter data collection periods while ensuring accurate accounts with quicker balancing iterations due to fewer variables being present within each transaction history detail found on the blockchain. For example, an auditor can avoid manually testing correspondence samples because all related records are anchored within each validated block in the blockchain itself. A relevant discussion can be found at "How Blockchain Innovation Can Affect the Auditing Profession: A Qualitative Study" by Najoua Elommal and Riadh Manita.

Private and authorized blockchains have proven invaluable for streamlining information sharing processes during audits while also ensuring that all shared information is accurate. The use of these technologies has enabled auditors to more easily gather necessary data about their clients' operations while also simplifying the process for validating transactions with third party stakeholders such as suppliers or customers.

By creating timestamped transactions within blocks in blockchain networks - which can be readily accessed by anyone with permission - firms can save significant amounts of time previously spent on manual correspondence testing across sample sets or other tasks requiring extensive documentation review.

Blockchain technology has multiple advantages concerning transaction security and reliability which are equally applicable when recording accounting transactions saved on the blockchain platform- these accounting records must also undergo auditing checks for precision purposes so that accurate company financial statements can be generated in turn. For auditors working within a blockchain environment encountering "chain" transactions linked with "off-chain" agreements or instances of fraudulent activities, the effectiveness of the internal control measures deployed around the blockchain is an essential area for concern during audits. Instead of direct transaction testing aimed at ensuring information reliability within this particular ledger, auditors should prioritize assessing and enhancing the quality of control tests instituted (eg; blockchain code quality, peer distribution power, and protocol changes).

Integration with other technologies like big data analytics serves to broaden access to transaction history for auditors in the blockchain environment. The ubiquity of this technology has transformative potential in auditing processes going forward. By creating an encrypted stockpile of approved information blocks that can't be altered by consensus (facilitated by timestamp functionality and unique hash ID assignment), blockchain presents an ideal opportunity for auditing reformation.

The current process for auditors involves verifying dated financial year records, however, future innovations in blockchain technology could enable ongoing validation through continual auditing processes.

With all blockchain-stored data made transparently accessible to auditors, requesting and waiting for client documentation is no longer necessary with significant benefits in terms of reducing associated costs and saving time.

Blockchain provides additional valuable opportunities through secure storage capabilities: facilitating diversified audit practices that further expand beyond solely finance-related matters as well as offering instantaneous availability of different data types which promotes improved implementation of continuous audits.

Traditional audit procedures contained multiple post-closure verification stages; such repetitive efforts would theoretically no longer be necessary with the availability and accessibility of real-time analysis provided via blockchain technology. Inventory counts are also simplified using blockchains' ability for ongoing automated tracking solutions always ensuring accurate stock management. With technological advancements paving the way for future developments, traditional confirmations are becoming outdated as instant verification is made seamless through the creation of blocks via blockchain technology. Furthermore, analytical methods once reliant on limited sampling have evolved into constant reviews inclusive of all available data sets.

By automating reconciliation for transactions carried out among parties existing within a singularly linked network enabled by this innovation; an auditor's productivity is set to soar significantly improved than what was previously attainable under classical auditing procedures yielding quality results with an efficient turnaround time.

Smart contracts, another attribute of blockchain technology, promise to reduce the costs associated with fraudulent activities, arbitrations, and transactions while efficiently administering documentation flows and secure management of transactions associated with audits.

Enabling continuous audits and minimizing errors is possible thanks to the adoption of blockchain technology. To achieve this goal, auditors must embrace new control procedures that suit the ever-evolving technological landscape. Blockchain avails new horizons through which auditors can expedite their work processes by scrutinizing transactions, verifying digital asset integrity, and ensuring information on blockchains matches real-world occurrences. Additionally, innovative techniques such as code verification and confirming ownership seamlessly blend with IT systems auditing expertise already acquired by most experts. As such, prospects necessitate technical training. In today's technological landscape, innovation is key; consequently, making it imperative for auditors seeking growth opportunities through provision of comprehensive advisory services have embraced Blockchain Technology. Providing clients with support in implementing Blockchain Technologies across various sectors is just one example where

auditors could step in by offering expert guidance while advising on the most suitable procedural steps needed toward successful implementation initiatives.

For businesses already utilizing Blockchain, Audit Firms could support improvements by recommending changes after assessing risk management systems in place.

Additionally, Audit firms can offer viable consulting assignments through their sectoral experience which can shape best practices for Blockchain Usage Protocols, acting as a planner and coordinator of potential participants of the Blockchain.

Audit Firms have the ability to leverage their extensive networks to suggest permissioned blockchains as well as developing new services such as Internal Control Audit on blockchain, information security, Change Management and governance encompassing data integrity.

International Applications

Estonia

The country has completely rebuilt the public service by bringing blockchain technology to be used in national infrastructure and government management. Currently, approximately 99% of public services is e-services (PWC, 2019). Access to government information and services can be made online by digitally identifying which is useful for updating information for the government sector, business operation, and public health. A key sophisticated digital infrastructure is “the X-Road” which allows the nation’s public and private sector e-service information system to link up and function harmony. KSI is the complement of X-Road to provide a high speed and real-time authentication for all digital asset network. This blockchain technology is used for independent verification of all government processes and protecting e-governance services offered to the public.

Estonia also applied Blockchain technology to the health sector. Blockchain technology secures health information and able to authorize individuals. For example, people can also access their own health information by inserting ID card to a data reader connected to an electronic device such as a laptop or tablet. As a result, patients who have to repeat the same drug do not need to go to the hospital but they can bring the prescription that the doctor has sent to show to any drugstore at your convenience. Elder people are able to take care of their health and access medical treatments more easily. At the same time, doctors can have access to health and medical history information of patient such as blood type, drug allergy history, and even X-ray films from other hospitals of the patient immediately; thus, allowing the treatment to be timely and doctors can diagnose the disease more accurately without having to rely on the words to tell the symptoms of the patient.

