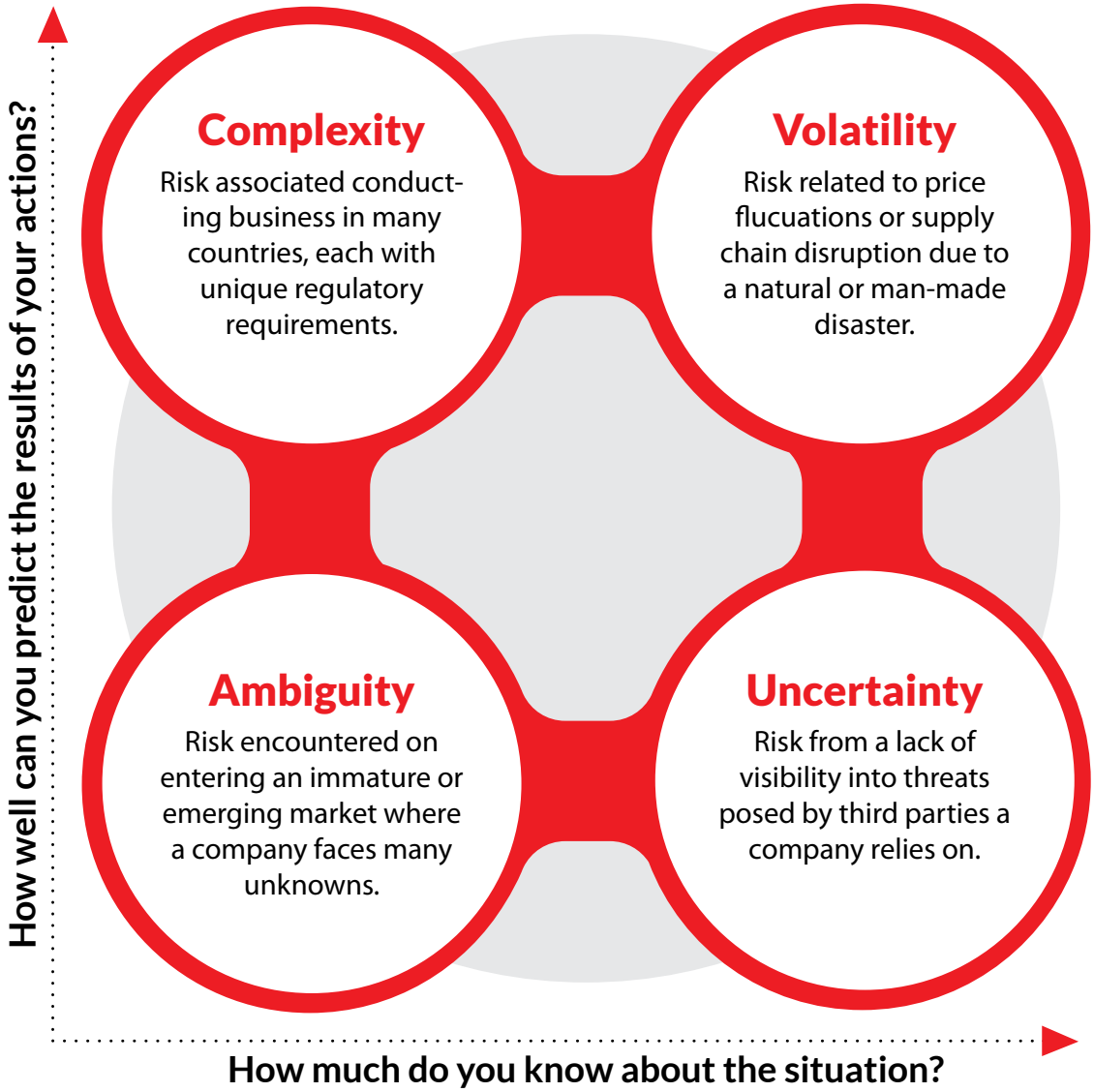
LexisNexis®

Nexis® Solutions

Risk Revolution: How Big Data is Shaping Risk Management

In recent years, many organisations have adopted the military acronym VUCA to describe a global business environment that is volatile, uncertain, complex and ambiguous. The pace of change is rapid, and disruption is frequent. This creates an intense risk landscape which presents a wide range of challenges for organisations.[1]

A Short Explanation of VUCA



The increasing globalisation of business, alongside the growth in digital communications, is resulting in vast digital corporate ecosystems where the performance of third, fourth and even fifth party contacts and suppliers can have a negative risk impact on the organisation. There are complex and often opaque interdependencies between a business, its customers, suppliers and partners.

