Inevitable technologies that will shape IA future

by Oleg Kourzanov

REFINITIV™

TECH agenda for today

- BIG data
    - CAATS
        - Cloud
            - Artificial Intelligence
                - Machine learning and predictive Analytics
                    - Blockchain

Sensitivity: Confidential

Intro

Internal Auditor is My Super Hero!

Independent, reliable, very knowledgeable and very strict!

Trusted advisor who holds the hand of business!

Big respect from a former External auditor!

Sensitivity: Confidential

You have NO time left!

¾ of you still work in  and 

Are you losing breath competing  with  ?

Can you handle that curve of change? 

You can't postpone things for tomorrow any longer!

New TECH will win the game! 

"Those who fail to integrate these initiatives risk becoming obsolete as their organizations continue to undergo digital transformation at an increasingly rapid pace."
Brian Christensen, executive vice president of global internal audit at Protiviti.

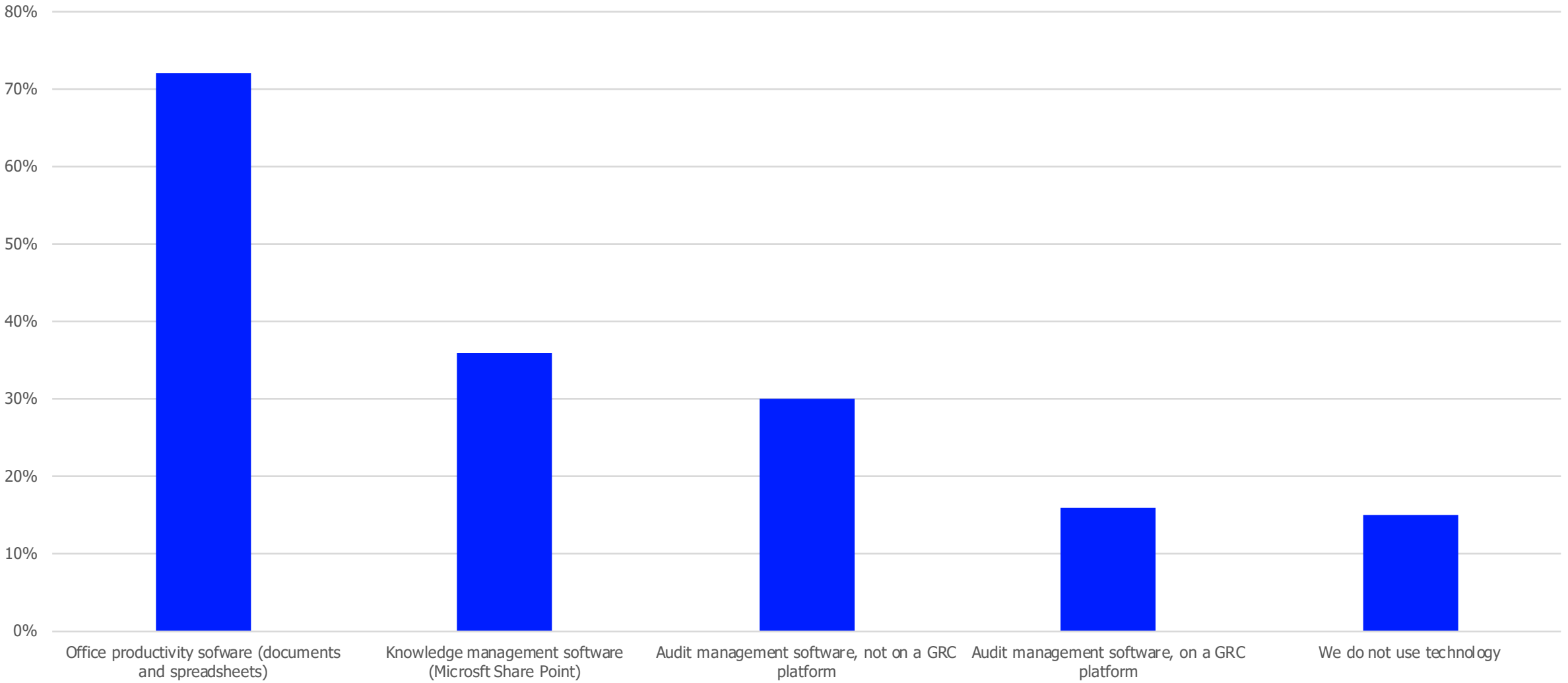
Quantitative change builds into a magic quality blow overnight!