Sweden

The Swedish Department of Lands (Lantmäteriet) has official launched a blockchain system for registering land and real estate information provided by companies, organizations, government agencies and all related to land management are recorded in the same system. The blockchain system is and intermediary for data storage, started in July 2017, to develop a management system for real estate transactions for buyers, sellers, tenants, and the government.

Blockchain technology allows the private and public sectors to manage land-related information in the country to solve the duplication of land assessment problems from the fact that financial institutions have to send their appraisal team to evaluate and the collect of information about the land constantly which resulted in enormous expenses. Putting the land title in blockchain system will establish a central condition that all parties must follow the same structure before importing data into and out of the blockchain system. This will enable all parties to access and use the information easily, conveniently, and quickly.

United Kingdom

The UK has the potential to become a leader of global blockchain as the country has sophisticated legal and regulatory system that will support the ecosystem for businesses and entrepreneurs. Blockchains have been implemented at the UK Government, Parliament, and the Financial Conduct Authority (FCA). The UK government has been assessed and invested more than $30 million in the blockchain technology. The UK Parliament has established the All-Party Parliamentary Group on Blockchain (APPG Blockchain) to analyses and advocates for the disruptive impact of blockchain and the positive effects that it can bring to the UK economy on both an industrial and governmental level. The FCA implemented policies to promote blockchain innovation along with eleven other financial regulators and related organizations. In addition, the UK government studied the use of blockchain technology for public service such as Department for Work and Pensions, Department for Environment, Food and Rural Affairs, HMRC's and HM Land Registry.

USA

The United States is one of the pioneers of blockchain with a pilot project many states such as Illinois, Colorado, Ohio and Delaware. Illinois launched the Illinois Blockchain Initiative to determine if this groundbreaking technology can be leveraged to create more efficient, integrated and trusted state services, while providing a welcoming environment for the Blockchain community. Colorado aims to exempt cryptocurrencies and certain digital tokens from securities laws. Ohio has amended the Uniform Electronic Transactions aim at promoting electronic signatures through blockchain technology (GovChain, 2021).

Delaware has been focused on the adoption of blockchain in government operations. The state

law legislation allows private companies to offer their stocks without issuing certificates but to confirm the various transactions through the blockchain system. Delaware has initiated a pilot program to register business through the blockchain system and in the process of studying and researching the feasibility of creating a system of IPO systems through blockchain.

China

The Chinese Government has announced on the 13th Five-Year National Informatization that would use blockchain technology to improve efficiency of government service such as taxes

collection, tax refund and issuing tax documents in the form electronic, health data recording, etc. Recently the country development plan is taking place in a concrete way.

The People Bank of China supported a blockchain-based trade finance platform to leverages the transparent and immutable properties of blockchain and to facilitate a regulatory system for trade finance.

China also apply blockchain technology in Food Supply Chain Traceability System. Currently, food safety attracted attention of academics, private and public sector as food safety is one of UN Sustainable Development Goal. Therefore, every sector has endeavor to innovate and develop Innovation for food safety traceability plus the evolution of IoT (Internet of Things) and Blockchain technology that enable to track the safety of food from the production process until reaching the consumer's hand.

Japan

Japan's Ministry of Internal Affairs and Communications has tested a blockchain system for facilitating the procurement and budget systems of government as well as share and store the information of procurement, approvals budget and private contract bidding among various departments to modernize the administration of Japanese government.

India

The National Institution for Transforming India (NITI) has an idea to apply blockchain system for suppressing counterfeit drugs by the end of 2018 because the World Health Organization (WHO) reports that about 20% of medicines sold in India are of inferior quality standard, and approximately 35 percent of counterfeit drugs sold worldwide come from India. Thus, NITI adopted blockchain system to suppress counterfeit drugs which have a unique identification code. At every step, consumers can also scan the QR Code or Barcode on the medicine bottle. A smartphone-based mobile application to check the production source and complete history of medicines.

In addition, NITI has also put the blockchain system to test in many sectors such as education, health, and agriculture.

Potential obstacles

Interoperability and Governance

As stated by Friedrich Holotiuk and Jürgen Moormann in their work: "Dimensions, Success Factors and Obstacles of the Adoption of Blockchain Technology", achieving interoperability among various Blockchain systems involves sharing messages and trusted values between them seamlessly. However, ensuring secure data exchange during this process presents significant challenges that require careful consideration. One issue is maintaining adherence to industry principles to regulate applications effectively.

Thus, designing a mechanism that enables different platforms to interact while defining suitable rules in line with industry guidelines is essential.

The deployment of this technology also faces legal and compliance hurdles due to varying agreement laws across industries. As such, some uncertainty around government regulatory bodies limits widespread adoption in large industrial domains significantly. For instance, stakeholders in manufacturing use Blockchain tools to ensure compliance with relevant legal frameworks governing their internal processes and goods transactions based on commercial law's requirements.

Failure to carry out a contract as intended due to miscoding would result in liability. Additionally, parties' legal and compliance arrangements must adhere to substantive law as well as governance rules such as jurisdiction and settlement while ensuring product privacy. Manufacturers face challenges when sharing manufacturing data across different platforms hence the need for protection of both user privacy and data on industry platforms.

Governments must uphold specific obligations concerning the public interest by making new laws that apply effectively in industries. One way towards this end involves implementing private Blockchains which discourage illicit activities such as money laundering or regulations bypassing alongside mechanisms that prevent fake miners from producing new blocks.

Scalability issues pose significant challenges within existing Blockchain technologies regarding widespread adoption or implementation; for example: where VISA processes approximately 2k transactions per second compared to Bitcoin's meager seven transactions per second.

