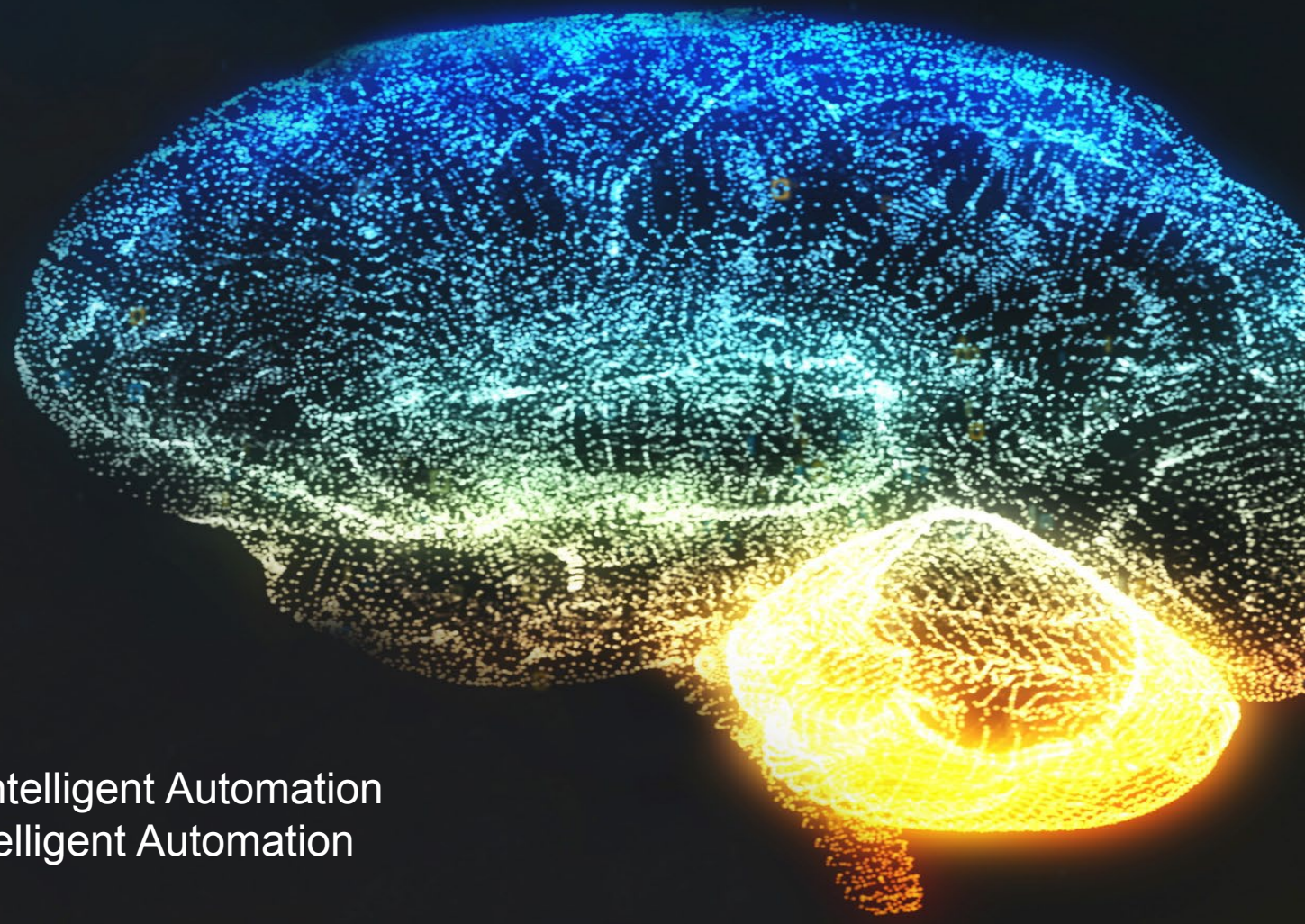
KPMG

How is AI transforming Audit

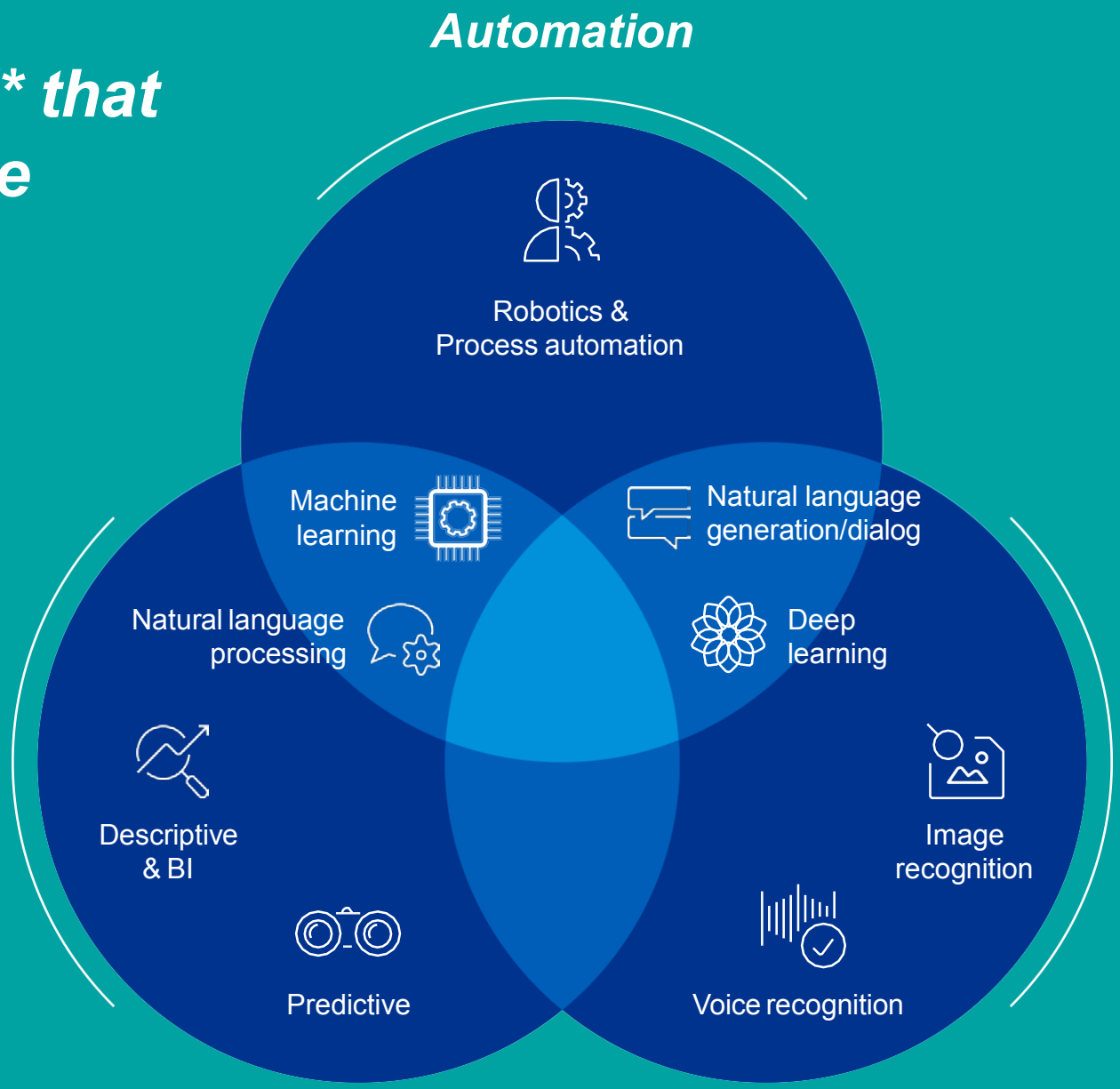


Payam Mousavi, Director, US Government Intelligent Automation
Michael Butler, **Director**, US Government Intelligent Automation