===➔ LEARN, LEARN AND LEARN!
===➔ Fight for budgets for education & automation as if there is no tomorrow!!!

REFINITIV

Sensitivity: Confidential

Don’t just take my word for it…



By MetricStream 2018 research

REFINITIV™

Sensitivity: Confidential

Things are not that bad… yet…

- **A majority of internal auditors are seeking technology solutions for real-time access to data, as well as detailed analysis and presentation**

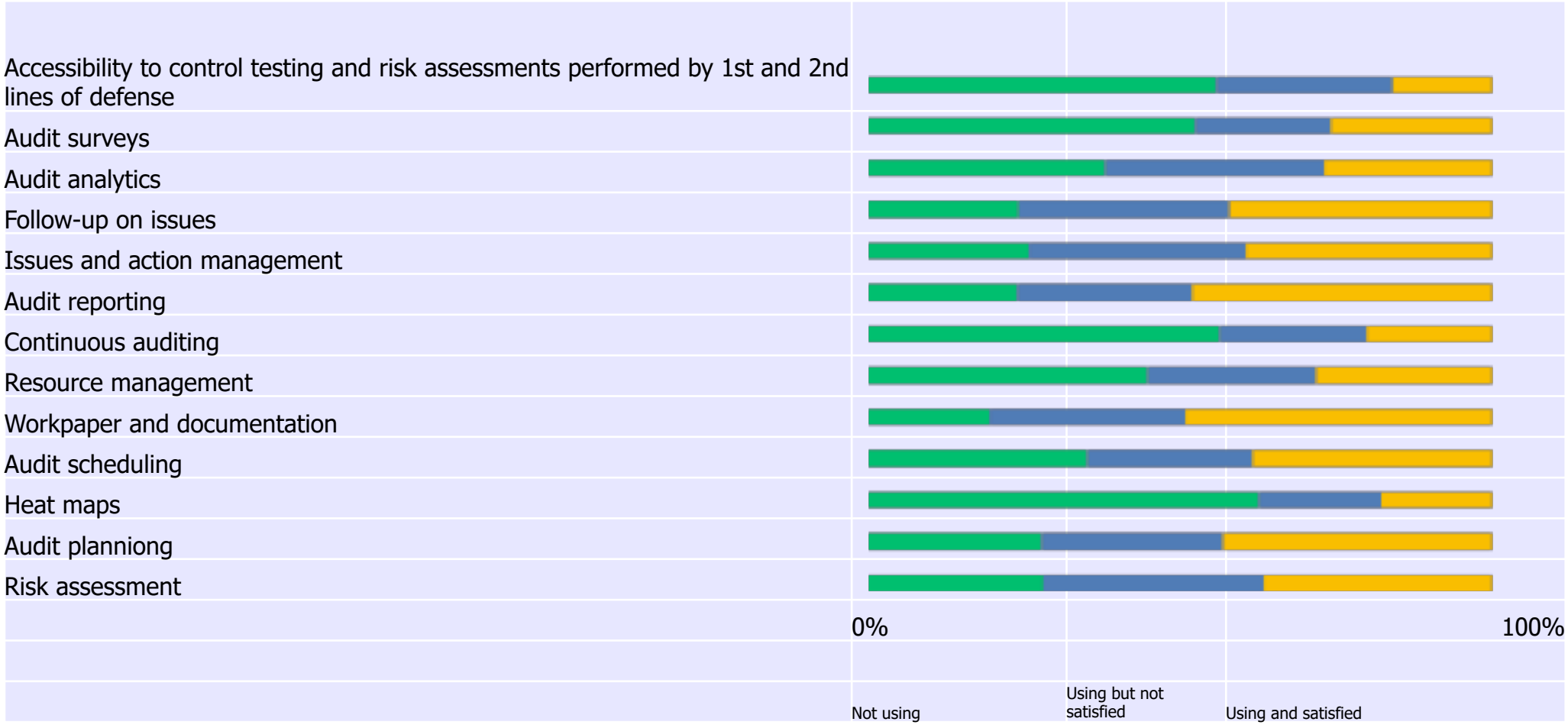
- ✓ **77%** of the respondents want data querying and analysis tools
- ✓ **75%** want continuous control monitoring tools
- ✓ **60%** want data visualization capabilities
- ✓ **58%** want modeling and predictive analysis tools

REFINITIV™

Sensitivity: Confidential

Good with workpapers… but missing on tech staff…

The areas where the majority of respondents do not use technology are **heat maps**, **continuous auditing**, and **accessibility to control testing and risk assessments performed by the first and second lines of defense**.