As Blockchain technology continues to gain traction and find relevance in Industry 4.0 applications, concerns have been raised over its scalability due to increased system length and growing demand for nodes to join networks for block creation and mining. These challenges pose significant obstacles for network security systems and their related uses.

One key area where issues have arisen is storage capacities in many blockchain-based applications that aim to store data on secure distributed ledgers. For example, Bitcoin's blockchain increases by one megabyte every ten minutes with each node on its network holding an identical copy of its chain.

Though full nodes can keep entire blocks stored locally; however, as transaction sizes rise exponentially so do overall storage requirements making it harder to incorporate blockchain into numerous industrial processes generating enormous amounts of manufacturing data.

Furthermore, underlying protocols cause traffic congestion worsening demand even more intensifying further need for additional blockchain storage space expanding beyond present capacities. When chains become too large, they can create problems for new users trying to synchronize with the network - particularly in the industrial IoT context where an increasing number of sensors are producing vast amounts of data. While Ethereum-inspired frameworks have been developed recently, resource-constrained IoT solutions are still immature and may not be equipped for supporting more advanced industrial applications at present.

Integrating Blockchain technology into many industrial applications (including but not limited to IoT, SG & eHealth) brings about significant challenges on account of node

computation limitations. These apps usually come with minimal computing capabilities along with restricted storage & energy resources - making it hard to mine blocks or carry out crypto operations like hashing or digital signatures which require intensive computation capabilities.

Several proposals put forth an alternative solution that distinguishes simpler nodes from mining ones in Blockchain-based IoT apps; these propositions aim to solve node performance issues altogether by reducing overheads arising from communication between leaner and heavier/mining nodes. IoT gadgets continuously monitor environmental factors, making them crucial components of industrial setups.

Yet, Industry 4.0's success hinges on overcoming barriers relating to device standards and communication protocols which have become even more critical given their broad usage across an array of smart devices.

Integrating these diverse smart gadgets can be costly due to the variable formats they use for storing data while also employing distinct protocols. Manufacturing giants such as Eclipse Foundation & Bosch are solving this issue by developing shared communication protocol like MQTT that provides universally accepted data formats for easy interaction between disparate devices.

However, it's important to be aware that increasing the number of shared protocols could increase the complexity of developing a comprehensive single data model. The adoption of Blockchain technology by various industrial applications has led to an increase in attack surfaces that bad actors are targeting. These attackers use multiple methodologies and discovered vulnerabilities in the system's applications, allowing them unauthorized access into the environment to manipulate user data for their gain. To cite an example is Bitcoin's Double Spending Attack that combines with Sybil attacks making it possible for hackers to gather wallet details of users, their balance as well as private keys.

In addition, if smart contract code vulnerabilities are present or open-source apps exist in these systems; attackers can exploit these weaknesses further increasing susceptibility risks of Blockchains. Nevertheless, carefully designed Blockchain application models guided by solid security protocols can minimize such threats.

Organizational changes needed

When adopting blockchain technology organizations must consider several dimensions.

To ensure a successful implementation of blockchain technology teams require individuals with expertise in both IT and business.[cite] Furthermore,[cite] it is essential that these team members also understand customer needs and business processes. Since implementing blockchain technology can significantly impact an organizations information systems,[cite] effective communication among team members becomes integral to its success. Unfortunately skilled workers in this field are scarce,[cite] forcing many companies to look beyond their organization for external service providers or consultants who can bridge knowledge gaps. In many companies across various industries there is growing acknowledgement that blockchain technology represents an opportunity for increased efficiency, transparency, cost savings--even the potential for expansion into new business areas. As such its not uncommon for key employees with a personal interest

in this field to spearhead efforts toward adoption within their organizations. Rather than relying solely on traditional forms of training or education on blockchain topics within their company walls these experts prefer hands on experience gained through prototyping as one way of building required skills sets in house. Despite these efforts however there remains significant challenges when it comes achieving full scale adoption across an enterprise ecosystem. Integration issues with existing IT systems continue to need attention in order to realize the full potential benefits promised by this promising technology. The adoption of blockchain technology is currently underway despite its limited productive state thus far. This major technological advancement during these early stages highlights the important role played by IT Units in its implementation process.

IT Units bring their valuable technological expertise into play while managing day to day operational tasks. These capabilities enable them uniquely positioned to incorporate nascent technologies like blockchain effectively into existing infrastructures. However this incorporation comes with significant challenges, particularly for established firms. With numerous existing systems to manage, replacing them with entirely new structures is not feasible in most cases.

In contrast start ups face fewer obstacles when integrating novel technologies into their operations compared to established companies.

Established organizations need to be cautious of not disrupting their critical day to day operations when adopting anything new.

As such adapting known processes and integrating blockchain based features where possible would be a more feasible approach for most firms. Still regardless of what adoption strategy companies take up- IT Units remain the critical players in bringing it forward; taking various roles based on their expertises- from leading autonomous adoptions to supporting initiatives by providing development know how as needed. In addition, we uncovered technology providers capable of managing IT department tasks within the context of blockchain technology. Presently, corporations prioritize the development of relevant use cases which must be either spearheaded or at least supported by various business units throughout an organization. Despite progress being made thus far with certain implementations and proof-of-concept developments, the full integration into operational aspects has yet to occur on all fronts This next phase involves developing new concepts/ideas while simultaneously realizing existing proof-of-concepts which come with extensive technical implementation efforts due to the underlying infrastructure nature inherent within this emerging industry trendline; consequently leading management teams overseeing various corporate departments (who control financial funding) hesitant towards investing money towards altering their current IT infrastructure given these challenges unique towards utilizing blockchain technologies themselves . Fundamentally different than traditional tech projects underscored within mainstream corporate culture today - companies must ask themselves the question, “where exactly do we see potential use cases from such applications? Does it really make sense for our business model?”

