How automation increases quality in tax compliance

By Michael Bloom, Partner and Filston Mongu Nkoy Bonsey, Senior Manager at Deloitte Tax & Consulting

Needless to say, the regulatory landscape becomes increasingly complex and abundant. This evolution has contributed to the rise of Big Data and is driving the move to a digitalized world.

Glancing in the rearview mirror, you might agree that this transition has improved life, but also generated new types of challenges. As such, tax compliance practitioners (hereafter **tax officers**) processing massive amounts of data are more and more exposed to different types of potentially time-consuming problems and therefore risks linked to data processing errors.

Keeping in mind that tax officers usually act as one of the key stakeholders in the application of tax regulations, can we say that automation helps them solve problems and add value to tax compliance services?

Here, we could evoke Oliver Wendell Holmes, Jr.'s prescience from 1897[1]: *"For the rational study of the law, the black-letter man may be the man of the present, but the man of the future is the man of statistics and the master of the economics"*

Digitalization has taken over more and more analogous data processing including in tax compliance where automation technologies are flourishing. We'll address some of those automation technologies and briefly describe how they can be leveraged in tax compliance.

Machine learning: predictive tax law interpretation to comfort tax positions?

Research and development are conducted on machine learning technology that addresses tax topics. This algorithmic technology aims to enable machines to become more accurate at spotting data patterns to help make decisions. One interesting development in machine learning is Blue J's[1] tools which are inspired by one of the basic principle of tax law: "equality before law."[2]

In a nutshell, as explained by Benjamin Alarie's (Chief Executive Officer at Blue J), Blue J's work starts with equal application of the law by calculating the occurrence probability of outcomes/resolutions of a specific tax case/issue to predict said outcomes for that given tax issue. As an example, he takes the problematic of a

classification of a very specific financial instrument as a debt versus equity for tax purposes, and simultaneously the valuation of said financial instrument. In such a case, Blue J's tool applies a reverse-engineering approach.

As such the machine is fed training data (like tax legislation, tax case laws, market's position for this specific case) and builds a model in order to provide a predictability percentage (80%, 60%, more likely than not, etc.) of said financial instruments classification.

Everyone (tax payers and tax administrations alike) stand to benefit from that resulting model of how the courts, market or tax administration are approaching the qualification and valuation problems of such financial instruments. It goes without saying that algorithms do not aim to replace court decisions but rather to provide a forecast of outcomes that save tax officers time in data processing while improving accuracy.

Natural Language Process (NLP) and Natural Language Generation (NLG)[3]

NLP is an artificial intelligence technology that enables machines to notably translate unstructured data, such as voice and video, into structured data with labels and quantities that machines can readily process. Completing the loop, NLG can create conversations and written reports from structured data that look and feel like human-created responses.

Let's assume the hypothetical case of tax due diligence where both NLP and NLG are used. In such a case, thousands of data types (tax returns, conference call recordings, videos, etc.) are first processed by NLP application and normalized (i.e. unstructured data converted into structure data) to enable comparisons, mergers and connections between data or to merge structured datasets. NLG can create customized narrative reports (addressing tax findings from tax returns, legal documents, contracts etc.) ready to be exploited by the tax due diligence team members.

Robotic Process Automation (RPA)[4] – the case of electronic filing of the tax returns

Robotic Process Automation (RPA) uses software "robots" to capture and interpret existing IT applications to enable transaction processing, data manipulation and communication across multiple IT systems.

RPA software performs routine business processes by mimicking the way that users interface with applications and by following simple rules to make decisions. Entire end-to-end processes can be performed by software robots with very little human interaction.

RPA can be used to automate processes that are:
- Repetitive
- Prone to error
- Rules based
- Involve digital data
- Time critical and seasonal

Typically, this software is used to automate the e-filing process of tax returns or tax reporting (like county by country reporting/notification, DAC6 form, etc.). Tax officers can use RPA to automate the upload of relevant forms/data on tax authority websites for reporting purposes.

Most of the above steps, if not all, can be performed by RPA which will navigate different tools and applications with greater efficiency and accuracy, freeing up tax officers to devote more time to more valuable tasks in the service cycle.

Optical Character Recognition (OCR)[5] and Extract, Transform and Load (ETL)[6]

OCR is a type of NLP technology that aims to analyze an image, use patterns to detect if the image contains text, and extract that text into a machine-readable format. It can also help to convert handwritten characters into a machine-readable format.

ETL tools combine three important functions: extract, transform and load. These functions are required to get data from one data environment and into another.

A typical data warehouse architecture extracts data from source systems (stored in databases, flat files, web services, etc.), followed by an ETL component that combines and transforms the data and loads it into the data warehouse. The data stream ends at the data marts or leads to reporting and analytics streams defined on top of the data warehouse.