By MetricStream 2018 research

Sensitivity: Confidential

What is changing…

Recent guidance by **The Basel Committee and the European Banking Authorit**y (EBA) and **IIA** procedures show little change - same way & similar tools….

HOWEVER! You must assess and evaluate the risk management and governance of multiple departments to:

=➔ stay ahead of any relevant technological innovation

=➔ be aware of how new technologies can be applied to risk management and governance & understand them well enough to be able to evaluate whether they are being used appropriately and effectively.

Extra work required to ensure that areas such as cybersecurity and the use of AI are being carried out with rigor, or are being used effectively.

Auditing AI requires careful consideration – as the technology becomes more prevalent, internal auditors must be able to identify whether it is being used correctly, and whether it is appropriate and cost-effective for a particular application.

REFINITIV™

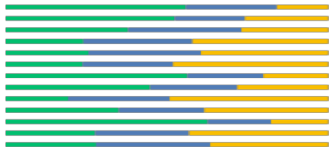
Sensitivity: Confidential

Ripe for automation… starting slow…

Automation can occur throughout the auditing process:

- **Generating alerts.** Audit calendars can be configured to send event-based reminders to those personnel responsible for specific actions. Alerts can also be set up to inform others about the progress of actions in the auditing process, including actions that have been completed, and those that need to be escalated.

- **Automating audits**. Although this is not always appropriate, some auditing processes can be automated, using CAATs, which can extract data from databases, check the data to ensure specific criteria are met, and store the findings in a database. Continuous auditing (remember previous slide???) is a good candidate for automation, as it requires repeated actions at regular intervals, or constant surveillance of a process or system for any changes.



- **Reporting**. Firms can use the results and findings from audits to create and deliver standard audit reports.

REFINITIV™

Sensitivity: Confidential

CAATS – one more time – but you know it already!

CAATs is Computer Assisted Audit Techniques

Facilitates you to make search from the irregularities from the given data to get more analytical results.

More forensic work with more analysis - efficient and productive.

Transforms large raw data into in statistical and analytical form. Saves  & detects fraud…

- ✓ Select the right data
- ✓ Selection process is very much tricky
- ✓ Import that to the CAAT tool
- ✓ The tool will automatically generate the analytical data.

REFINITIV™

Sensitivity: Confidential

Here comes the BIG difference & BIG data…

- “Good buy!” sample – “Hello!” complete review!

- **For example**, an insurance company may want to ensure that it doesn't pay any claims after a policy is terminated. Using traditional audit techniques this risk would be very difficult to test. The auditor would "randomly select" a "statistically valid" sample of claims (usually e if any of those claims were processed after a policy was terminated. Since the insurance company might process millions of claims the odds that any of those 30–50 "randomly selected" claims occurred after the policy was terminated is extremely unlikely.

- Using CAATs the auditor can select every claim that had a date of service after the policy termination date. The auditor then can determine if any claims were inappropriately paid. If they were, the auditor can then figure out why the controls to prevent this failed. In a real life audit, the CAATs auditor noted that a number of claims had been paid after policies were terminated. Using CAATs the auditor was able to identify every claim that was paid and the exact dollar amount incorrectly paid by the insurance company. Furthermore, the auditor was able to identify the reason why these claims were paid.

REFINITIV™

Sensitivity: Confidential

CAATS impact on your conclusion...

Example of an audit report statement:

"Audit reviewed 50 transactions and noted one transaction that was processed incorrectly"

or

"Audit used CAATs and tested every transaction over the past year. We noted XXX exceptions wherein the company paid YYY dollars on terminated policies."

DATA IS KEY!

However, the CAATs driven review is limited only to the data saved on files in accordance with a systematic pattern. Much data is never documented this way. In addition saved data often contains deficiencies, is poorly classified, is not easy to get, and it might be hard to become convinced about its integrity. So, for the present CAATs is complement to an auditor's tools and techniques. In certain audits CAATs can't be used at all. But there are also audits which simply can't be made with due care and efficiently without CAATs.

REFINITIV™

Sensitivity: Confidential

Managing data sources!

- Methodology shift from prohibiting & over-regulation to genuine approach to responsible business.

- Managing disparate data sources is central to risk management

- This data is typically drawn from multiple sources

=➔ **Data of varying quality - a blessing or a curse? Both!**

- Nonetheless, risk professionals have found that existing technologies struggle with the complex nature of risk data. New solutions are required.