The escalating regulatory environment adds to the pressure, as companies wrestle with regional variations and the global reach of an increasing raft of regulations such as the Foreign Corrupt Practices Act (FCPA), the General Data Protection Regulation (GDPR) and anti-money laundering legislation.

This constantly changing ecosystem demands that organisations manage risk on a day-to-day, and sometimes hour-to-hour, basis.

If the challenge is growing exponentially, the tools to meet it are also evolving. Collecting, managing and analysing of big data—from internal systems, the Internet of Things (IoT), and data-as-a-service providers offers strategic risk management advantages to organisations as they turn to artificial intelligence to proactively identify, manage, mitigate and prevent risk.

Risk management: The quest for perfect knowledge

Risk management focuses on identifying factors or events that could negatively impact an organisation and assessing the probability of their occurrence. By predicting their impact and subsequent effects, organisations can take action to prevent the risk, reduce and mitigate it, or transfer it via insurance. In this way the organisation establishes its risk posture, namely the amount of risk it is prepared to accept to meet its business objectives.

The more detailed knowledge an organisation has of the risks it faces, the more informed and strategically effective its decisions can be. Therefore, the practice of risk management relies heavily on collecting, structuring and analysing relevant data to seek as perfect knowledge as possible. Big data and analytical processing power enabled by cloud computing has brought us closer to this nirvana of omniscience.

The vast universe of information on everything from company performance, consumer trends and economic, political and social activity to climate change and weather conditions offers a rich dataset for businesses to mine. When cross-referenced with a company's own data, comprising millions of client records and transactions, businesses can start to identify patterns, trends and connections that would previously have been impossible to uncover.

Furnished with this information, the organization can then predict and plan for previously unforeseen incidents and potential disruptions. Analysing historical and current data allows organisations to gain a more comprehensive and real-time picture of the risk environment than has been possible to date.

> Some risks that are thought to be unknown, are not unknown. With some foresight and critical thought, some risks that at first glance may seem unforeseen, can in fact be foreseen. Armed with the right set of tools, procedures, knowledge and insight, light can be shed on variables that lead to risk, allowing us to manage them.
>
> **DANIEL WAGNER**
> CO-AUTHOR OF *GLOBAL RISK AGILITY AND DECISION MAKING*[1]

> In our fast-paced world, the risks we have to manage evolve quickly. We need to make sure we manage risks so that we minimise their threats and maximise their potential.
>
> Risk management involves understanding, analysing and addressing risk to make sure organisations achieve their objectives.
>
> **THE INSTITUTE FOR RISK MANAGEMENT**[2]

By using big data to underpin risk and compliance activities, businesses can become more agile, intelligence-led entities, proactively identifying emerging risks.

In today's fast-paced corporate environment, this can be turned to competitive advantage across several key areas of operation from compliance to supply chain management.

Four Stages of Big Data Analytics

Descriptive Analytics use data to describe what has occurred in the past to make assumptions about the future.

Diagnostic Analytics cross-references data from a variety of sources to identify why an event occurred and its potential outcomes.

Predictive Analytics use historical and current data, statistical algorithms and machine learning to anticipate future risks and opportunities.

Prescriptive Analytics goes a step beyond prediction and prescribes actions aimed at preventing or mitigating risks.

Addressing a growing compliance challenge

The global regulatory environment has grown in scope and intensity in recent years. Mismanaged risk in the sub-prime mortgage market was a major contributor to the financial crisis in 2008 and this, followed by a series of high-profile corporate scandals, has ushered in an era of increasingly tighter regulation. As a result, compliance has become one of the most important areas a business must address if it is to minimise the risk of legal action, fines and the reputational damage associated with a breach of regulations.

Legislation regarding to bribery and corruption, money laundering and terrorist financing and data privacy, for example, place significant burdens on organisations to ensure their operations are compliant. Moreover, it is increasingly clear based on recent prosecutions and court decisions that corporate leaders, including board directors, may be held accountable for compliance failures that take place as a result of their own actions, lack of oversight or both.

This has led to rapidly increasing costs associated with managing compliance risk.