For blockchain adoption to be successful here in the present day and beyond, it must receive ample organizational support from differing entities across multiple levels of any given corporation. The key factor in all these moving pieces involves securing buy-in from management level decision-makers who regard blockchain adoption as a strategic imperative towards optimizing or transforming their firm’s current operational

effectiveness. Top management displays significant interest in examining how they may harness the potential of blockchain technologies as they recognize its importance.

This enduring engagement results in organizational changes aimed at adopting this innovative technology. To do so, firms may opt for two main approaches: creating a sub-unit focused on building and implementing blockchain prototypes within existing digitalization initiatives or establishing a separate lab dedicated exclusively to investigating this cutting-edge invention.

Successful attempts at adoption require pooling knowledge from different areas, identifying possible uses that are relevant and useful while also providing training opportunities across all organizational departments. Still, not every employee within a company is fully aware of the promise that this new technology holds nor support these efforts with equal enthusiasm. When it comes to understanding the innovative technology known as blockchain people typically fall into one of two camps: those who view its potential benefits positively and support its implementation versus those who have serious concerns about how disruptive it could be long term. In order to promote broader engagement across an organization on this topic specifically - companies must develop internal processes that encourage wider participation regarding blockchain related matters.

Project managers play a critical role in ensuring smooth coordination among team members when it comes to implementing a successful and efficient approach to using blockchain technology within an organizations daily operations. Among others responsibilities include identifying dedicated "go to" personnel for all matters involving the technology; managing required resource allocation; facilitating ongoing knowledge transfers between business teams; identifying key talent- both from within & outside of the organization- for various roles; organizing additional educational opportunities where needed; maintaining strong communication channels with external industry participants including regulatory authorities. Utilizing proven project management techniques is essential for effective team operations with agile methodology like scrum proving particularly effective for developing blockchain prototypes.

A shift occurs from bottom-up planning to top-down decision-making when it comes to resource allocation and strategic direction related to implementing blockchain technology. This change is attributable to high visibility levels coupled with strong anticipated impact on markets which requires heightened managerial attention; highlighting how senior management should be connected with blockchain adoption efforts.

The environment surrounding adopting blockchain technology plays an integral role in its success compared with other technologies. There are several differences arising from this dimension such as indirect pressures caused by media exposure or demands for disruptive solutions by business partners (including customers) or start-ups venturing into developing new products or business models that revolutionize existing markets.

Expected benefits and costs

Benefits

It is apparent that Supreme Audit Institutions stand to benefit greatly from adopting Blockchain technology as it offers various advantages toward streamlining operations while enhancing credibility levels simultaneously. As privacy remains a critical concern among these institutions; attributes found within Blockchain technology empower users with ownership and control over their data - mitigating risks associated with unauthorized access perhaps from third parties looking to exploit flaws in current systems. These tools aid SAIs in upholding the confidentiality of audited entities - a crucial mission aspect.

Moreover, the transparency aspect of blockchain transactions offers immense potential to conduct comprehensive and transparent audits by means of the enhanced accountability that it provides - fundamental to maintaining public trust in both audited entities and future audit processes. Lastly, the decentralized structure of blockchains provide SAIs with superior protection against potential attacks or damage when compared to traditional centralized databases.

The advantages of blockchain technology cannot be overstated when it comes to efficiency in auditing processes. It provides a swift reduction in overhead expenses while streamlining audits which leads to more comprehensive results within a reduced timeframe - great news for SAIs under increased pressure to produce high-quality work without increasing budgets. Blockchain's immutability guarantees that transaction history remains unaltered; this makes it possible for auditors to provide an irrefutable audit trail hence reinforcing reliability and precision for future auditing projects.

In addition, this technology facilitates faster transactions requiring fewer steps allowing auditors agility when responding to changes within complex financial landscapes enabling timely conclusions crucial in effective audits. Blockchain further supports collegiality as governing parties follow agreed-upon rules hence enhancing trust- a key concern within SAI's work. The application of blockchain technology presents an avenue for enhancing the potency and authenticity of SAIs. Consequently, this facilitates more productive, open, and secure audits that cater to modern-day requirements.

Costs

Optimizing Efficiency while Cutting Down Costs: How does adopting blockchain technology aid businesses with their transactions? Blockchain eliminates intermediaries leading to decreased expenses and increased efficiency.

Probability of Increased Transaction Expenses due to Growing Energy/Storage Costs: Will escalating energy or storage expenditures in the future affect blockchains' transaction expenses? This factor may cause conducting businesses via this method more expensive.

Influence of Transaction Volumes on Energy Usage: Is there a relation between energy usage and upper limits in transaction volumes when using blockchain? Energy consumption will increase as transactions' numbers rise thus affecting operational expenses.

Storage Expenses Conundrum: What effect does storing data indefinitely on blockchain databases have on financial institutions? As the amount of stored data increases with time so does storage expenses for the concerned institutions. This issue is of utmost importance when considering Supreme Audit Institutions.

Efficiency can be improved through cost reduction using blockchain technology. Nevertheless, it's crucial to manage associated rises in transaction, energy, and storage costs if we want sustainable and beneficial use of this technology.

Report conclusions

Based on the realization that the accelerated development of information technologies in contemporary society is having a strong impact on all aspects of its functioning, it is clear that SAIs face the challenge of ensuring that governments and state agencies make prudent and regulated use of these technologies to achieve their own objectives, while SAIs use them extensively to achieve their objectives of controlling the legality and efficiency of state actions with increasing effectiveness.

Although the various sections of this report overlap in many respects, the intention is not to draw final conclusions on the extent to which to adopt and how to conduct the development of the technologies studied, but rather to provide an overview to serve as a basis for a more advanced discussion of these topics at a later stage.