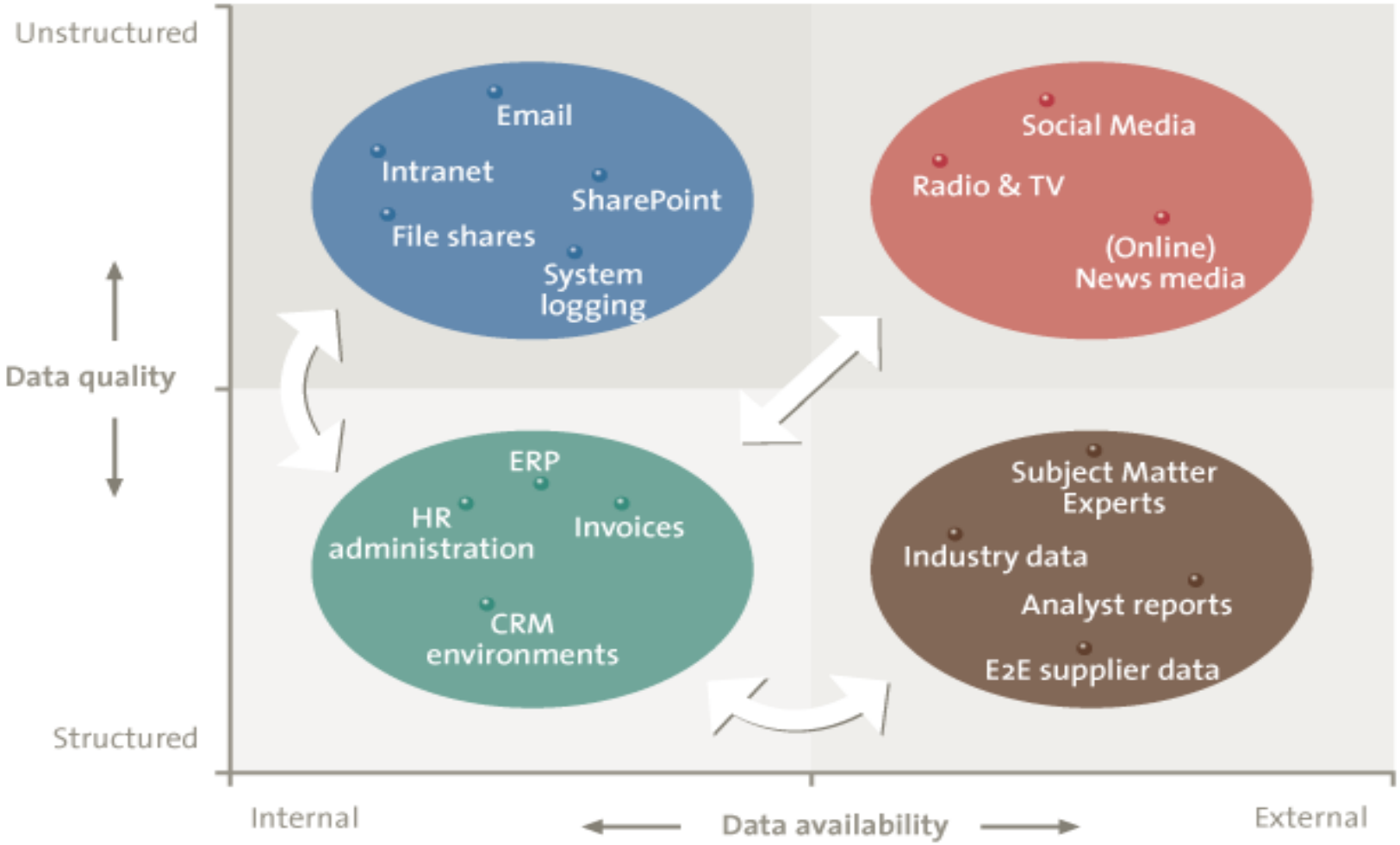
- There is no shortage of data in the modern world.
  - Multiple instances of same data
  - Data that is not consistently available
  - Data does present challenges.

- Data availability could become a burden!

REFINITIV™

Sensitivity: Confidential

Some data is important but hard to digest…



By: H.B. van Veen MSc RA | M.A.P. op het Veld MSc RE | W.E.J. van Kessel MSc RE - Audit and Assurance

REFINITIV

Sensitivity: Confidential

Real life example!