Just imagine how combining the "arms and legs" of RPA with the "eyes" of OCR and "brain" of machine learning can help businesses overcome challenges in processing semi-structured and unstructured documents.

For instance, integrating OCR and machine learning helps systems learn and improve as they are exposed to larger volumes of documents. This synergy results in higher straight-through processing rates and enhances productivity for the human team, who can focus on dealing with exceptions and more complicated scenarios.

Several solutions were designed by Deloitte member firms, including the Deloitte Intelligence Document Processing or CognitiveTax Insight™ developed by Deloitte Tax LLP (via its multistate tax services team).

CognitiveTax Insight™ (CogTax) enables Deloitte tax officers to advise clients about their indirect tax needs including:
- Efficiently identifying, recovering and remediating overpaid indirect taxes for companies operating in complex transactional data environments.
- Capturing key data points from thousands of invoices and documents within days – or even hours – as opposed to weeks or months.
- Transforming indirect tax analysis, such as recovery, from a backward-looking assessment to a real-time analysis and remediation.
- Quickly and accurately analysing refund potential and exposure/liabilities.

Other tools are being designed in the same spirit and aim to:
- Use both advantages of OCR and ETL to capture data (notably using metadata) from standard communication from tax authorities (like tax assessment, audit letters, etc.)
- Allow the extraction, transformation and generation of formatted documents (like e-mail, letters etc.) for use when communicating with the client.

The solutions are contributing to the reduction of corporation's costs but also help tax payers to proactively avoid missing deadlines, overpaying taxes or missing tax's reimbursements.

Automation tools, an ally to tax officers

The work of tax officers evolves in data-driven environments where leveraging technology and automation to provide operational efficiency can be part of the answer to the challenges evoked.

As such, most of the above mentioned tools are using technology relying on artificial intelligence theories, concepts and technology pertaining to human being intelligence (such as visual recognition, algorithms trained to make predictions and decisions, etc.). But "*human intelligence*" does not (yet) mean that tax officers simply need to push a button for tools to handle the entire cycle of tax compliance services.

So far, these tools are designed and trained to process and combine complex rules through massive amounts of different data types via increasingly sophisticated systems that performed quicker than individuals could.

Implementing the above technologies in incremental stages in the most painful parts of the tax compliance service cycle will be crucial to ensure both risk and cost reduction.

Combined with tax officers' analytical skills and expertise (concentrated in adding value), let there be no doubt: tax compliance services and professionals are navigating this automation shift. But to go even further, a holistic and a fully integrated strategy might be necessary to bring this service into a "3.0" world.

1) The Expanding Role of Artificial Intelligence in Tax - YouTube Featuring B. M. Willis and B. Alarie – consulted on 30 March 2022
2) Article 6 of the declaration of the human and civil rights / Article 10bis of the Luxembourg Constitution or article or article 13 of the declaration of the human and civil rights
3) Natural language processing in IM | Deloitte Insights - consulted on 20 April 2022
4) Robotic Process Automation (deloitte.com) – consulted on 4 April 2022.
5) Deloitte Uses AI to Transform Indirect Tax Recovery – Press Release | Deloitte US – consulted on 4 April 2022
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consultancy/deloitte-uk-intelligent-document-processing-report.pdf consulted on 4 April 2022
6) The Future of ETL | Part I | Deloitte Netherlands – consulted on 4 April 2022

Cybersécurité : les banques doivent privilégier une approche Zero Trust

Le secteur financier demeure l'un des principaux secteurs ciblés par les cybercriminels : selon l'analyse de Mastercard sur l'évolution de la cybercriminalité durant la pandémie (chiffres de 2021), les institutions financières de Belgique sont les cibles privilégiées des hackers (21%), juste après les organisations gouvernementales (24%). Suite à l'invasion russe en Ukraine, l'Autorité Bancaire Européenne (EBA) a déclaré que le risque d'effondrement des banques russes, biélorusses ou ukrainiennes constituait une menace moindre que les effets de «second tour», comme les cyberattaques qui «peuvent conduire à des dégâts plus importants en matière de stabilité financière».

«La cybersécurité est une priorité des banques depuis de nombreuses années, mais les craintes augmentent encore. Aujourd'hui les criminels sont des pirates informatiques experts qui ciblent les services bancaires, et en particulier les guichets automatiques, avec le triple objectif de voler de l'argent, subtiliser des informations financières précieuses et provoquer des interruptions de service. Génératrices d'importants revenus, les attaquants travaillent comme de véritables organisations criminelles structurées dont les niveaux de formation, de coordination et de financement sont similaires à ceux d'une entreprise de technologie de pointe, avec même des budgets importants de recherche et développement.», indique Stefano Cipollone, Business Development Manager chez Auriga.