Agenda

- What is AI
- How is AI transforming Audit

The *"Trifecta"* that will change the face of Audit*



* Source: Image inspired by *The HfS Triple A Trifecta: Automation, Analytics, and Artificial Intelligence,* by Phil Fersht, Jamie Snowdon, Tom Reuner, Saurabh Gupta (August 31, 2017)

KPMG

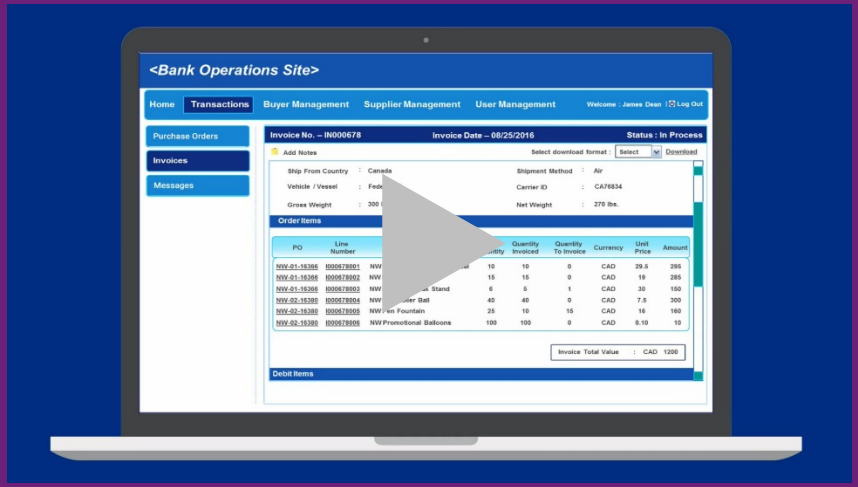
Control Testing

Demo

Link: https://vimeo.com/245282322

Automated contract management

Demo



https://www.youtube.com/watch?v=qOko42eQZIg&feature=youtu.be

How can internal audit help the organization?

In a business environment that's changing at a faster rate than ever before, internal auditors play an increasingly important role.

With the vast uncertainties presented by an onslaught of disruptive forces, the internal audit function must keep pace to help the organization understand and manage the associated risks, achieve expected results from automation, and continue to innovate to add value.

Key opportunities for internal audit within intelligent automation initiatives include the following:

Internal Audit can help to integrate **governance, risk and controls** considerations throughout the automation program life cycle as an organization establishes and implements its program.