68%

of directors see understanding of risks related to company performance as a key area for board improvement[3]

49%

of board directors say changing regulations represent the greatest potential impact on their organisation[4]

Lifting the compliance burden with big data analytics and automation

For businesses faced with this regulatory environment, big data and analytics have a lot to offer.

Put simply, computers can accurately record, cross-reference and analyse vastly larger quantities of data and variables than their human counterparts. Companies are using this increased capability to interrogate their records and identify compliance issues earlier, so they can move from a reactive to a proactive risk management posture and prevent or neutralise threats before they become a problem. Automating previously manual, time-consuming processes helps to reduce costs, improve compliance efficiency and free up human resources for tasks that require emotional intelligence.

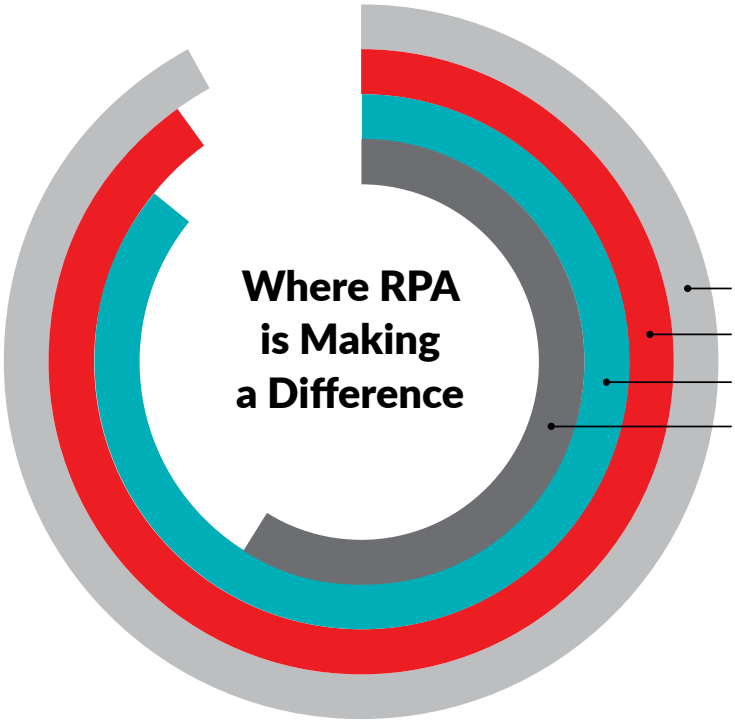
CASE IN POINT:

Credit Suisse

The adoption of big data analytics has been particularly successful in the heavily regulated financial services sector. A case in point is Credit Suisse, which deployed an advanced data analytics platform in 2017. It moved from a manual, human-led system to a technology-led approach to identifying suspicious transactions and potential fraud. Since deployment, the bank has seen a 45-fold increase in the number of productive alerts generated by its predictive monitoring system and a 60 percent faster time-to-resolution, despite the enormous increase in data volumes. This has been achieved at a fraction of the cost of historical compliance activity, which had been rising continuously over the previous three years.

The platform is also tuned to offer visibility of Credit Suisse's complex network of relationships with clients, and to support the assessment of new international clients. This includes identifying and assessing politically exposed persons (PEPs)—those who have connections with governments. Compared to previous practices, assessment of PEPs is now around 60 percent faster at 40 percent lower cost.

"Over the past two years we have gone from a human-led approach to compliance, where we were carrying out periodic checks, to a technology-led approach in which we are continuously monitoring activities across the bank to enable earlier prevention and detection," says Lara Warner, Head of CCRO and Member of the Executive Board of Credit Suisse.[5]



In a 2017 survey on RPA adoption, companies reported that RPA was meeting or exceeding expectations in several key areas.[6]

Improving efficiency and accuracy with Robotic Process Automation

One of the biggest advantages of artificial intelligence and machine learning is the ability to perform repetitive tasks with consistent accuracy. This has distinct benefits when it comes to compliance activities such as customer, vendor and third-party screening. This activity requires the aggregation of disparate data sources including internal systems and external sources such as watchlists, sanctions data and PEPs information. It is a time-consuming process that is prone to human error.

Robotic Process Automation (RPA) eliminates these errors, automatically collecting, storing and analysing data from regulatory agencies such as the FSA and law enforcement agencies like Interpol as well as from internal datasets, with a high degree of accuracy.