From the review of the technologies studied in this report, it is concluded that they interact and leverage each other and that together they have a broad scope and offer very significant potential benefits for audit functions and that their awareness and use is spreading rapidly among governments and IASs.

Examples and applications in the use of the technologies investigated were compiled, showing that they are increasingly being used by governments and state agencies in several countries and also in some SAIs, albeit to a lesser extent.

The adoption of these technologies poses requirements with respect to the organization of the IAS, including:

- Overcoming resistance to change
- Assessing the capacity and skills of the IAS's own staff.
- Establishing tasking units or task forces as may be needed
- Assigning qualified personnel to their development
- Interacting with external agencies, including universities, research organizations and consultants
- Manage knowledge within the SAIs
- Strengthen data governance

In addition to internal personnel and external consultants, the development of the technologies analyzed require advanced resources, both in hardware and software, which are often not available, concluding that it will be necessary to allocate adequate budgets to the task at hand.

It was agreed that all these technologies, to a greater or lesser degree, have ethical, privacy and confidentiality implications that are of concern to society and must be addressed, while realizing their full potential benefits.

Bibliography

Bibliography

Advanced Data Analytics

SAI India

Stanton, J. M. (n.d.). Introduction to Data Science. Surface at Syracuse University. Retrieved November 2, 2022, from https://surface.syr.edu/istpub/165/

Guidelines on Data Analytics. (2017). cag.gov.in. https://cag.gov.in/uploads/guidelines/Guidelines-on-Data-Analytics-book05de4f7fd52e56567820093.pdf

(PDF) Big Data and Analytics in the Modern Audit Engagement: Research Needs. (n.d.). ResearchGate. https://www.researchgate.net/publication/313286738_Big_Data_and_Analytics_in_the_Modern_Audit_Engagement_Research_Needs

Krieger, F., Drews, P., & Velte, P. (2021). Explaining the (non-) adoption of advanced data analytics in auditing: A process theory. International Journal of Accounting Information Systems, 100511. https://doi.org/10.1016/j.accinf.2021.100511

Al-Saaideh, M., & Tarraf, A. (2022). The Boundaries and Difference between business intelligence, big data analytics, and big data: A review Walid kaskas. Indian Journal of Economics and Business, 21(3). http://www.ashwinanokha.com/resources/3.%20Majdi%20Al-saaideh.pdf

NetSuite.com. (n.d.). What Is Advanced Analytics? Oracle NetSuite. https://www.netsuite.com/ portal/resource/articles/erp/advanced-analytics.shtml

Advanced Analytics vs Business Intelligence. (n.d.). RapidMiner. Retrieved November 2, 2022, from https://rapidminer.com/glossary/advanced-analytics-vs-bi/

Saghafian, M., Laumann, K., & Skogstad, M. R. (2021). Stagewise Overview of Issues Influencing Organizational Technology Adoption and Use. Frontiers in Psychology, 12. https://doi. org/10.3389/fpsyg.2021.630145

Ting Si Xue et al., A Literature Review on Knowledge Management in Organizations, Research in Business and Management, Vol. 4, No. 1, February 2017, https://www.researchgate.net/

publication/313872580_A_Literature_Review_on_Knowledge_Management_in_Organizations Team, E. ai. (2017, June 26). The Disruptive Nature of Taxonomy and Ontology Management. Expert.ai. https://www.expert.ai/blog/enterprise-taxonomy-ontology-management/

Prakash, Protiviti, Data Analytics, Audit Tools & Techniques, Institute of Chartered Accountants of India, July 2019, https://www.wirc-icai.org/images/material/Data-analytics-auditttools-15072019.pdf

Guidance Note on Usage of Remote Sensing Data and Geographic Information System for effective audits. (n.d.). Comptroller and Auditor General of India. https://cag.gov.in/uploads/guidence_notes/guidanceNotesPracticeGuides-05f10744c088698-54461273.pdf

Report Number 1 on the accounts of Government of Assam by the Comptroller and Auditor General of India. (2018). Cag.Gov.In. Para 2.9.2.2 and 2.9.2.3, Pg. 41-42, https://cag.gov.in/uploads/download_audit_report/2018/Chapter_2_Performance_Audit_relating_to_Government_Company_of_Report_No_1_of_2018_-_Public_Sector_Undertakings_Government_of_Assam.pdf

Audit Report N°3. (2020). Comptroller and Auditor General of India (Performance and Compliance Audit). Para 2.1.6.3, Pg. 24, https://cag.gov.in/webroot/uploads/download_audit_report/2020/Eng_Audit%20Report%20(P&CA)%202019-20_compressed-062e78118d6a603.39117079.pdf (2022). Unesco.org. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Guidelines on Data Analytics. (2017b). Office of the Comptroller and Auditor General of India. https://cag.gov.in/uploads/guidelines/Guidelines-on-Data-Analytics-book05de4f7fd52e565-67820093.pdf

Advanced Data Analytics for IT Auditors. (n.d.). ISACA. Retrieved November 2, 2022, from https:// www.isaca.org/resources/isaca-journal/issues/2016/volume-6/advanced-data-analyticsfor-it-auditors

Shu, H. (2016). Big data analytics: six techniques. Geo-Spatial Information. Science, 19(2), 119– 128. https://doi.org/10.1080/10095020.2016.1182307

Louzada, F., & Ara, A. (2012). Bagging k-dependence probabilistic networks: An alternative powerful fraud detection tool. Expert Systems with Applications, 39(14), 11583–11592. https:// doi.org/10.1016/j.eswa.2012.04.024

Shu, H. (2016). Big data analytics: six techniques. Geo-Spatial Information Science, 19(2), 119–

128. https://doi.org/10.1080/10095020.2016.1182307

High Dimensional Data Analysis | Department of Statistics. (n.d.). Statistics.berkeley.edu. https://statistics.berkeley.edu/research/high-dimensional-data-analysis