Internal Audit as an independent assurance provider

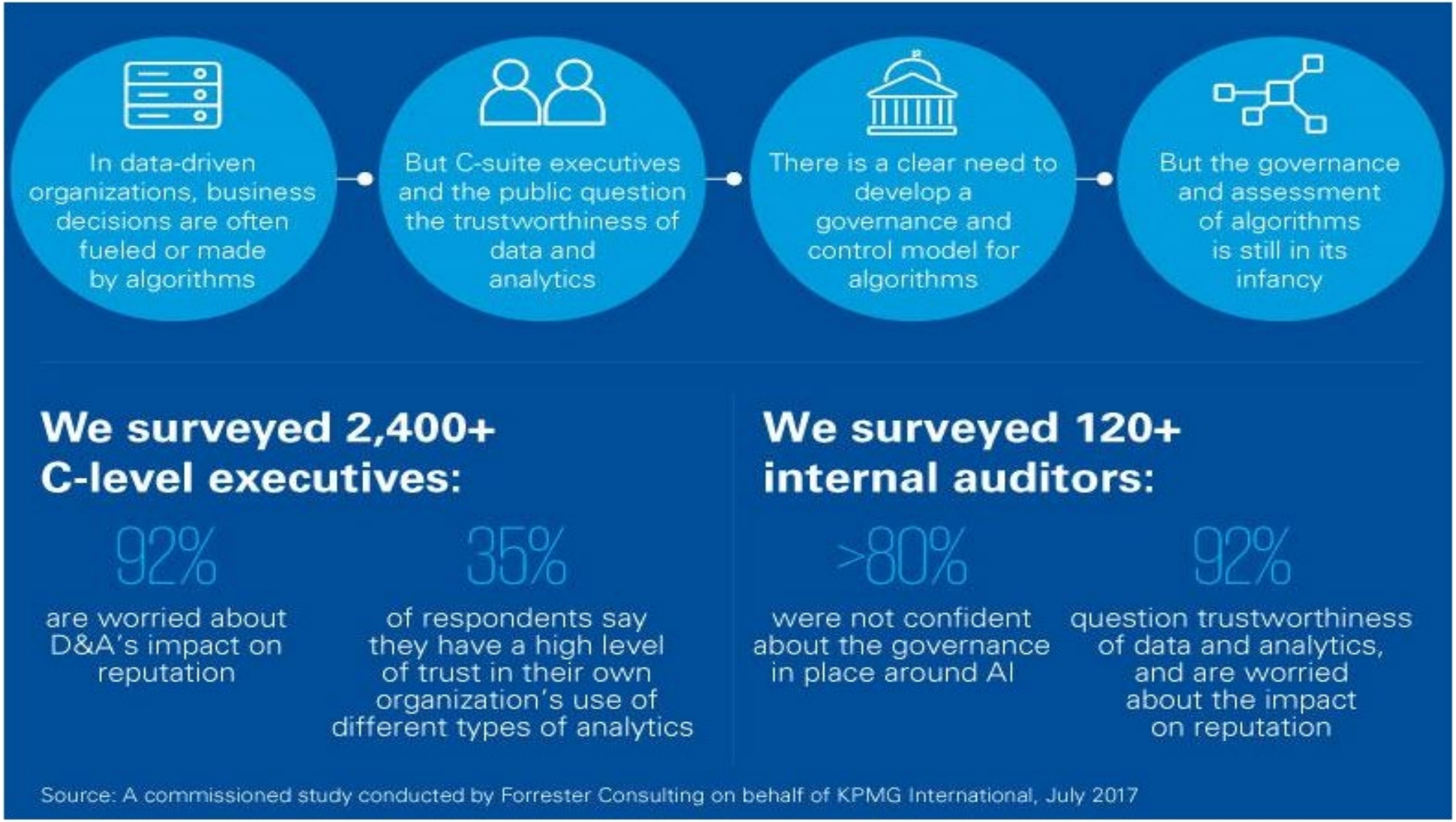
Internal audit can help the organization identify opportunities to **embed automation-enabled control activities within the impacted business processes and functions**.

Internal Audit as a business advisor

Finally, the internal audit organization can capitalize on intelligent automation innovations to **increase the efficiency and effectiveness of its own activities.**

Internal Audit as a business leader

Audit as independent assurance



How to approach Risk, Security, and Privacy?

Applying Leading Practices
(i.e., What's new)

Plan the bot

- Select the right processes; Optimize these processes before automation
- Establish ownership of bots & accountable individuals for each bot between business and CoE
- Establish baseline bot architecture, logging, security control patterns, and monitoring requirements

Build the bot

- Automation tools should refer to screen elements or field level attributes rather than position
- Where possible, ensure bots can work with web services or write directly to a database so that bots can be more resilient to screen level changes
- Integrate 'privacy by design' considerations as required under applicable laws
- Ensure input and output bot datasets are tamper proof and have integrity

Applying industry leading frameworks
(i.e., What we already knew)

Plan the bot

- Establish or integrate with a governance framework to enable and support security and risk management
- Identify impacted regulatory requirements, including data privacy and data protection
- Establish a mapping of all controls impacted before design and build
- Ensure appropriate redundancy and backup processing is retained for specific high risk processes