EXAMPLE OF USING SOCIAL MEDIA DATA IN IMPAIRMENT TESTING

An international retail organization buys its own production forest to ensure delivery of high-quality wood for its own production. The forest, however, adjacent to a protected wildlife area. Threats to occupy the production forest have recently been posted on social media by activists claiming that the production forest threatens the fragile wildlife in the nearby protected area. Should the internal auditor be aware of such threats for his audit of the impairment test on the biological assets of the company? It is very much the question whether the auditor will be able to adequately audit the impairment test by solely using the data available within the organization.

EXAMPLE OF AN EXTERNAL UNSTRUCTURED DATA ANALYTICS SOLUTION

An IA solution uses complex algorithms to analyze large amounts of streaming data. This ranges from Twitter and online news-feeds to radio and TV broadcasts. On a daily basis, it analyzes over 72 billion data records. Such an enormous amount of data can never be analyzed by one person. By using an online and live stream analytics solution, the organization as well as the auditor can immediately spot any potential threats to its biological assets once a message has been posted online. Rather than waiting for the actual damage to be done and being too late in identifying the impact on the valuation of the assets, the organization can immediately point out this development and act upon the potential impact.

REFINITIV™

Sensitivity: Confidential

Warning: SILOS will become history… Here comes the Cloud!

The trend continues towards increasingly **integrated** GRC platforms. This will continue despite regulatory uncertainty and shifting definitions of what constitutes misconduct, largely driven by a set of supply side factors and costs:

- ✓ An increasing focus on cost of GRC and compliance specific technologies. Firms' aggressive cost prioritization programs have placed a higher than usual emphasis on the cost of GRC and compliance technology.
- ✓ The need to keep customers front and center of all operations.
- ✓ Developments in sophisticated data-driven technologies. A whole new ecosystem of data analytics has developed, including: standard big data platforms such as Hadoop, AI on the cloud, and new analytical languages such as Python, R, and Lua.
- ✓ The emergence of AI and robotics as fundamental components of the workflow platforms and robotics (technological mechanisms to mimic humans).

REFINITIV™

Sensitivity: Confidential

Note to self: “I have to watch technology to know my vulnerabilities!”

- The growing complexity of organizations’ technology infrastructures + increased use of new technologies = increases potential attack points and the frequency of attacks.

- Reliance on IT systems also makes them more susceptible to outages and downtime, which most organizations experienced at least once in the last year.

- Organizations must overcome the following hot spot risk areas:

Cybersecurity Preparedness

Cloud Computing

REFINITIV™

Sensitivity: Confidential

Back to cloud - will it rule? Yes… and analytics!

- Cloud, Analytics, And Customer Support Are Key Differentiators

- Opt for a **SaaS** model as a cost effective solution compared to on-premises deployment.

- Pure **SaaS** vendors are viewed as business partners instead of providers.

- **SaaS** providers can monitor customer environments for usage and performance.

- **SaaS** GRC platforms are designed with best practices built into the tool.

REFINITIV™

Sensitivity: Confidential

AI, AI, and AI again…

AI - far more than just aggregating data, you can now normalize, integrate and connect disparate data points, helping you drive insights and reveal opportunities you might otherwise have missed.

AI for GRC: a growth area

- AI technologies (such as Robotic Process Automation [RPA] and Machine Learning) are already being used for pattern recognition, communications monitoring, information capture and the analysis of regulations.

- However, the level of sophistication of many of these systems – in the context of 'pure AI' – is relatively basic, and closer to RPA.

Sensitivity: Confidential

AI for GRC… still experimental but growing fast…

- The use of AI is one of the fastest growing areas in financial services, fueled by an evolution in technology and a reduction in its cost.

- Part of the challenge in the application of AI in GRC has been defining what constitutes AI. RPA - screen scraping, rules engines, macros, graph databases and graph analytics – it is really **advance filtering**!

- True "AI" is broad range of advanced, statistical mechanisms that include neural networks, fuzzy logic, genetic algorithms, heuristic search techniques such as taboo search, topological data analysis, and multi-dimensional factor analysis are generally considered AI. Particularly valuable in the GRC space are statistical and cognitive algorithms (machine learning, topological data analysis).

- At present, AI as it's used in financial services is more commonly associated with RPA than more complicated applications, such as the use of neural networks.

-The use of AI to address aspects of GRC is a relatively new development

REFINITIV™

Sensitivity: Confidential

Enough of theory! Give us some real cases!

1. Analyzing interpersonal communications

Method used: A cognitive computing platform is used to monitor human communications for suspicious patterns. The platform is designed to uncover foreign exchange rate manipulation, unauthorized trading, bribery and money laundering, using a mixture of supervised and unsupervised machine learning. This takes unstructured data (email, chat, image, voice) and structured data (Anti-Money- Laundering [AML], Human Capital Management [HCM], Customer Relationship Management [CRM] and trade surveillance data) to uncover complex relationships. It uses supervised machine learning, trained on customer data, to 'read' the chat, and performs actions such as entity and fact extraction. Then, using unsupervised machine learning, the data is resolved through global coreference, disambiguation and entity reconciliation.

• *Benefits of the method*: Traditional methods can generate excessive false positives and few relevant alerts, so analysts waste time filtering the true positives from the false ones. AI software lowers the false-positive rate for alerts, and increases the number of relevant alerts that are identified.

REFINITIV™

Sensitivity: Confidential

And some more…

2. Reputational risk

Method used: Bayesian networks are used to quantify reputational risk. This works on the assumption that the reputational risk of a bank depends not just on that particular institution, but on the reputation of the industry as a whole. The system can create a network of dependencies between itself and other banks, by scanning news articles, doing simple text searches and classifying certain sets of text matches with positive and negative scores. In this way the network is calibrated with historical data. Today's reputational news items are passed through the network to give a positive or negative score for reputational risk for that particular day.

• *Benefits of the method:* A key benefit of the method is that it gives a sense of how the public feels about other banks, and banking in general. It also provides a quantitative result to allow unambiguous day-to-day comparisons.

REFINITIV™

Sensitivity: Confidential

And another one…

3. AML monitoring rules

Method used: Topological Data Analysis is used to uncover critical patterns and relationships within data. The system can work on the outputs of machine learning analysis to identify geometric relationships between data points and clusters of data points. This enables analysts to look at highly dimensional problems with many variables, to provide a simplified visual representation.

• *Benefits of the method*: By centralizing its analysis, the system was able to reduce the ruleset by five times.

REFINITIV™

Sensitivity: Confidential

Imagine the future….

Future scenarios | A central anti-money-laundering utility is formed

What if… anti-money-laundering (AML) surveillance were provided to all institutions by a centralized and collectively owned service provider?

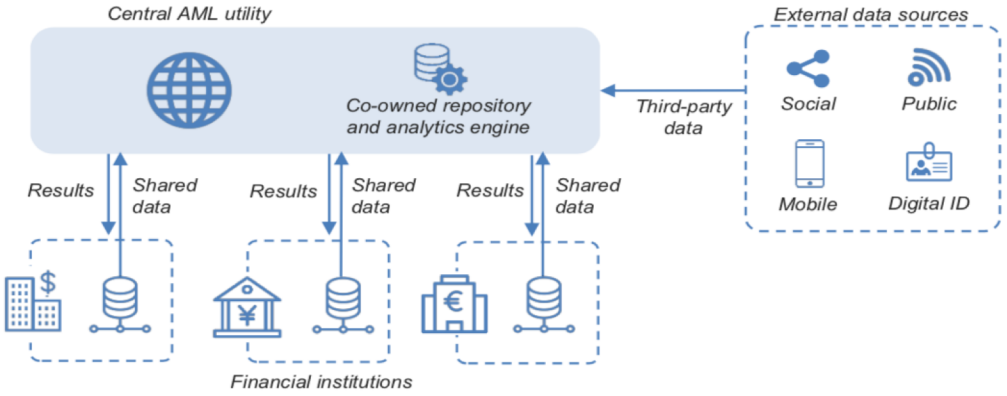
WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

What if…?

Instead of managing AML on an institution-by-institution basis, a central utility is formed by:

- Consolidated data-sharing and analytics models that allow for new, more robust prevention systems with more accurate detection and insight
- Development of "collective intelligence" to protect against money laundering, terrorist financing and other systemic threats, particularly threats employing transactions across multiple institutions that would otherwise be difficult to detect for any one institution

Future state



What would be the implications?

- **Increased financial inclusion** as institutions and regulators become more confident in servicing customers with limited financial histories, or from more risk-prone geographical areas
- **Positive impact on financial institutions' bottom lines** through cost savings in managing AML. Spillover benefits include the reduction in associated prices and a potential revenue uplift from targeting untapped markets
- **A consistent consumer-consent model is required** as current privacy regimes may restrict the creation of a central utility and cross-border data movement
- **A redefined liability model is required** to clearly identify and define the legal and financial responsibility structure for when AML requirements are breached
- **Increasing concentration of risk** as a single false positive or false negative from a central utility is propagated through the entire financial ecosystem
- **Risk of displacement for a large number of financial professionals** as many current AML personnel across individual institutions are made redundant

Why might this happen?

- Sharing data to form a central utility would allow institutions to access more advanced capabilities than even the most sophisticated incumbents could develop independently; machine-learning systems would be able to work on a more complete view of the transaction landscape, allowing institutions to identify suspicious patterns that may be spread across the environment
- Institutions would be able to collectively decrease costs through the commoditized service, removing efficient compliance as a source of competitive differentiation and allowing them to focus investment on more critical areas of expertise (e.g. investments in customer experience)

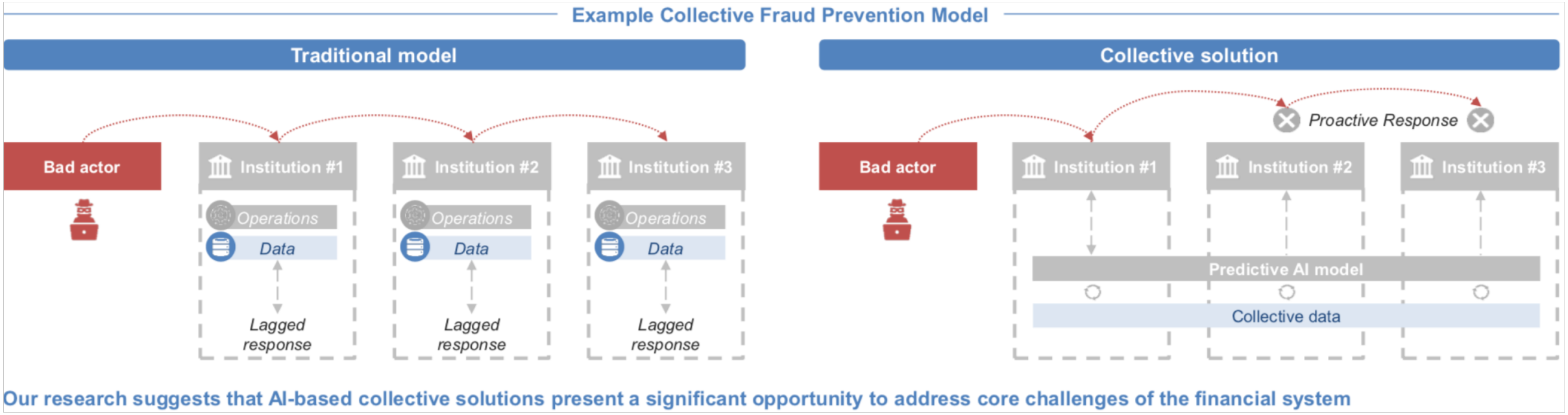
Why hasn't this happened?

- Current solutions are not sophisticated enough to derive meaningful insights from these fragmented cross-institution data feeds, which lack standardization and normalization
- Financial institutions are wary of sharing sensitive customer data with third parties, due to security, regulatory and competitive risks

REFINITIV

Sensitivity: Confidential

Give and Take Data… remember wildlife example?



By World Economic Forum

REFINITIV™

Sensitivity: Confidential

Machine learning and predictive analytics… some real cases

- **ISSUE:** frequently a consequence of multiple, overlapping audit, risk and compliance programs that are fundamentally seeking to address the same considerations. Previous-generation solutions failed.

- **How technology can help:** The necessary data mapping is complex, but has been done in other areas (mapping and modeling customer relationships). Therefore, leveraging technology used for these purposes would advance our ability to streamline risk processes.

- **ISSUE:** Using technology to fully execute, not merely facilitate, audit and risk processes is somewhat of a holy grail that is already achievable with current technologies (IT audit and risk). Challenges arise when the processes, controls or underlying systems to be interrogated are bespoke. For example, automated transaction monitoring is an effective solution to risk profiling, but only if the technologies used can manage non-standardized or qualitative data.

- **How technology can help:** fuzzy logic can been used to at least narrow down critical transactions that would benefit a manual review.

- **ISSUE:** Previous-generation solutions provided both dashboards and automated reporting, with the former seemingly offering drill-down capability – although with limited success.

- **How technology can help:** use dedicated visualization solutions for a multitude of applications.

Sensitivity: Confidential

Last but not least - Blockchain…

- Blockchain first introduced in 2008.

- Bitcoin has become one of the most popular blockchain implementations.

- Blockchain properties:
- 1. Distributed: Each node can obtain all blocks in the chain simply by connecting to the neighboring node. Therefore, everyone in the network has a copy of the blockchain. The public distribution of the complete, intact block chain also precludes any attempt to defraud or contaminate the transaction through the mechanisms of double spending or replaying a duplicate transaction.
- 2. Autonomous: Blockchain network system is an open platform where anyone can participate in the blockchain network without registration or being authenticated to serve as a node, and/or withdraw from the network at will.
- 3. Contractual: All nodes should act in accordance to the rule (also known as a chaincode1) to reach a consensus.
- 4. Trackable: This property is useful in that any transaction is immutable and cannot be altered once the transaction has been completed and added to the block chain.

REFINITIV™

Sensitivity: Confidential

Blockchain is not about Bitcoin….

When corporations like Mastercard, Amazon and Accenture get together to introduced a "circular supply chain" allowing consumers to make more sustainable choices about what they buy, its worth looking at what other circular sustainable business models could be created using distributed ledger technology.

By Forbes

REFINITIV™

Sensitivity: Confidential

Blockchain – revolutionary implications for you!

Blockchain requires a change in the way organizations and individuals think about where to find the "truth" about transactions and information.

BEFORE: A system of record was thought of as the place where there is a definitive value for some unit of data.

NOW: no longer one specific system, within one specific organizational structure, where the truth resides. Instead, there is a permanent shared ledger that provides all interested parties or stakeholders with exactly the same "truth" simultaneously.

IMPACT 1: you need to access information in new formats.

IMPACT 2: you need to maximize the value of "real-time" information.

IMPACT 3: you need to work collaboratively across organizations.

IMPACT 4: finally, some work being routinely performed today will become redundant.

REFINITIV™

Sensitivity: Confidential

Blockchain – what do you do?

1. Training some of IAs on blockchain.
2. IAs must be involved at the planning stage of blockchain-based applications.
3. Internal audit departments must include continuous auditing as part of their standard audit methodology.
4. Meet the demands of their clients while maintaining their professional standards.
5. Perform due diligence to ensure that blockchain applications are the best choice for a specific objective.

In summary: One of the key strategic advantages that IAs have is their knowledge of the business and organization they support. This knowledge will be critical when it comes to supporting the implementation of blockchain for, without this knowledge, adequate assessment of the governance, risk, and control environment will be difficult to provide.

REFINITIV™

Sensitivity: Confidential

TECH training and skills challenge...

Inflexible employment relationships

"The traditional constraints of employment no longer serve the aspirations of institutions and workers"

Extensive effort is required to construct a new employment contract: one that favours flexibility over rigidity, rewards productivity with protection, and structures skills and capabilities around solutions rather than functions or tasks

Mismatch of skills and capabilities

"Leaders are currently crippled by the talent they do and do not have"

Not only is there a severe lack of AI talent within the market, this scenario is worsened by internal structures that are inefficient in their ability to recruit, retain or transition the needs for talent across roles (i.e. deep domain expertise and complementary attributes to machines)

Narrow capacity for training

"We know we need to train, but for what purpose, and to what end?"

Due to limited supply of "AI talent", there is an immediate need to invest resources in more proactive forms of enterprise-wide upskilling and awareness. These efforts are helpful in driving change, but inhibited by the shortage of 'trainers', pace of learning and natural limitations of individuals' capabilities

Incompatible corporate cultures

"It can't be seen, but you can feel it. Culture is a factor that builds you up or breaks you down"

Rules-based environments, predicated on narrow scopes of authority and routine work arrangements, have difficulty in transitioning to a future that demands agility to be a core competency. While culture is nebulous, it serves as an essential obstacle to effective transformation

REFINITIV

Sensitivity: Confidential

Smarter Humans with Smarter Machines!

- IA & AI - NOT - IA VS AI

- "While technology will continue to advance and push boundaries, the industry will continue to rely on human talents to fully understand Internal Audit, think creatively about complexities, and implement solutions successfully and without bias. So continue to invest in ongoing learning for your internal experts and continue to empower future generations to be successful in this critical field."

    - Ellen Wolfe, Product Director, AutoAudit, Refinitiv

Sensitivity: Confidential

Thank you!

REFINITIV™