Outcomes that raise red flags are escalated to human judgement currently, but as neuro-linguistic analysis and cognitive automation mature, RPA could extend to automated rules-based decision-making around compliance risks.[7]

RPA allows organisations to benefit from a much higher degree of confidence in their current risk exposure because, rather than offering a point-in-time assessment, the position can be continuously monitored, and issues flagged as soon as they occur.

Employing RPA also means organisations can divert employees to higher value tasks, while remaining confident that their risk mitigation process is robust.

There are challenges to implementing RPA, mainly around data quality and the preparedness of existing systems to support automation, as Liz Jordan, managing director Deloitte Risk and Financial advisory explains: "RPA's heavy reliance on data to automate compliance processes makes data quality paramount. It's also critical to determine whether technology infrastructure has the capacity to accommodate RPA, and that existing systems are compatible with the new automation tools and system security can be maintained in the automated environment."[8]

Hunting the “needle in a haystack” with Forensic Data Analytics

While vast amounts of data can deliver deep insights, sheer volume can cause problems for businesses seeking to identify suspicious activity that could constitute compliance risk—particularly when dealing with historical transactions. This is where Forensic Data Analytics (FDA) comes into its own.

Data scientists use FDA and build algorithms to rigorously mine transactional data and discover patterns that indicate issues such as money laundering and fraud. Given enough historical data, they can model, quantify and forecast risk, helping companies move toward the prescriptive analytics stage where they can put measures in place to protect their business and prevent fraud.

A further application for FDA is in highlighting data privacy compliance risk by identifying where data is stored across the business, how it is managed and who has access to it. This is particularly valuable in light of the GDPR and other data privacy laws such as the California Consumer Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA).

FDA can be applied across all areas of business risk and compliance to identify gaps in governance and compliance controls and help companies achieve greater transparency.

Identifying and managing risk in the supply chain

Supply chain integrity and resilience is a major challenge for today's organisations. Supply chains have become more complex, multinational, and spread across multiple jurisdictions. They are exposed to multiple risks—from operational, compliance and reputational risks to physical and cyber security hazards. Managing beyond Tier 1 risk is a considerable undertaking in which insights gained from big data analysis are the key to proactive management and improvement in supply chain transparency, sustainability and resilience.

MINIMIZING SUPPLY CHAIN DISRUPTION RISK

Digitisation and the rise of the Internet of Things (IoT) has made supply chain management a far more accurate and responsive activity as businesses can now integrate real-time information about factors such as weather conditions, transport logistics and stock inventories with insights gained from predictive analytics that anticipate shifts in customer demand and the future availability of raw materials. This allows companies to see risks earlier and respond more quickly, cutting reaction times from weeks to just minutes.

In a world where incidents such as extreme weather events, for example, are becoming more frequent, the ability to predict and react to changing situations with an intelligence-led strategy is a considerable commercial advantage.

ASSESSING AND IMPROVING ENVIRONMENTAL AND SOCIAL GOVERNANCE

Monitoring partner performance in areas of environmental and social governance (ESG) can be achieved through analysis of datasets from global news sources, social media posts, regulatory agencies and public company information to gain an objective perspective on risks and achievements.

The insights gained from this analysis can be used to inform partner selection and as a lever in partner management to improve supply chain transparency and support businesses in their efforts to continuously improve ESG performance.

CASE IN POINT:

Bechtel

Human trafficking and modern-day slavery (MDS) affect an estimated 40.3 million people worldwide; 25 million of those are subject to forced labor. Businesses have an ethical and legal responsibility to eradicate forced labor from their supply chains but achieving visibility across multiple partners and territories poses a significant challenge.

As part of its commitment to contribute 100 ideas towards realising the UN's 2030 Sustainable Development Goals, engineering company Bechtel used big data analysis to build an objective understanding of the risk of MDS in different industries. Text analysis of millions of public data sources and unstructured business information tracked mentions relating to MDS practices associated with, for example, the Oil and Gas sector.

The analysis shows a high likelihood of MDS becoming a key human rights issue for the sector in coming years. In the margins of the data they also uncovered a plausible link between MDS and oil price variability, which may encourage suppliers to cut corners, including using illegal labor.