De nouveaux risques pour la sécurité bancaire

La numérisation de nombreuses activités bancaires, l'utilisation de technologies avancées dans les agences de nouvelle génération et l'utilisation de connexions à distance également pour les activités de conseil ont stimulé un changement aussi du côté des cyberattaques qui, outre les structures bancaires, visent désormais plus directement les clients des services. L'augmentation des attaques par rançongiciels devrait particulièrement susciter l'inquiétude. Une étude récente menée par des experts en cybersécurité de l'unité 42 de Palo Alto Networks a révélé que la demande de rançon moyenne a grimpé de 144% pour atteindre 2,2 millions de dollars. Selon le rapport Hiscox Cyber Readiness 2022, qui examine l'état de la cybersécurité au sein des entreprises dans huit pays, ce sont la Belgique et l'Allemagne qui ont subi le plus d'attaques par ransomware. Pour leur stratégie de cybersécurité, les banques doivent tenir compte de la manière dont les nouvelles méthodes de travail et de gestion bancaire affectent l'équilibre des risques. Avec la fin des confinements, des modèles de travail hybrides maison/bureau subsistent, ce qui conduit à ne pas sous-estimer le risque que les employés travaillant à domicile deviennent par inadvertance des failles de sécurité.

Dans le même ordre d'idée, la forte augmentation du nombre de clients effectuant des opérations bancaires en ligne comporte des risques car l'utilisateur moins averti est une cible plus facile pour les escroqueries en ligne ou les attaques de phishing.

L'approche Zero Trust pour les terminaux en libre-service

Tous les terminaux bancaires, depuis les postes de travail jusqu'aux guichets automatiques et ASST, sont des dispositifs critiques qui fournissent des services essentiels aux citoyens et doivent garantir la disponibilité et la fiabilité du service, en continu et sans interruption. Pour cette raison, du point de vue de la sécurité, l'absence de politiques de mise à niveau proactives, associée à l'accessibilité physique de ces dispositifs, crée un environnement intrinsèquement vulnérable qui rend les appareils en libre-service très difficiles à protéger avec les technologies de sécurité traditionnelles. Ainsi, il faut définir une stratégie de sécurité adaptée à l'environnement à protéger et revoir en permanence les stratégies de cybersécurité.

Fondamentalement, les banques doivent avoir un aperçu plus rapide des activités anormales ou suspectes dans leurs systèmes. La meilleur pratique consiste à conserver ces systèmes critiques et les autres composants de l'infrastructure des services bancaires dans une infrastructure dédiée, séparée du réseau de l'entreprise par des politiques d'accès strictes qui sont contrôlées et surveillées dans le temps. C'est ce que l'on appelle l'approche Zero Trust (confiance zéro), qui s'avère être l'une des philosophies les plus efficaces pour sécuriser les terminaux critiques.

Le Zero Trust consiste à minimiser le niveau de confiance implicite afin de ne pouvoir accéder à un système et l'utiliser lorsque des contrôles rigoureux sont effectués. Ce concept clé peut être appliqué aux guichets automatiques et aux ASST, qui comptent plusieurs couches logicielles : système d'exploitation, couche logicielle du fournisseur de matériel, couche multi-fournisseurs éventuelle, et différents outils d'exploitation, de surveillance, de sécurité, etc. Ce grand nombre de couches est source de vulnérabilités, qui peuvent se glisser dans les logiciels par inadvertance.

«La valeur qu'apporte le Zero Trust pour sécuriser les services bancaires numériques en libre-service est de ne pas faire confiance à la sécurité supposée des logiciels grand public, mais plutôt à un processus de certification des ressources et des interactions considérées comme dignes de confiance en fonction des besoins opérationnels, réalisé par les équipes de sécurité», ajoute Cipollone.

L'application de ce modèle permettrait de réduire la surface d'attaque en autorisant les opérations uniquement lorsqu'elles sont nécessaires et certifiées correctes, et en définissant des politiques basées sur l'état du dispositif, qui sont plus ou moins strictes lorsque les DAB sont en service (donc physiquement accessibles et potentiellement vulnérables à la cybercriminalité), ou lorsqu'ils sont vides et en maintenance.

Une stratégie Zero Trust, en effet, devrait s'étendre aussi aux outils et services tiers de maintenance de ces appareils, en mettant en place un système de surveillance qui interroge les autorisations d'accès à tout moment ou tout lieu. Le technicien tiers autorisé à intervenir en cas de maintenance devra se soumettre à un processus d'authentification (par exemple avec un code OTP) afin de pouvoir procéder à la manipulation du logiciel ou du matériel de l'appareil», conclut Cipollone.