Build the bot

- Apply principles like DevOps to the model lifecycle to mitigate the risk of false positives
- Establish separate environments for Bot development, QA and production
- Ensure bots are developed to specified requirements and secure coding practices
- Apply principles of 'least privilege' and 'privacy by design' to constrain bot access

How to approach Risk, Security, and Privacy? (continued)

Applying Leading Practices
(i.e., What's new)

Run the bot

- Manage changes to the robot configuration and any integrated up and downstream processes in a controlled manner
- Establish sensors and detailed logging to enable activity monitoring and traceability for transactions where applicable
- Ensure that bot communications over wire are encrypted

RPA Experience

Applying industry leading frameworks
(i.e., What we already knew)

Run the bot

- Ensure the robotic workforce have turned up for work – i.e. are logged in, functioning, balancing workloads
- Backup all bots in production. Consider the use of redundant / backup parallel processing for critical bots
- Regularly assess the failover and recovery capability and plans to ensure any disruption in the robotic availability does not impact the business

NIST

COBIT

GAPP

Trusted and Explainable AI has several dimensions

Agile and Robustness

Here we're talking about being sure the model can be served up as an API; that it's serviceable across vendors; and resilient to adversarial attacks, an emerging vector that manipulates the training data to warp the integrity of the model's output, creating bias or inaccurate results that could damage a brand. The attack is not visible to the naked eye, of course, and AI audits are one way of detecting them.

Fairness

Models as well as the training Algorithms can't be trusted if features are not appropriate for the goal—the use of age or gender, for example, when there is no statistical difference in these aspects. Explicit information about these features is not always the leading factor in producing discriminatory algorithms; another issue involves proxies, data that is very closely related to these identifiers. A postal code can be a proxy for ethnic origin or income, for example. It's important to note that, in many instances, personal information is relevant to the model.

Integrity

Think of a home inspection that checks the 'bones' of a house for any structural flaws to see what the integrity of an algorithm means: understanding the lineage of training data, the identity and actions of the subject matter experts involved, from start to finish, and the verification that no changes mar the original goal or intent of the algorithm.

Explainable

This is a subjective capability in AI. Being able to explain why and how a model produced an output depends on the definition of success established and the overall governance of the algorithm. Here the focus is on what the model has learned and how the system works.

Audit as Business Advisor

Opportunities for the 1st and 2nd Lines of Defense

Agency functions

Human resources

- Employee on-boarding and off-boarding
- Payroll
- Time recording and compliance
- Repeatable tasks in ERP
- Email notifications
- Populating/Aggregating employee information

Citizen engagement

- Social media mining/monitoring
- Predicting high priority incidents
- Manual CRM updates
- Application data entry

Customer support

- Virtual agents (chat bots)
- Call center “agent assist”
- Task execution

Finance and accounting

- IPAC
- CARS
- Invoice processing/exceptions
- AP/AR actions
- Reporting
- Auditing
- Filings

Compliance

- Research/document review
- Document preparation
- Controls automation

Supply chain & procurement

- Contract management
- Exceptions/fallout

Fraud and data validation

- Interfaces to 3rd party sources
- Predictive analytics
- Data quality improvements

Information Technology

- Automate Dashboards and metrics reporting
- Automate IT GRC controls execution/validation
- UAM and IAM requests/reviews
- Testing
- HW/SW requests/fulfillment
- Automate backups, archives, & upgrades

Example areas of automated solutions for control testing

Business process testing – Automated testing of manual and automated controls

Manual

- Reconciliations
- A/R Aging
- Cash Transfers
- Journal Entry Analysis
- Fee Audits
- Loan Review
- Nightly Settlement
- Contract Compliance

Automated

- Edit Checks
- Validations
- Calculations
- Interfaces
- Reports

Other Control Testing

- Compliance testing
- Cyber security testing
- P&C Reserving
- Payments – OFAC compliance
- Payments reconciliations
- Positive pay validation