GAINING VISIBILITY OF THIRD-PARTY CYBER SECURITY RISK

The data generated, stored and managed by businesses creates significant compliance, reputational and financial risk.

A critical aspect of data privacy is its symbiotic relationship with cyber security. Section 32 of the GDPR states organisations must demonstrate they are "processing personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."[9]

This means companies need to be confident not only of their own cyber security, but also that of third-party providers or subsidiary organisations that are connected to their digital ecosystem. This is particularly important given the growing prevalence of the cyber-crime tactic of "island hopping" where cyber criminals make a breach in a vendor company and use its access privileges to infiltrate the network of their ultimate target.

Historically compliance has been achieved through point-in-time screening via questionnaires and interviews, as part of supplier contracts. However, the speed at which a business' cyber defence posture can change as a result of emerging threats means this is no longer a sufficient process. Companies need to understand their cyber risk exposure in real time through continuous assessment of third-party performance throughout the supply chain.

In fact, Gartner predicts that by 2020, 100 percent of large enterprises—compared to only 40 percent in 2018—will be expected to report on cybersecurity and technology risk to their Board of Directors.[10]

Big data is helping to achieve this through security ratings services—tools that analyse objective, comprehensive cyber security data and build an independent picture of an organisation's performance.

Businesses can continuously monitor this picture over time to inform decisions about the level of access that partner has to critical systems and data. Any major change in the organisation's posture, as the result of a new vulnerability or emerging threat, is visible to partners, who can adjust accordingly. This is particularly valuable in mergers and acquisitions, where cyber due diligence is becoming as critical as financial and legal due diligence in understanding the risks associated with the transaction.

MAKING BIG DATA WORK FOR YOUR ORGANISATION

The volume and complexity of business risk in today's digital corporate environment goes far beyond manual management. To gain the most effective knowledge needed to navigate compliance, supply chain and security risks, big data and AI-powered data analytics are a crucial tool, offering significant benefits.

As it gains currency in organisations, big data is revolutionising risk management by making it more nuanced, comprehensive and effective, as businesses are operating from a far stronger position of knowledge. This enables them to proactively manage and mitigate risk, identify future areas of concern using predictive analytics, and use risk appetite strategically to achieve business objectives.

The primary risk in big data analysis itself lies in poor data quality and difficulties in integrating disparate internal and external datasets to gain the complete picture. However, as its application in risk management increases and technologies evolve, we are likely to see businesses prioritising data integrity to improve performance.

Learn how organisations can benefit from Nexis® Data as a Service or our risk mitigation technologies to enhance visibility into potential third-party risk.

For More Information

internationalsales.lexisnexis.com · information@lexisnexis.com +31 20 485 3456

About Nexis® Solutions

Nexis Solutions, a division of LexisNexis, is dedicated to developing innovative tools to support data-driven decision-making. Our commitment extends beyond comprehensive content and outstanding search technology to world-class client service support, ensuring that our clients gain maximum insights and value from our solutions.

LexisNexis®

[1] Wagner, Daniel and Disparte, Dante. *Global Risk Agility and Decision Making*. Palgrave Macmillan. 2016. Accessed at: http://bit.ly/2GJF24Q

[2] "What is Risk Management?" Institute of Risk Management. 2019. Accessed at: http://bit.ly/2MEpFOW

[3] "Uncertain Regulatory and Economic Climate Tops List of Corporate Directors' Concerns for 2019," National Association of Corporate Directors (NACD) Public Company Governance Survey. December 6, 2018. Accessed at: http://bit.ly/2yCT17T

[4] IBID

[5] "How Big Data Analytics is Transforming Regulatory Compliance," Credit Suisse. November 30, 2017. Accessed at: http://bit.ly/2Yp8hV7

[6] "The robots are ready. Are You?" 2017 Deloitte Global Robotic Process Automation Survey. 2018. Accessed at: http://bit.ly/31kbylP

[7] "How Robotics Can Drive Compliance Modernization in Financial Services," *WSJ Risk & Compliance Journal*. June 15, 2018. Accessed at: http://bit.ly/2YMnAGO

[8] IBID

[9] "Guide to the General Data Protection Regulation," Information Commissioner's Office. Accessed August 4, 2019 at: http://bit.ly/33bJJOc

[10] "Digital Business Requires Cybersecurity," Gartner. 2018. Accessed at: https://gtnr.it/2OEyz1a