What is deep learning? (2018). Sas.com. https://www.sas.com/en_us/insights/analytics/deeplearning.html

Precision analysis. (2012, October 2). Www.ibm.com. https://www.ibm.com/docs/en/iis/9.1?topic=overview-precision-analysis

Shu, H. (2016). Big data analytics: six techniques. Geo-Spatial Information Science, 19(2), 119– 128. https://doi.org/10.1080/10095020.2016.1182307

How data analytics can help with audits - National Audit Office (NAO) insight. (n.d.). National Audit Office (NAO). Retrieved November 2, 2022, from https://www.nao.org.uk/insights/howdata-analytics-can-help-with-audits/

Cordero, M. (n.d.). Data Analysis & Analytics at GAO. Retrieved November 2, 2022, from https:// portal.tcu.gov.br/data/files/0D/A6/24/16/79D44510739E11452A2818A8/11-SAI%20USA%20 Data%20Analysis%20Analytics%20At%20GAO.pdf

RPA

SAI Pakistan

Benefits of RPA. (2022, Oct). Retrieved from www.kofax.com: https://www.kofax.com/learn/blog/benefits-of-rpa

Dr. David K. Rehr, D. M. (June, 2022). The Promise of Robotic Process Automation for the Public Sector. A Research Paper from the Robotic Process Automation (RPA) Initiative at the Center for Business Civic Engagement George Mason University .

Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures. (2022, October). Retrieved from The CPA Journal: https://digital.gov/guides/rpa/rpa-use-caseinventory/

Feiqi Huang, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. International Journal of Accounting Information Systems .

History of RPA. (2022, October). Retrieved from ww.javatpoint.com: https://www.javatpoint. com/history-of-rpa

Marc Eulerich, J. P. (July, 2021). A Framework for Using Robotic Process Automation for Audit Tasks.

Robotic Process Automation - Challenges. (2022, Oct). Retrieved from www.theecmconsultant. com: https://theecmconsultant.com/robotic-process-automation-challenges/#:~:text=Some%20of%20the%20robotic%20process,scalability%2C%20maintenance%2C%20and%20integration

RPA for Government. (2022, October). Retrieved from www.rearch.aimultiple.com: https://research.aimultiple.com/rpa-government/

RPA in the Government Sector. (2022, October). Retrieved from www.nanonets.com: https://nanonets.com/blog/rpa-in-the-government-sector/

RPA Private best Practices. (2022, October). Retrieved from www.raconteur.net: https://www.raconteur.net/technology/automation/rpa-failures/

Steps to Ensure Robotic Process Automation Security, confidentiality & ethics. (2022, October). Retrieved from www.Gartner.com: https://www.gartner.com/smarterwithgartner/4-steps-toensure-robotic-process-automation-security

The Evolution of RPA Past, Present and Future. (2022, October). Retrieved from www.uipath.com: https://www.uipath.com/blog/rpa/the-evolution-of-rpa-past-present-and-future

The History of Robotic Process Automation. (2022, October). Retrieved from www.adaptivegrowth.com: https://adaptivegrowth.com/the-history-of-robotic-process-automation/#:~:text=The%20History%20of%20RPA%20Automation,systems%20and%20incompatible%20legacy%20 systems

Artificial Intelligence

SAI Thailand

Ad Hoc Committee on Artificial Intelligence Policy Development Group. (2021, May 21). Artificial Intelligence in the Public Sector. Retrieved from https://rm.coe.int/cahai-pdg-2021-06-27793226-6755-v-1/1680a29927

Anastassia Fedyk et. al (2022) in "Is artificial intelligence improving the audit process?", Review of Accounting Studies (2022) 27 : 938-985.

Artificial intelligence for more efficient public spending audits. (n.d.). Ods.fapesp.br. Retrieved November 6, 2022, from https://ods.fapesp.br/artificial-intelligence-for-more-efficient-publicspending-audits/8180

Chowdury, M. (2021, August 12). The Evolution of Artificial Intelligence: Past, Present, Future. Retrieved from https://www.analyticsinsight.net/the-evolution-of-artificialintelligence-past-present-future/

Dotel, R. (2020). Artificial Intelligence: Preparing for the future audit. Retrieved from http://intosaijournal.org/artificial-intelligence-preparing-for-the-future-of-audit/.

Fedyk, A. and Hodson, J. and Khimich N., and Fedyk, T. "Is artificial intelligence improving the audit process?", Review of Accounting Studies (2022) 27: 938-985.

Genest, V. (2019). Artificial Intelligence and Auditing: Overview of Potential Impact On Public Sector Auditor. Research Highlights of Canadian Audit & Accountability Foundation.

Ghanom, S. and Alaba F. (2020). Integration of Artificial Intelligence in Auditing: The Effect on Auditing Process. Master thesis in Auditing and Control of The Kristianstad University.

Gullichsen, I. (2020). PowerPoint Presentation of the National Audit Office of Finland in the ECA conference on Big and Open Data for European Union Supreme Audit Institutions.

Julian Torres Santeli, & Gerdon, S. (2019, August 16). 5 challenges for government adoption of AI. World Economic Forum. https://www.weforum.org/agenda/2019/08/artificial-intelligencegovernment-public-sector/

Koerner, K. (2022, January 11). Privacy and Responsibility AI. Retrieved from https://iapp.org/ news/a/privacy-and-responsible-ai/

McCarthy, J.(2007, November 12). What is Artificial Intelligence?. Retrieved from http://www. formal.stanford.edu/jmc/ Minister for Communications and Information of Singapore. (2020). Model Artificial Intelligence Governance Framework.

Neves, F., Silva, P., Carvalho H. (2019). Artificial ladies against corruption: Searching for legitimacy at the Brazilian Supreme Audit Institution. Retrieved from http://www.revistas.usp. br/rco/article/view/158530/157720

Noordin, N., Hussainey, K, and Hayek, A. (2022). The Use of Artificial Intelligence and Audit Quality: An Analysis from the Perspectives of External Auditors in the UAE. Journal of Risk and Financial Management.

OECD. (2019). Hello, World: Artificial Intelligence and its Use in the Public Sector, OECD Working Papers on Public Governance No.36.

Santeli, J. and Gadon, S. (2019, August 16). 5 Challenges for Government adoption of AI. Retrieved from https://www.weforum.org/agenda/2019/08/artificial-intelligence-governmentpublic-sector/

Santiso, C. (2022, July 6). Artificial intelligence in the public sector: An engine for innovation in government if we get it right! Retrieved from https://oecd-opsi.org/blog/ai-an-engine-forinnovation/

Machine Learning

SAI Chile

Decarolis, F. (2022, 18 marzo). Corruption red flags in public procurement: new evidence from Italian calls for tenders - EPJ Data Science. SpringerOpen. https://epjdatascience.springeropen. com/articles/10.1140/epjds/s13688-022-00325-x

Mazrekaj, D. (2021, 4 junio). Identifying Politically Connected Firms: A Machine Learning Approach. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3860029 Using machine learning for anti-corruption risk and compliance. (2021). Coalition for Integrity. https://www.coalitionforintegrity.org/

Artificial Intelligence – a promising anti-corruption tool in development settings? (n.d.). U4 AntiCorruption Resource Centre. Retrieved October 26, 2022, from https://www.u4.no/publications/ artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings

Petheram, A., Pasquarelli, W., & Stirling, R. (2019, May). THE NEXT GENERATION OF ANTICORRUPTION TOOLS - Artificial Intelligence. Oxford Insights. https://www.oxfordinsights.com/ ai-for-anti-corruption

Haenlein, M., & Kaplan, A. (2019, July). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. California Management Review.

Hello, World: Artificial intelligence and its use in the public sector | READ online. (n.d.). oecdilibrary.org. Retrieved October 26, 2022, from https://read.oecd-ilibrary.org/governance/helloworld_726fd39d-en

Danielkievych, A. (2022, October 1). Your Guide to Machine Learning in Fraud Detection. Forbytes. https://forbytes.com/blog/fraud-detection-in-machine-learning/

Kapadia, S. (2022, August 3). 6 Steps towards a Successful Machine Learning Project. Medium. https://towardsdatascience.com/6-steps-towards-a-successful-machine-learning-project3a56f59e2747

Jordan, J. (2021, January 3). Organizing machine learning projects: project management guidelines. Jeremy Jordan. https://www.jeremyjordan.me/ml-projects-guide/

C3.ai. (2021, April 21). Infrastructure: Machine Learning Hardware Requirements. C3 AI. https:// c3.ai/introduction-what-is-machine-learning/machine-learning-hardware-requirements/

Pazzanese, C. (2020, December 4). Ethical concerns mount as AI takes bigger decision-making role. Harvard Gazette. https://news.harvard.edu/gazette/story/2020/10/ethical-concernsmount-as-ai-takes-bigger-decision-making-role/

Brown, S. (2021, April 6). 7 lessons to ensure successful machine learning projects. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/7-lessons-to-ensure-successful-machinelearning-projects

Santiso, C. (2022, August 24). Artificial intelligence in the public sector: An engine for innovation in government . . . if we get it right! Observatory of Public Sector Innovation. https://oecd-opsi.org/blog/ai-an-engine-for-innovation/

West, D. M. (2022, March 9). Using AI and machine learning to reduce government fraud. Brookings. https://www.brookings.edu/research/using-ai-and-machine-learning-to-reducegovernment-fraud/

Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities. (2021, June 30). U.S. GAO. https://www.gao.gov/products/gao-21-519sp

Ariwala, P. (2020, October 14). How Machine Learning Facilitates Fraud Detection? Maruti Techlabs. https://marutitech.com/machine-learning-fraud-detection/

11 Most Popular Machine Learning Software Tools In 2022. (2022, October 25). Software Testing Help. https://www.softwaretestinghelp.com/machine-learning-tools/

López-Iturriaga, F. J. (2017, November 22). Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces. SpringerLink. https://link.springer.com/article/10.1007/ s11205-017-1802-2?error=cookies_not_supported&code=90bcf1ad-f19a-4861-a05235267fc46957

Machine Learning Basics: An Illustrated Guide for Non-Technical Readers. (2021). Dataiku.

Seita, D. (2019, August 13). Evaluating and Testing Unintended Memorization in Neural Networks. The Berkeley Artificial Intelligence Research Blog. https://bair.berkeley.edu/blog/2019/08/13/ memorization/

Engstrom, D. F., Ho, D. E., Sharkey, C. M., & Cuéllar, M. F. (2020). Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3551505

A guide to the types of machine learning algorithms. (n.d.). SAS UK. Retrieved October 26, 2022, from https://www.sas.com/en_gb/insights/articles/analytics/machine-learning-algorithms. html

5G

SAI Philippines

CISCO. (2019, June 7). Five Steps to 5G Deployment. Retrieved from CISCO: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-offers-service-provider/whitepaper-c11-742416.html

Curtis, B. (2022, October 19). 5G Innovations and Cybersecurity Risk. Retrieved from ISACA: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/5g-innovations-andcybersecurity-risk#62

Dahlman, E., Parkvall, S., & Skold, J. (2018). 5G NR: The Next Generation Wireless Access Technology. London: Academic Press.

GSMA Intelligence. (2019, June 13). Intelligence Brief: How much will we pay for 5G? Retrieved from mobileworldlive.com: https://www.mobileworldlive.com/blog/intelligence-brief-howmuch-will-we-pay-for-5g#:~:text=Based%20on%20operators'%20data%2C%20the,%245%20to%20%2472%20per%20month.

Institute of Internal Auditors. (2019). 5G and the Fourth Industrial Revolution Part II. Global Perspectives and Insights. Florida: Institute of Internal Auditors.

Jenal, C., Endreß, S., Kühne, O., & Zylka, C. (2021). Technological Transformation Processes and Resistance—On the Conflict Potential of 5G Using the Example of 5G Network Expansion in Germany. Sustainability, 1-20.

Lin, X., & Lee, N. (2021). 5G and Beyond: Fundamentals and Standards. Cham: Springer Nature Switzerland AG.

Miolo, A., & Lussu, F. (2018, June 8). 5G and Audit: How smartphones and devices will revolutionise the future of business and our services. Retrieved from Deloitte:

https://www2.deloitte.com/ ch/en/pages/audit/articles/future-5g-audit-smartphones-devices-switzerland.html

Office of Auditor General of Ontario. (2021). Value-for-Money Audit: 5G Network Technology and 5G Pre-commercial Program. Ontario: Office of Auditor General of Ontario.

Protiviti. (2022). At a Crossroad: Weighing the Realities and Risks of 5G. Retrieved from Protiviti: https://www.protiviti.com/US-en/insights/whitepaper-crossroad-weighing-realities-andrisks-5g

Statista. (2022, July 14). Total 5G enhanced mobile broadband base costs in Europe between 2019 and 2040, by country. Retrieved from Statista: https://www.statista.com/statistics/1245950/ europe-5g-embb-base-cost-by-country/

Wazid, M., Das, A., Shetty, S., Gope, P., & Rodrigues, J. J. (2021). Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. IEEE Access, 4466-4489.

World Economic Forum. (2020). The Impact of 5G: Creating New Value across Industries and Society. Geneva: World Economic Forum.

Yu, H., Lee, H., & Jeon, H. (2017). What is 5G? Emerging 5G Mobile Services and Network Requirements. Sustainability, 1848.

Blockchain

SAI Vietnam

Khizar Hameeda, Mutaz Barikab, Saurabh Garga, Muhammad Bilal Amina Byeong Kanga, “A Taxonomy Study on Securing Blockchain-based Industrial Applications: An Overview, Application Perspectives, Requirements, Attacks, Countermeasures, and Open Issues”, Journal of Industrial Information Integration, Volume 26, March 2022, 100312, https://www.sciencedirect.com/science/article/abs/pii/S2452414X21001060

Iman Supriadi, Hendra Dwi Prasetyo ,Miya Dewi Suprihandari, “The Effect of Applying Blockchain to The Accounting and Auditing”, Ilomata International Journal of Tax & Accounting, Vol. 1 No. 3 July 2020 pp.161-169 https://www.ilomata.org/index.php/ijtc

Friedrich Holotiuk, Jürgen Moormann, “Dimensions, Success Factors and Obstacles of the Adoption of Blockchain Technology”, Australasian Conference on Information Systems 2019, Perth Western Australia, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1016&context=acis2019

Osmani M., El-Haddadeh, R.Hindi N., Janssen M., Weerakkody, Vishanth J.P. “Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis”, Journal of Enterprise Information Management, ISSN: 1741-0398, 12 April 2021, https://www.emerald.com/insight/content/doi/10.1108/JEIM-02-2020-0044/full/html

Francesca Fallucchi, Marco Gerardi, “Blockchain, State-of-the-Art and Future Trends”, Computer Science, 2022

Suyel Namasudra, Ganesh Chandra Deka, Prashant Johri, Mohammad Hosseinpour, Amir H. Gandomi, “The Revolution of Blockchain: State-of-the-Art and Research Challenges”, Archives of Computational Methods in Engineering volume 28, pages1497–1515 (2021), https://link.springer.com/article/10.1007/s11831-020-09426-0

ADGSOM Project Completion Report, “Blockchain for digital government – the ASEAN way”, https://asean.org/wp-content/uploads/2022/02/02-Final-_-Report-Blockchain-for-digital-government.pdf

Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne, “Blockchain for 5G and beyond networks: A state of the art survey”, Journal of Network and Computer Applications, Volume 166, 2020, 102693, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102693.

ELOMMAL Najoua, MANITA Riadh, “How Blockchain Innovation could affect the Audit Profession:
A Qualitative Study”, Journal of Innovation Economics & Management, 2022/1 (N° 37), p. 3763. DOI : 10.3917/jie.pr1.0103. URL : https://www.cairn.info/revue-journal-of-innovationeconomics-2022-1-page-37.htm

A. Chaer, K. Salah, C. Lima, P. P. Ray and T. Sheltami, “Blockchain for 5G: Opportunities and Challenges,” 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1-6, doi: 10.1109/GCWkshps45667.2019.9024627.

Archana Chhabra, Rahul Saha, Gulshan Kumar, Tai Hoon Kim “A Survey of Privacy Concerns in Blockchains and Information Retrieval” Algorithms, Computing and Mathematics Conference, August 19 – 20, 2021, Chennai, India, https://ceur-ws.org/Vol-3010/PAPER_01.pdf

Otia, J. E., & Bracci, E. (2022). Digital transformation and the public sector auditing: The SAI’s perspective. Financial Accountability & Management, 38 252– 280. https://doi.org/10.1111/faam.12317

Pietro De Giovanni, “Blockchain Technology Applications in Businesses and Organizations”, February 2022 DOI:10.4018/978-1-7998-8014-1,
https://www.researchgate.net/publication/358900259_Blockchain_Technology_Applications_in_Businesses_and_Organizations

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."

WGISTA Project Participants

Chair – United Arab Emirate

Vice-chair – United States of America

SAI Chile

SAI India

SAI Pakistan

SAI Philippines

SAI Thailand

SAI Vietnam