IT controls testing – Automated testing of IT general controls by platform and/or ERP

Change Management

- Changes are Authorized
- Changes are Tested
- Changes are Approved
- Dev Access to Production

Logical Access

- Passwords
- New Users
- Periodic Review
- Terminations
- SOD

Computer Operations

- Incident Management
- Backups
- Job Scheduling
- Physical Security

Audit as Business Leader

CMS Intelligent Automation Project

Modernizing a time-consuming and manual document intake validation process

Challenge

- Congressionally mandated to annually measure accuracy of payments
- **100,000** records submitted for evaluation
- Limited funds and resources allocated to perform tasks
- Untimely feedback to stakeholders due to volume of records

Approach

- Solution a combination of:
  - RPA
  - Optical character recognition (OCR)
  - Machine learning
  - Natural language processing

Benefits

- Annual cost and time savings
  - **$1M+** [estimated]
  - **5** months
- Improved customer experience
  - **75%** faster feedback
- Identified human errors
- Increased workforce satisfaction
  - Specialized resources focus on more meaningful reviews instead of clerical tasks

Large State Agency

Predicting and recommending records to audit

Challenge

This agency's mission is to maximize state revenues and prudently manage state lands and natural resources.

- In recent years, a relatively small staff has annually audited just a fraction of the thousands of oil and gas lease contracts to make sure leaseholders pay royalties owed. The process is fraught with potential errors and omissions as lease contracts are bought and sold over many years.
- Process is mundane with over 100 manual steps and can only review one lease at a time even though many leases can be related.

Approach

- Using IBM Watson predictive analytics and machine learning we provided agency a prioritized list of records to audit with the highest potential of revenue generation.
- Our solution ingests data from a number of different sources including volume data from third party agencies, pricing, and other structured and unstructured data in addition to historical data for machine learning.
- A user interface was built bringing together in an interactive layout data from all sources and predicting the additional potential royalty owed as well as complexity of the record for processing.

Benefits

- 100% compliance by reviewing all leases.
- Discovered over $30M in potential additional revenue missed from previous 5 years.
- Provided insights to reduce effort by 80% by prioritizing the records with the highest potential.
- Provided additional insights on data issues and other metrics and trends from reviewing all leases in the last 5 years.

Defense Logistics Agency (DLA)

Building and governance of RPA for audit readiness

Challenge

- Highly manual and large volume of processes
- Inconsistent processes that impact financial reporting and lead to audit deficiencies
- Reduced and aging workforce
- Multiple audit findings based on inconsistent processes, lack of documentation, ICOFR (internal controls over financial reporting)
- Lack of understanding and inability to quickly respond to audit requests
- Limited collaboration across functional departments
- Nonexistent RPA Governance structure

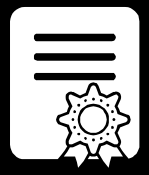
Approach

- Supported selection of an RPA vendor most suited to be integrated into DLA's operational process and security requirements
- Identified a digital workforce capability consisting of RPA for process owners to address operational and audit challenges
- Invested in highly skilled resources from IT and finance to pilot RPA at DLA, and leadership leaned in to support this initiative

Benefits

- Automated financial and CIO processes by deploying 10 bots
- Transitioned workforce from manual, low value tasks to high value tasks
- Helped support the remediation of NFRs around posting logic and Evidential Matter
- Reduced error in transactional tasks
- Estimated up to 5,600 hours to be saved from initial unattended bot deployment
- Working to establish DoD leading Governance structure/Center of Excellence (COE)

Why integrate AI?



Audit Quality

— Amid ubiquitous information and exploding data

Insights

— More detailed audit evidence

— Enhanced transparency, consistency, depth of audit procedures

— Deeper views into organizations' risks, controls, operating environment

Empower and Enable

— Future success for audit professionals

Confidence

— Identify anomalies

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia