CENTRE FOR FINANCIAL REGULATION AND INNOVATION

Literature review

Examining the Impact of Artificial Intelligence on the Evaluation of Banking Risk

George Daniel Brown Swankie[1] | **Daniel Broby**[1]*

[1]Strathclyde Business School, Glasgow, Scotland

Correspondence
Daniel Broby (Director).
Strathclyde Business School, Stenhouse Wing, 199 Catherderal Street, Glasgow G4 0QU
Email: daniel.broby@strath.ac.uk; george.swankie.2013@uni.strath.ac.uk

Funding information
The University of Strathclyde is a leading international technological university that has made *Fintech* one of its strategic clusters.

This paper examines the relationship between Artificial Intelligence (AI) and banking risk management. The global financial crisis highlighted their importance and now banks are subject to more stringent regulation regarding their capital adequacy. Meanwhile, advances in technology are driving changes in the way banks operate. AI is at the core of this and has the potential to revolutionise financial services. It is comprised of several techniques that allow computers to mimic human behaviour and analyse vast quantities of data in seconds. These techniques include machine learning, deep learning, speech recognition, natural language processing and visual recognition. We investigate the extent to which each of these techniques can be implemented in the context of financial services. In this respect, we look at credit, operational, liquidity and reputational risk, all of which can have a negative impact on the earnings of an organisation. AI has the potential to help mitigate these risks in banks and address some of the highlighted management issues. We conclude that the application of AI can add significant economic value to banking operations.

KEYWORDS
Banking, Regtech, Fintech, Regulatory models, Financial Services, Disruption, Artificial Intelligence, Risk, Regulation Reporting.

Abbreviations: AI - Artifical Intelligence

*Director, Centre for Financial Regulation and Innovation

1 | INTRODUCTION

The axiomatic importance of bank risk management was highlighted by the 2008 global financial crisis (GFC). The economic and financial calamity that followed the GFC was primarily due to banks exhibiting a complete disregard to risk management in the years leading up to 2008 (Ellul Yerramilli, 2013). The pernicious effect of the GFC was experienced across all business sectors and in virtually every economy (Bekaert, Ehrmann, Fratzscher Mehl, 2014), with subsequent government support reaching unprecedented levels (Miles, Yang Marcheggiano, 2012). To combat the failings and shortcomings that were revealed in the financial services sector, significant regulatory changes have since been implemented which have resulted in changes to the culture and structure of banks. As well as regulatory changes, there has been substantial debate on the issue of bank governance and the risk culture of banks in an effort to prevent the re-occurrence of the events preceding 2008 (Srivastav Hagendorff, 2015).

Technology innovation has also increased dramatically in recent years and has resulted in a change in the way banking business operates. This pace of change will continue and gather momentum. Companies will have to adapt to the changes and alter their processes in order to remain competitive. As a result, risks for banks are changing, existing risks are evolving, and new risks are being identified as business processes change.

Artificial Intelligence (AI) as an example of technological innovation has many benefits for the banking industry such as the potential to reduce costs and increase competition. Indeed, it can help mitigate certain risk factors however, AI also brings with its introduction, new risks. This paper critically examines AI within the context of the current literature regarding risk management in banks. It further synthesises these studies in the context of how AI has the potential to impact the industry.

2 | RISK MANAGEMENT IN BANKS

From a business perspective, financial risk refers to the uncertainty of outcomes that have adverse consequences on the earnings of a firm (Bessis, 2015). Banks are financial intermediaries that transfer funds between two economic units – units in deficit and units in surplus. These economic units tend to favour using an intermediary because of the information asymmetries that exist between the units/parties. The result is that the risk associated with the transaction is passed to the bank as the intermediary instead of to the individual or party who is the unit of surplus. The risk to the bank is that part (or all) of the investment is lost. This risk refers to the probability that an investment's actual return will differ from its expected return. Managing this risk is a fundamental component of the business model of banks (DeAngelo Stultz, 2015).

Effective risk management is the process of identifying, measuring and monitoring the different sources of risk that a bank faces, e.g. market risk, credit risk and liquidity risk. The process of managing these risks is therefore intrinsic to banking. The concept of risk for a bank however, attracts not only negative ramifications, known as downside risk, but it can also provide an opportunity to enhance value for a bank, known as upside risk (Saunders Cornett, 2014). In order to meet the key goal of maximising shareholder value, a bank must take risks that are expected to be profitable. If too many measures are taken to mitigate risk at the expense of avoiding profitable investments of higher risk, it can ultimately prove costly for shareholders (Stulz, 2015). Thus, the goal of a bank's risk management is not to eliminate risk as might be desired from the perspective of its shareholders, but rather to ascertain the optimal level of risk for the organisation. This will ultimately determine the value that is created for the bank's shareholders.

An important component of a bank's risk management is the risk culture that the bank has in place. The culture of an organisation is very intricate and because it is ingrained throughout the structure of an organisation, it can be

extremely difficult to change (Fahlenbrach, Prilmeier Stulz, 2012). It is a result of behaviour and beliefs, the values shared by employees of the organisation, the strategic decisions and experiences of the organisation together with any underlying assumptions (Galbreath, 2010).

A bank's goal of maximising shareholder value is supported by its attitude and its appetite towards risk. An example of defective risk culture was the irresponsible incentive structure for bank employees whose widespread practice played a role in the GFC. Sales/profit targets were central to the salaries and bonuses that many bank employees received at the time and these targets did not take into consideration the quality of the sales/loans that were being supplied. Research conducted following the GFC found that profitable banks in the lead up to 2008 were the most likely to take greater risks (Weiß, Bostandzic Neumann, 2014). Prior to the GFC, there were a number of cases where individuals had conducted fraudulent activity to help exceed their targets, e.g. Jérôme Kerviel at Société Générale who lost the bank a total of 4.9 billion (Anderson, 2013). This case demonstrated the failings of a weak risk culture and poor control mechanisms. Together they would prove catastrophic for the bank.

A bank's risk culture can help to determine how it is structured and this is particularly relevant now that the UK government has introduced ring-fencing legislation (Cullen, 2018). A key component of a strong risk culture is ensuring that effective, internal communication is in place throughout the organisation so that employees are fully aware of the bank's attitude to risk and its risk parameters. This will ensure that employees can distinguish between which risks are acceptable to the organisation and which are to be avoided.

Another significant component of a bank's risk management is its risk governance (Aebi, Sabato Schmid, 2012). A well-governed bank will have mechanisms in place to identify its optimal level of risk and to make sure that there is not excessive divergence from this figure. These mechanisms will support managers in making important, value maximising, risk/reward trade-offs whilst ensuring that they are complying with all banking regulations (Stulz, 2015).

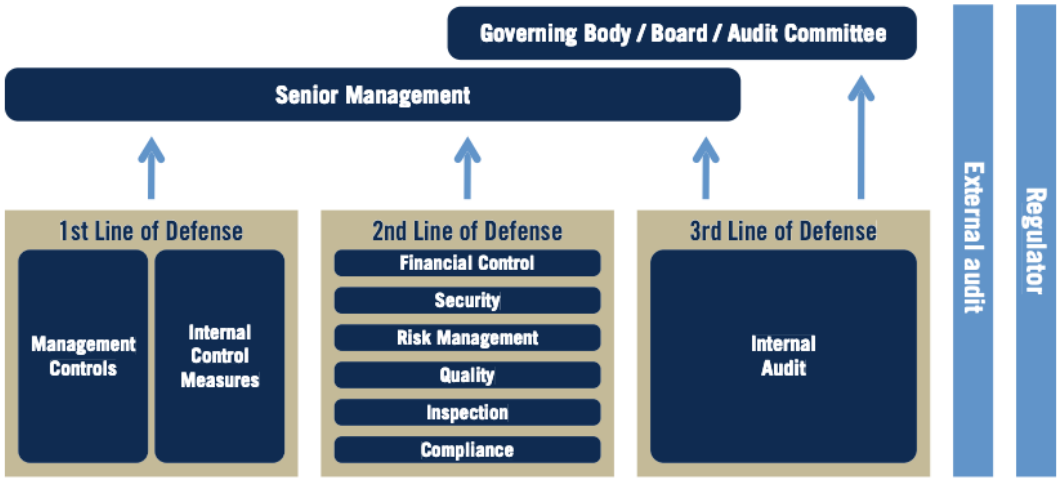
The Chief Risk Officer (CRO) is responsible for risk management across a bank. In order to hold the position of CRO, the individual requires formal approval from the appropriate regulator. The CRO then reports directly as a senior executive to the Board Chairperson and to the Chief Executive Officer (CEO). The CRO will ensure that the bank's risk appetite is reflected in its strategic plan and will regularly communicate and meet with the bank's Board to discuss issues relating to risk (Aebi, Sabato and Schmid, 2012). The CRO is responsible for establishing a risk framework that the bank will use to ascertain and manage the quantitative and qualitative risks which the organisation faces. A common risk governance framework that is often adopted to ensure an optimal structure is known as the 'Three Lines of Defence' model (see Figure 1.1) (Bank for International Settlements [BIS], 2015).

This model is often used by banks to demonstrate the interaction between internal control systems and corporate governance. It is an essential component of a bank's integrated risk management framework and acts as a benchmark, clearly defining and assigning management responsibilities for risk across a bank (BIS, 2015). The model allocates responsibility and ensures that accountability is taken for managing risk.

The first line of defence is addressed by the areas of the bank that generate revenue such as sales, trading and client relationships (BIS, 2015). The model assumes that the employees involved in such business operations on a daily basis are the most appropriate and best equipped to quickly identify potential weaknesses and failings. In theory, line management who are responsible for managing their own processes and control frameworks would be notified by employees expeditiously and appropriate actions would be taken to rectify any risk related issues.

The first line of defence is supported by the second line of defence, which in turn is comprised of supervisory functions. It establishes controls for detection and prevention and then ensures these are integrated into the strategy and framework of the first line of defence. To prove effective, it is vitally important that these oversight functions are independent and are based on transparent risk assessment criteria (BIS, 2015). The Jérôme Kerviel case at Société Générale was an archetypal example of where the second line of defence proved ineffective with deleterious effect

FIGURE 1 An illustration of the 'Three Lines of Defence' model (Institute of Internal Auditors, 2013



(Anderson, 2013).

Internal audit provides the third line of defence which requires objectivity and independence in order for it to be effective. The internal audit function exists to provide independent assurance on a range of matters, including the protection of assets and the efficiency of business operations to both senior management and the Board (BIS, 2015).

Finally, ancillary external audits are executed to augment the internal three lines of defence framework. External audits are of particular importance to banks as the financial sector is subject to stringent review by its regulatory bodies. These audits are important to bank risk governance and control as they confirm that the bank is complying with the rules and standards set by regulatory bodies (BIS, 2015).

Regulation is necessary to protect customers, to reduce crime, to support governments' macroeconomic policies and also to maintain the confidence of investors. However, regulation in itself is not a panacea and despite its existence in the UK, from 2000 onwards the financial services sector had fallen prey to some challenges including the mis-selling of payment protection insurance and endowment policies. This drove a change in the regulatory framework leading to the introduction in 2012 of the Financial Conduct Authority (FCA) and the Prudential Regulatory Authority (PRA), both of which report to the Bank of England (Bank of England, 2012).

The focus of the PRA is to safeguard financial stability by ensuring financial institutions adhere to an appropriate balance between risk and return. A key to enabling such a balance is for banks to hold sufficient levels of capital to act as a buffer against unexpected losses. While each country will have its own prudential regulator there is still a global risk, as the GFC revealed. Hence the need for an internationally agreed standard as created in the Basel framework. This resulted in the launch of the Basel Accord, introduced by the Basel Committee on Banking Supervision (BCBS) (BIS, 2018).

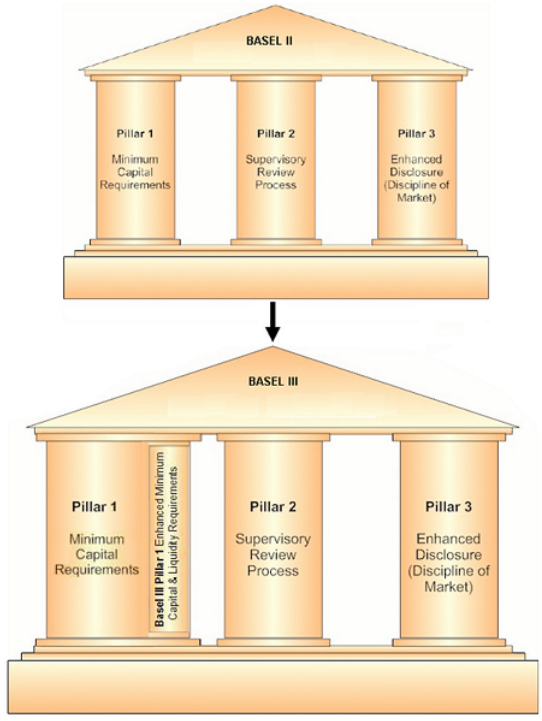
Basel I was launched in 1988 and introduced different levels of bank capital instituting an 8 percent minimum capital condition on banks in accordance with their risk-weighted assets (Arnold, 2014). However, this first Accord was criticised for being overly simplistic on account of two key failings: it gave equal risk weighting to various categories of loans and in terms of the capital requirement, it did not take in to account possible variations in default risk. This allowed banks to circumvent certain elements of Basel 1, misreporting their positions and thereby potentially

increasing their levels of market risk.

To address these shortcomings, Basel II was released in 2004 and introduced a three-pillar framework. Pillar 1 focused on capital requirements and refined the definition of assets adding two more classifications. A further level of capital was also added. Pillar 2 concentrated on the oversight process requiring nation-wide regulatory bodies to evaluate the different risk groups. Pillar 3 required banks to provide a number of disclosures and so increase their transparency in terms of risk. However, Basel II was also subject to criticism and a major weakness was that it was left to the banks themselves to calculate a key risk ratio. This led to some lenders maintaining lower levels of equity than the regulators would consider prudent. The Basel II framework therefore needed to be strengthened to assist banking and financial stability (Acharya and Ryan, 2016).

The Basel III framework was agreed in 2010 to be implemented in phases between 2013 and 2019. It continued with the three pillars of Basel II but sought to enhance the quality and quantity of regulatory capital held by banks by imposing more stringent requirements (see Figure 1.2). It proposed the introduction of a conservation capital buffer as well as a minimum leverage ratio for Tier 1 capital. To address the liquidity issues of Basel II, it is now mandatory for banks to sustain a high liquidity coverage ratio (LCR). In addition, it was proposed banks adhere to a Net Stable Funding Ratio (NSFR). Basel III received criticism because of the significant increase required in data reporting. The cost of achieving this together with the complexity could prove challenging for some banks. Furthermore, certain banks have also voiced concern with regard to using the LCR, viewing it as too simplistic.

FIGURE 2 Basel II to Basel III (IBM, 2018)



The banking industry continues to evolve, and technology is giving rise to new and unforeseen risks. Going

forward, these will be issues which Basel IV will need to address.

3 | ARTIFICIAL INTELLIGENCE

AI is not a new phenomenon, the concept having been introduced in 1955 (Chishti and Puschmann, 2018). AI is defined as being the theory and development of computer systems which exhibit characteristics normally associated with human intelligence. The primary scientific goal of AI is to better understand the components that enable intelligent behaviour in humans to then enhance human-machine systems (Tecuci, 2011).

There are three primary types of AI that are presently acknowledged: current/narrow AI (non-biological intelligence), artificial general intelligence (the ability to complete any cognitive task as well as a human) and superintelligence (general intelligence that far exceeds the levels experienced in humans). Despite the fast pace of technological change, artificial general intelligence and superintelligence are still beyond the bounds of current technology.

There is an ongoing debate as to when (and even if) artificial general intelligence and super-intelligence will ever be developed. At this stage in its development, AI recognises sequences of words but does not have the ability to interpret such input in relation to real world applications. Examples of tasks that current AI can complete include speech recognition, learning under uncertainty, decision making and visual perception (Tegmark, 2017). AI comprises a number of different techniques that allow it to mimic human behaviour. Some of the most relevant at this time in the context of financial services include machine learning, deep learning, speech recognition and natural language processing as well as visual recognition (Deloitte, 2018).

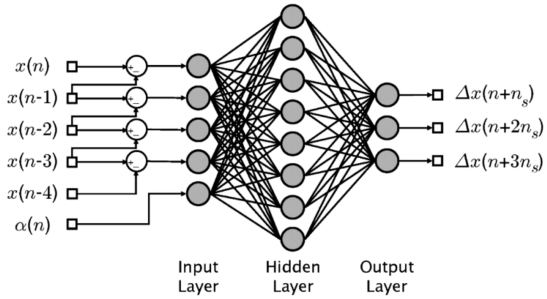
Machine learning involves computers having the ability to acquire their own knowledge by extracting patterns from data using algorithms (Côté, 2018). It emanates from a division of computational algorithms that is fast developing, drawing upon and using concepts from numerous areas including control theory, information theory and probability and statistics (Naqa et al., 2018).

Machine learning algorithms can be divided in to two main categories, unsupervised and supervised learning. Unsupervised learning has three basic components: a dataset, a model and a cost function. It is used primarily to develop an understanding of the inherent structure of a dataset but without any reference to labels. Supervised learning incorporates all of the components of unsupervised learning with a key difference that the data is labelled. Supervised learning is primarily used to aid in classification and has the ability to measure accuracy in a reliable way (Côté, 2018). Machine learning is a branch of AI that has been successfully adopted in a number of areas, including medicine (Cleophas Zwinderman, 2013), spacecraft engineering (Ao, Rieger Amouzegar, 2010) and finance (Gyōrfi, Ottucsák Walk, 2012).

Deep learning is a type of machine learning that is based on artificial neural networks (Tran Garcez, 2018). A neural network is a group of interconnected neurons that are able influence the behaviour that each network or neuron performs (Tegmark, 2017). At its most basic level, a neural network is a collection of nodes that are divided in to three separate functions: the input layer, the hidden layer which determines the model by applying an algorithm and the output layer (see Figure 1.3). The computational algorithms that deep learning utilises are effective for model prediction and learning data representation. The latter allows the computer to develop intricate theories based on relatively basic concepts (Goodfellow, Bengio and Courville, 2017).

Two other components of AI are speech recognition and natural language processing. Speech recognition is the process of making a computer understand human speech (Stephenson, Doss Bourlard, 2004). Much like deep learning, speech recognition utilises neural networks, specifically recurrent neural networks (RNNs) as the model for prediction. RNNs store sequential information in their memory, using this information to predict future outcomes. This

FIGURE 3 Illustration of a neural network (Najmaei and Kermani, 2010)



technology is used to interpret human speech and then transform the speech in to a text format. Natural language processing is a type of speech recognition where a machine processes human language with the aim of being able to understand and communicate with humans using a familiar language (Pattern Jacobs, 1994). It involves the application of computational techniques to analyse large volumes of language data as well as synthesising human language and speech.

Visual recognition uses deep learning, specifically convolutional neural networks (CNN) to analyse images and scenarios for faces and objects. The CNN neurons are arranged in a three-dimensional topological structure. These neurons analyse a specific area of an image or a scenario, breaking the area down to a set of information (Nebauer, 1998). The CNN then combine these sets of information amalgamating them to generate an accurate depiction of the image. Following the amalgamation, the CNN can make a prediction as to what the image or scenario is. An example of where a computer applies this prediction is when facial recognition is used to unlock a phone. A key issue for visual recognition is its high degree of variability which can impact its effectiveness. As the technology advances, it is crucial that it not only identifies the image, but that it also verifies the image has been correctly distinguished (Wang, Hu and Deng, 2017).

3.1 | Uses in non banking industries

AI has a wide range of applications and is currently being used in a number of industries. The degree to which it has been introduced and applied varies, but industries such as transportation, healthcare, manufacturing and finance are all being affected by AI technology (Quan and Sanderson, 2018). The potential applications for this technology are the subject of much debate. However, AI has already had a significant impact on a number of industries, revolutionising how they operate.

- In manufacturing, AI has begun to control robotics, which has resulted in significant improvements in precision and efficiency causing a change in the operations and processes of manufacturing companies.
- In transportation the use of AI is developing at a fast pace with research stating that as the majority of current accidents are a result of human error AI will reduce the number of road fatalities moving forward (Tegmark, 2017). Advancements in self driving cars have the potential to completely transform the transportation industry (Jones, 2017).
- In the communication industry AI has also been widely used. Services such as Google Translate, and Siri offered by Apple Inc. are now used around the world bringing significant benefits. A further area forecast to benefit from

AI is the healthcare industry.

Due to advances in deep learning, research predicts that AI could become more accurate at making certain diagnosis than doctors (Tegmark, 2017). This view was supported by research from Ardila and colleagues (2019) who ascertained that an AI system performed as well as human radiologists in identifying lung cancer. In addition, research has also suggested that as AI technology advances, it may become more reliable in conducting surgeries using robotics rather than human surgeons (Tegmark, 2017).

The financial services sector has also benefited from AI which has been incorporated in to operations with the goal of improving efficiency, providing greater levels of automation as well as reducing human error. AI has commonly been applied in areas such as wealth management, e.g. robo advisory services (Chishti Puschmann, 2018) as well as in high frequency trading, e.g. algorithmic trading (Chaboud et al., 2014). One area in this sector which may further benefit from use of AI is risk management. This will now be examined in the next section of the report.

4 | ARTIFICIAL INTELLIGENCE APPLIED TO RISK MANAGEMENT IN BANKS

The emergence of financial technology (FinTech) has seen a surge in interest and comment with regard to how AI might be developed and incorporated to better serve more traditional financial services and operations (Zhang and Kedmey, 2018). While wealth management and investment banking profit from the use of AI there is a paucity of research regarding the impact and potential impact AI has and could have on bank risk management. This is an area that merits closer examination and research.

As mentioned previously, banks are subject to a number of risks and successful risk management involves ensuring that these risks are appropriately identified, measured and monitored. Some of the main financial risks include credit risk, liquidity risk, reputational risk and operational risk. This section will review existing literature and critically discuss how AI can be applied in the identification, measurement and monitoring process for each of these risks.

4.1 | Credit Risk

One of the main activities of a bank is lending money to customers. This carries adherent risk as it is not guaranteed that the customer will repay the bank. Credit risk is the probability that the bank will experience an economic loss as a result of a customer not meeting their contractual obligation or failing to repay a loan supplied by the bank. Credit risk can also comprise a deterioration in a counterparty's creditworthiness (Horcher, 2005). It is one of the most significant risks a bank faces and is a difficult challenge to address (Angelini, Tollo and Roli, 2008).

Credit risk is recognised by the Basel regulation which requires banks to hold capital reserves against credit risk (Stulz, 2015). The practices that are in place to manage credit risk differ between banks, depending on the complexity and types of credit activities in which they are involved. In order to effectively model the calculation for credit risk, the probability of default (PD), the exposure at default (EAD) and the loss given default (LGD) must be estimated. The identification and measurement of each of these three drivers of credit risk are crucial for the success of a bank.

Credit risk is quantified by assessing two fundamental parameters, expected loss and unexpected loss. Expected loss is built into the bank's initial evaluation and is covered by the reserves that the bank holds. Therefore, it does not represent the actual risk for the bank and is calculated using the following formula: Expected Loss = PD x EAD x LGD (Saunders Cornett, 2014). Unexpected loss is the volatility of the actual loss rates in relation to the expected loss. It represents the risk that the financial loss is greater than what was initially expected and so is the actual risk for a bank.

Standard deviation is the most widely used metric to measure unexpected loss. (Saunders and Cornett, 2014).

The most commonly used, traditional method to quantify credit risk is multiple discriminant credit score analysis which was developed by Edward Altman (Altman, 1968). Given this method is still in use today, AI has the potential to develop the process and so improve the way a bank quantifies credit risk. Traditional, multiple discriminant analysis (MDA) identifies financial variables that act as parameters and that have the potential to differentiate between individuals/companies that are deemed "good" and "bad" in terms of repaying loans.

The main objective of credit scoring models is to assess the risk profile of an individual/company and then to assign a credit risk score dependent on the probability of default (Blöchlinger and Leippold, 2006). Depending on the model employed, the output score can be used to assign individuals/companies to a specific group ('good' or 'bad') or to allocate a numerical score that represents the probability of default. In order to effectively analyse how AI can affect this method of quantifying credit risk, a brief overview of the different MDA methods used to measure is required.

There are three primary MDA methods that are used to measure credit risk. These are the linear probability model, the logit (logistical regression) model and the linear discriminant model. However, these models all have statistical restrictions that can affect their accuracy. The linear probability model is based upon historical data relating to past loan repayments the individual has made. From this data, predictions are then made with regard to repayment probabilities on future loans. This model divides loans into two groups, those that had defaulted ('bad' loans = 1) and those that had not defaulted ('good' loans = 0). The assumption that the variables are binary (or dichotomous) is a shortcoming of this model as individuals may have a probability of default that is out with the interval of 0 or 1. The logit model confronts this shortcoming by using an exponential transformation where the results of the regression can lie between 0 and 1.

The linear discriminant model separates low and high-risk default classifications based on their observed properties. It utilises historical data to predict whether a loan falls in to the low or high risk default class. The Altman Z-score uses the information derived from the linear discriminant model to quantify the credit strength of a publicly traded company. In doing so it predicts the probability that a company will go bankrupt in the next two years. The Altman Z-score model is based on five financial ratios (Altman, 1968).

There are a number of issues associated with the current methodologies used to measure credit risk which AI could help alleviate. These include difficulties in combining and analysing qualitative and quantitative data measures as well as quantifying the total credit risk evident at bank portfolio level. The Altman Z-score model takes only five financial ratios into consideration. However, using AI technology, big data would be analysed using a much greater range of sources than would be possible using the traditional MDA. This in-depth analysis could then be combined with the customers' credit history resulting in the provision of greater insights and more reliable decisions than those possible from a human analyst.

AI allows banks to examine significant quantities of qualitative and quantitative customer data. In doing so it would address the shortcoming of the traditional MDA models which do not take into consideration qualitative information (Saunders and Cornett, 2014). This is supported by literature which suggests that artificial neural networks make more accurate classifications when compared to the traditional methods of quantifying credit risk (Yeh and Lien, 2009).

The incorporation of AI to help measure credit risk could significantly reduce the loans that a bank supplies to individuals that have a high chance of default, thus providing the bank with considerable cost savings. However, AI is still at a stage whereby it cannot definitively interpret qualitative information. The ability to emulate human conscious reasoning, something that is critical to understanding qualitative information, remains a shortcoming of AI technology (Hopgood, 2003). This challenge has received some focus in recent years with greater attention in research and development having been placed on emotional intelligence. This together with more data becoming available to interrogate has allowed AI technology to develop (Cabrera et al., 2018). However, new issues have arisen in terms of

the available data differing in regard to its structure and complexity (Quan and Sanderson, 2018). This ongoing cycle of data becoming ever more complex is one of the main challenges that banks/organisations face in terms of how to use AI safely and effectively.

A key issue for banks is the availability, the quality and the cost of obtaining information to effectively identify, measure and monitor credit risk using the methods discussed above. This proves a challenge for the introduction of AI. It has the potential to analyse large amounts of data through its big data algorithms (the latest semiconductor chips produced by Intel for AI can run over 10 trillion calculations a second (Quan and Sanderson, 2018)). However, AI requires high quality data in order to develop and predict accurate outcomes. If the information provided to the AI system is substandard, the output of the computational algorithms may be inappropriate. Given AI solutions can learn and evolve rapidly, if there is insufficient data it could result in a high rate of errors on a large scale.

4.2 | Operational Risk

Operational risk refers to possible loss emanating from failures in internal control, operational, and accounting systems; failure of procedures and processes; and failure of personal oversight functions, relating to fraudulent activity and human error (Brown, Goetzmann, Liang and Schwarz, 2008). This is a serious risk for a bank as it encompasses a number of different elements, all of which can result in significant loss should they occur.

The methodology involved with identifying, measuring and monitoring operational risk should align with the operational risk rules that were set originally as part of the Basel II framework (Guill, 2016), but which have since been subsequently revised. The BCBS has developed a standardised measurement approach (SMA) for operational risk. This single method approach combines the business indicator (BI), a representation of operational risk exposure, with the internal loss multiplier, a risk-sensitive component of operational loss data that is specific to the bank (BIS, 2016). The BI consists of three elements:

1. the interest, dividend and lease component;
2. the services component; and
3. the financial component.

Each of these components is calculated as an average over a time period of three years (BIS, 2016). Prior to the SMA's introduction, there was no numerical proxy for the measurement of operational risk, which made it challenging to quantify (Brown, Goetzmann, Liang and Schwarz, 2008). The SMA placed an increased focus on data analytics as part of the modelling process and so allowed a greater quantitative basis to be in place when assessing operational risk.

One area of operational risk that AI could have a significant impact upon is the identification of fraudulent activity. Delays in the detection of fraudulent activity have been shown to lead to considerable resource reallocation (Yu Yu, 2011). Research has shown that AI allows banks to ascertain in real-time if a loan application is likely to be fraudulent (Linthicum, 2017). JP Morgan Chase Co has estimated that using AI to review its credit applications has brought them an annual saving of some USD150 million in terms of benefits and efficiencies. Furthermore, the organisation has approved one million additional loans which would previously have been declined for suspected fraud and has declined an additional one million loans which would have previously been approved (JP Morgan Chase Co, 2018).

It is worth stating that certain research has found that statistical techniques are more accurate at detecting less complex fraudulent activity (that is in a simple structure) than AI (Duhart and Hernández-Gress, 2016). Credit card fraud is a common concern and a significant cost for many banks. Due to the speed at which credit card fraud can

occur following loss of a card, the importance of early, intelligent fraud detection methods is paramount.

When the vast quantity of transactions that are carried out each day is considered, a major challenge for banks is to analyse and identify those which raise suspicion. Identifying inconsistent credit card spending patterns that are not in line with the spending behaviours of individual customers is extremely complex. Research conducted by Sudjianto and colleagues (2010) has shown that AI is effective at utilising clustering algorithms to better identify suspicious spending patterns and identify individuals that are working together to commit fraudulent activity.

AI is not yet able to interpret information in relation to its impact on real world events and at this time is only able to identify patterns in the data that is provided to it (Tegmark, 2017). The research while valid, only highlights this fundamental shortcoming. As the literature proposes, further research is required to address the shortcomings of AI in measuring operational risk (Chen Wen, 2010).

A significant contribution to operational risk arises from human error and this is an area which AI has the potential to address in a variety of ways. Research stated that 80 percent of loan servicing errors arose as a result of contract interpretation errors (JP Morgan Chase and Co, 2016). Banks have now used technological advancements to address this issue. JP Morgan Chase and Co have introduced a contract intelligence platform, known as COIN (2016). This platform, using machine learning technology, allows for 12,000 credit agreements per year to be analysed and the pertinent information to be extracted in a matter of seconds. Without this automated AI technology, this would have taken approximately 360,000 hours of work (JP Morgan Chase and Co, 2016).

The errors associated with human intervention have been significantly reduced, providing a more comprehensive analysis whilst also making the process significantly more efficient. The employment of virtual assistants (robots driven by AI) is now common and these are used to handle web site enquiries, maintain help desks and route enquiries. These together with other AI, which reduce human involvement, raises an important consideration which is the potential loss of human jobs as areas of risk management become automated. Morris and colleagues (2017) stated that a number of jobs could be displaced due to the use of AI. However, the research also concluded that a number of jobs could be created as a result of the technology.

Society will increase its demand for data scientists and individuals who have specific skills relating to AI (Morris, Schlenoff and Srinivasan, 2017). This could help to counteract the issue of job losses. However, the number of individuals with the desired skill sets are disproportionate to the number of jobs that will become available (Morris, Schlenoff and Srinivasan, 2017). This will become a challenge for society impacting our education, training and recruitment practices. In the future, responsible companies will need to retrain or redeploy their employees for other roles (JP Morgan Chase and Co, 2018). Significantly reducing employee numbers could have adverse consequences for banks should there be an unexpected failure in technology as the necessary expertise and skills may be lost. The loss could also impact development of the next generation of leadership (Deloitte, 2018).

It is in the area of operational risk that AI perhaps has the greatest opportunity to drive benefit for banks both in terms of reducing costs (man hours and fraud) as well as increasing the scalability of banks' operations.

4.3 | Liquidity Risk

A key focus for banks is to ensure that they have adequate levels of liquidity to meet loan demands and withdrawals from depositors. This is crucial for banks to meet their short-term financial obligations as well as for their survival. The ramifications of having low levels of liquidity are severe and can ultimately result in bank insolvency (Horcher, 2005). The Basel III framework has concentrated attention on liquidity, and insists that banks adhere to regulation guidelines, having sufficient liquid assets to meet their cash requirements (Bai, Krishnamurthy and Weymuller, 2017). Thus, the measurement, monitoring and assessment of liquidity risk is extremely important to a bank.

Following the GFC, the Basel III framework was revisited, and two additional quantitative ratios were proposed to help improve liquidity risk measures. The LCR is in effect a stress test used to ensure a bank has a sufficient quantity of highly liquid assets to meet any ongoing short-term demands made of the organisation over a 30-day period. The LCR should be at least 100 percent. The second quantitative measure proposed by the BCBS was the NSFR. The main objective of the NSFR is to promote medium and long-term liquidity funding for banks who would be required to hold sufficient sources of stable funding to survive a one-year period of stress. However, this metric has its limitations, with research suggesting that the ranking of assets based on this measure is equivocal (Tavana, Abahi, Caprio and Poortarigh, 2018). The NSFR is also required to be at least 100 percent.

Complementing the LCR and NSFR are two primary metrics currently used to ensure that banks maintain adequate levels of liquidity. These are the internal liquidity adequacy assessment rules (ILAA) and the overall liquidity adequacy rule (OLAR) (Bank of England, 2015). The ILAA rules require that banks measure, manage and monitor their liquidity risks in accordance with the bank's risk appetite as articulated by the bank's executive. These rules are in place to ensure a bank assesses its liquidity requirements across a number of different stress scenarios and does so on a regular basis using the internal liquidity adequacy assessment process (ILAAP). The OLAR demands that each bank maintains sufficient liquid resources including buffers which are appropriate both in terms of amount and quality to meet any liabilities as they fall due. This rule is in place to ensure that each bank has an adequate level of liquid assets in place at all times to meet its obligations (Bank of England, 2015).

A key task involved in liquidity management is cash flow forecasting. The analytical power of AI means that it would be able to identify and predict future potential outcomes arising from existing transaction data which would impact the liquidity levels of a bank. Then should these outcomes occur, AI could trigger automated response protocols to help address such events (Deloitte, 2018). AI thus has the potential to eliminate the manual processes associated with the measurement and management of liquidity risk.

The current forecasting methodology used to a great extent human judgement and intuition based on the experience of individuals. If AI can replace this, it would change the way that liquidity forecasts are made. There is a gap in the literature regarding the use of AI to measure liquidity risk (Tavana, Abahi, Caprioa and Poortarigh, 2018). However, it has been shown that the application of AI, specifically artificial neural networks (ANNs), is capable of distinguishing the most pronounced risk factors and making consistent approximations of liquidity risk (Tavana, Abahi, Caprio and Poortarigh, 2018).

The lack of research is a restriction which makes it difficult to discuss AI's effectiveness in this area. However, the research conducted by Tavana and colleagues (2018) suggests that AI has the potential to not only result in cost and effort savings from an operational standpoint, but also to enhance the level of automation and potentially help optimise the liquidity management process.

4.4 | Reputational Risk

The reputation of a bank is linked to the perceived financial strength of the organisation (Fernando, Gatchev, May Megginson, 2015). Reputational risk refers to the risk of negative publicity impacting the reputation or brand of an organisation to the detriment of its economic wellbeing (BCBS, 2009). Research has shown that the probability of reputational damage rises as the size and profits of a bank increases (Fiordelisi, Soana Schwizer, 2013). The attention placed on reputational risk has grown over the past two decades due primarily to the incidence of operating losses caused by internal fraud in a number of banks and the consequent adverse financial impact this has provoked (Dyck, Morse and Zingales, 2010).

In terms of measuring reputational risk a number of studies have applied ordered logit models (formula shown in

Appendix Five) (Efendi, Srivastava and Swanson, 2007; Roberts and Sufi, 2009). The main issue with using ordered logit models is that they make a parallel odds assumption. The models assume that the factors impacting reputational risk exhibit an equi-proportionate effect on the probability that the resultant impact is either a reputational gain or loss. Research has deemed this form of measurement to be inappropriate when trying to determine the causes of reputational risk (Fiordelisi, Soana and Schwizer, 2013). A more flexible approach that is not based upon such a rigid assumption, and one that analyses more factors, such as an approach using AI could be of significant benefit to a bank in identifying, measuring and monitoring sources of reputational risk.

While the introduction of AI in a bank can have many benefits, it can also have a negative impact on the reputation of a bank. AI technology would be analysing large amounts of very sensitive customer data including employment, health care and credit history before making financial decisions based on this information. AI identifies patterns in the data available to them and machine learning algorithms which are part of the AI framework then codify this data to make predictions and decisions. If an existing bias is or becomes evident in these patterns, the algorithms will amplify this bias which may subsequently culminate in the production of erroneous and/or inappropriate results (Wong and Wang, 2003).

A major concern for banks is the potential to seriously damage the reputation of an organisation. The lack of transparency in terms of the data analysis could result in societal retaliation. In addition, the opacity associated with the data when using AI technology could provide challenges with current regulation. The stringent General Data Protection Regulation (GDPR) that is in place in Europe for example requires organisations to explain to customers how their personal data is being used. Compliance with this will be a challenge for AI going forward.

With over 2.5 billion users of social media worldwide, communication via social media platforms is a key source of reputational risk for an organisation. Many individuals regularly use social media as a method to communicate with banks, publicly posting questions, comments and complaints online (Preece et al., 2017). The content of such posts has the potential to impact the reputation of a bank. The ability to identify posts on social media which have the potential to either negatively or positively impact their reputation is a growing challenge for banks. The application of AI to monitor social media allows extremely large quantities of data to be analysed, providing firms with a valuable insight to help aid decision making and situational understanding (Gao, Barbier and Goolsby, 2011). However, research has also suggested that current AI is less than reliable at distinguishing between genuine complaints and those which are disingenuous. This is a text classification problem caused by social media posts that are intentionally deceitful (Zhou, Shi, Zhang, 2008).

One challenge for a bank in using AI technology to analyse social media would be data privacy. In addition, it would also raise a number of ethical dilemmas and might lead to negative public perceptions and so increase reputational negativity for the organisation. The literature regarding the effectiveness of AI for monitoring social media for potential reputational threats is inconclusive. Further research is required.

5 | THE CHALLENGES

AI has the potential to transform banking and specifically its risk management. However, its progress in this area is not without challenge. A crucial consideration going forward is to ensure that the AI systems incorporated in banks' technologies and practices are secure. This needs to be achieved by ensuring that the technology receives adequate verification, validation, security and control (Tegmark, 2017). Data privacy is a key challenge which compliance with GDPR should help address. Related to the concern of data security is the requirement for AI technology to complete its function to a predetermined standard eliminating, where needed and appropriate, any inherent algorithmic bias.

Providing algorithmic transparency will be necessary but this itself may have unintended consequences (Financial Stability Board, 2017).

Despite the anticipated cost savings, current literature has stated that the introduction and implementation of AI could be a costly intervention (Scherer, 2016). Changes in operational structure would have to be made to align with the new technology, new hardware and software purchased, as well as existing staff retrained or replaced with those who have the necessary skills. While perhaps not such an issue for large financial institutions, it may be more of a barrier for smaller banks leading to an impact on competition.

Understanding the risks and implications associated with further introducing AI into risk management functions is not only a challenge for banks, it is also a major area of concern for supervisors and regulatory bodies. The potential benefits of AI are undeniable and regulators themselves are looking at areas where they might incorporate the technology into their own operations. However, given the potential risks associated with AI technology, the regulators' duty is to ensure that the technology benefits do not disrupt the necessary equilibrium between the protection of bank customers, financial stability and market integrity (Deloitte, 2018).

At this time there are very few regulations that currently address the challenges that could arise from AI (Scherer, 2016). As previously discussed, a key challenge for banks is the recruitment of individuals with the necessary AI related skills (Morris, Schlenoff and Srinivasan, 2017). To address this issue, one possibility presented in the literature involved banks combining AI software and hardware sourced from different companies (Scherer, 2016). However, adopting this outsourcing approach would complicate how the bank manages the risk factors that AI presents. In addition, if the AI technology were to operate from different geographical locations, this may give rise to the requirement for the bank to comply with a number of regulatory bodies from such locations and so lead to undesired complications (Scherer, 2016).

As AI technology advances and banking services become more automated, there will be an increased threat of cybercrime. JP Morgan Chase and Co state that they spend almost USD 600 million per year and have more than 3,000 employees working towards enhancing their cyber security (JP Morgan Chase and Co, 2018). A challenge for those banks seeking to introduce AI will be the increasing demand for data scientists and individuals that have specific AI skills. Indeed, research has indicated that a major concern going forward is the lack of skilled staff that are able to implement this technology (Wilson, Daugherty and Bianzino, 2017). This will raise a number of issues for banks as it may require significant investment in recruitment and training in order to retain and employ staff with the necessary skill set.

6 | CONCLUSION

In conclusion, the management of risk is crucial for the success of banks and for the stability of the financial system. There is little doubt that beyond the major cost reduction impacts of using AI in banking, it has the potential to transform the working environment and add significant business value. Banks such as HSBC (2018) and Barclays (Noonan, 2018) have committed to developing the potential of AI in their risk management functions.

In terms of risk management, the focus on financial risk in the literature examined was biased toward credit risk and operational risk. Much of the discussion was centred on automation of repetitive tasks albeit the results of the recent European elections, the ongoing review of financial regulation and the impact of climate change are all sources of financial risk which will be subject to discussion and debate going forward.

AI is part of the solution but should not be seen as a panacea that will address the shortcomings associated with current risk management. The technology has still to progress and develop before it will be able to effectively measure

and assess qualitative information and then apply this knowledge in real world situations. AI is extremely effective at analysing big data and identifying patterns that exist within datasets. However, when measuring risk, subjective analysis is best at this time combined in tandem with objective analysis.

The human element remains crucial. There are a number of issues which must be addressed before AI will become a central component of the infrastructure of a bank. There are also a number of concerns which need to be addressed before its introduction such as data security and how the technology will be regulated. These concerns together with a lack of familiarity and knowledge of AI may lead to a hesitation in terms of AI's adoption in banks.

Furthermore, there is an ongoing question relating to AI and ethics. This is an area for future study and which may shortly receive more attention given the recent donation of £150 million to Oxford University to fund a new Institute of AI Ethics (Jack, 2019). However, given the fast pace of technological innovation, particularly in the field of AI and the potential impact it will have on a bank's risk management function merits further research.

7 | BIBLIOGRAPHY

Acharya, V.V., and Ryan, S.G., (2016), "Banks' Financial Reporting and Financial System Stability", Journal of Accounting Research, Vol. 54, No. 2, pp. 227-340.

Aebi, V., Sabato, G., and Schmid, M., (2012), "Risk Management, Corporate Governance, and Bank Performance in the Financial Crisis", Journal of Banking and Finance, Vol. 36, No. 12, pp. 3213-3226.

Altman, E.I., (1968), "Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy", The Journal of Finance, Vol. 23, No. 4, pp. 589-609.

Anderson, E., (2013), Business Risk Management: Models and Analysis, 1st Ed, John Wiley and Sons.

Angelini, E., Tollo, G., and Roli, A., (2008), "A Neural Network Approach for Credit Risk Evaluation", The Quarterly Review of Economics and Finance, Vol. 48, No. 4, pp. 733-755.

Ao, S., Rieger, B., and Amouzegar, M.A., (2010), Machine Learning and Systems Engineering, 1st Ed, Springer International Publishing.

Ardila, D., Kiraly, A.P., Bharadwaj, S., Choi, B., Reicher, J.J., Peng, L., Tse, D., Etemadi, M., Ye, W., Corrado, G., Naidich, D.P., and Shetty, S., (2019), "End-to-End Lung Cancer Screening with Three-Dimensional Deep Learning on Low-Dose Chest Computed Tomography", Nature Medicine, Vol. 25, No.1, pp. 954-961.

Arnold, G., (2014), The Financial Times Guide to Banking, 1st Ed, Opus Eris Limited.

Artzner, P., Delbaen, F., Eber, J., and Heath, D., (2001), "Coherent Measures of Risk", Mathematical Finance, Vol. 9, No. 3, pp. 203-228.

Bai, J., Krishnamurthy, A., and Weymuller, C., (2017), "Measuring Liquidity Mismatch in the Banking Sector", The Journal of Finance, Vol. 73, No. 1, pp. 51-93.

Bank of England. (2012). "The Bank of England, Prudential Regulation Authority: The PRA's Approach to Banking Supervision"

Bank of England. (2015). "Supervisory Statement: The PRA's Approach to Supervising Liquidity and Funding Risks"

Bank for International Settlements. (2009). "Enhancements to the Basel II Framework"

Bank for International Settlements. (2015). "The 'Four Lines of Defence Model' for Financial Institutions"

Bank for International Settlements. (2016). "Standardised Measurement Approach for Operational Risk" [online].

Bank for International Settlements. (2018). "History of the Basel Committee"

Bekaert, G., Ehrmann, M., Fratzscher, M., and Mehl, A., (2014), "The Global Financial Crisis and Equity Market Contagion", The Journal of Finance, Vol. 69, No. 6, pp. 2597-2649.

Bessis, J., (2015), Risk Management in Banking, 4th Ed, TJ International Ltd.

Blöchlinger, A., and Leippold, M., (2006), "Economic Benefit of Powerful Credit Scoring", Journal of Banking and Finance, Vol. 30, No. 3, pp. 851-873.

Brown, S., Goetzmann, W., Liang, B., and Schwarz, C., (2008), "Mandatory Disclosure and Operational Risk: Evidence from Hedge Fund Registration", The Journal of Finance, Vol. 63. No. 6, pp. 2785-2815.

Cabrera, D., Cubillos, C., Cubillos, A., Urra, E., and Mellado, R., (2018), "Affective Algorithm for Controlling Emotional Fluctuation of Artificial Investors in Stock Markets", IEEE Access, Vol. 6, No. 1, pp. 7610-7624.

Chaboud, A.P., Chiquoine, B., Hjalmarsson, E., and Vega, C., (2014), "Rise of the Machines: Algorithmic Trading in the Foreign Exchange Market", The Journal of Finance, Vol. 69, No. 5, pp. 2045-2084.

Chen, Q., and Wen, Y., (2010), "A BP-Neural Network Predictor Model for Operational Risk Losses of Commercial Bank", IEEE 2010 Third International Symposium on Information Processing.

Chishti, S., and Puschmann, T., (2018), The Wealthtech Book: The Fintech Handbook for Investors, Entrepreneurs and Finance Visionaries, 1st Ed, TJ International Ltd.

Cleophas, T.J., and Zwinderman, A.H., (2013), Machine Learning in Medicine, 1st Ed, Springer International Publishing.

Côté, D., (2018), "Using Machine Learning in Communication Networks", IEEE/OSA Journal of Optical Communications and Networking, Vol. 10, No. 10, pp. 100-109.

Cullen, J., (2018), "Securitisation, Ring-Fencing, and Housing Bubbles: Financial Stability Implications of UK and EU Bank Reforms", Journal of Financial Regulation, Vol. 4, No. 1, pp. 73-118.

DeAngelo, H., and Stulz, R.M., (2015), "Liquid-Claim Production, Risk Management, and Bank Capital Structure: Why High Leverage is Optimal for Banks", Journal of Financial Economics, Vol. 116, No. 2, pp. 219-236.

Deloitte. (2018). "AI and Risk Management"

Duhart, B.A.M., and Hernández-Gress, N., (2016), "Review of the Principal Indicators and Data Science Techniques Used for the Detection of Financial Fraud and Money Laundering", 2016 International Conference on Computational Science and Computational Intelligence (CSCI).

Dyck, A., Morse, A., and Zingales, L., (2010), "Who Blows the Whistle on Corporate Fraud?", The Journal of Finance, Vol. 65, No. 6, pp. 2213-2253.

Efendi, J., Srivastava, A., and Swanson, E.P., (2007), "Why do Corporate Managers Misstate Financial Statements? The Role of Option Compensation and Other Factors", Journal of Financial Economics, Vol. 85, No. 3, pp. 667-708.

Ellul, A., and Yerramilli, V., (2013), "Stronger Risk Controls, Lower Risk: Evidence from U.S. Bank Holding Companies", The Journal of Finance, Vol. 65, No. 5, pp. 1757-1803.

Fahlenbrach, R., Prilmeier, R., and Stulz, R.M., (2012), "This Time is the Same: Using Bank Performance in 1998 to Explain Bank Performance During the Recent Crisis", The Journal of Finance, Vol. 67, No. 6, pp. 2139–2185.

Fernando, C.S., Gatchev, V.A., May, A.D., and Megginson, W.L., (2015), "The Value of Reputation: Evidence from Equity Underwriting", Journal of Applied Corporate Finance, Vol. 27, No. 3, pp. 96-112.

Fiordelisi, F., Soana, M.G., and Schwizer, P., (2013), "The Determinants of Reputational Risk in the Banking Sector", Journal of Banking Finance, Vol. 37, No. 5, pp. 1359-1371.

Financial Stability Board. (2017). "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications"

Fohlin, C., (2002), "Relationship Banking, Liquidity, and Investment in the German Industrialisation", The Journal of Finance, Vol. 53, No. 5, pp. 1737-1758.

Galbreath, J., (2010), "Drivers of Corporate Social Responsibility: The Role of Formal Strategic Planning and Firm Culture", British Journal of Management, Vol. 21, No. 2, pp. 511-525.

Gao, H., Barbier, G., and Goolsby, R., (2011), "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief", IEEE Intelligent Systems, Vol. 26, No. 3, pp. 10-14.

Goodfellow, I., Bengio, Y., and Courville, A., (2017), Deep Learning, 1st Ed, MIT Press.

Graves, A., Mohamed, A., and Hinton, G., (2013), "Speech Recognition with Deep Recurrent Neural Networks", 2013 IEEE International Conference on Acoustics, Speech and Signal Processing.

Guill, G.D., (2016), "Bankers Trust and the Birth of Modern Risk Management", Journal of Applied Corporate Finance, Vol. 28, No. 1, pp. 19-29.

Gyōrfi, L., Ottucsák, G., and Walk, H., (2012), Machine Learning for Financial Engineering, 8th Ed, Imperial College Press.

Hopgood, A.A., (2003), "Artificial Intelligence: Hype or Reality?", IEEE Computer, Vol. 36, No. 5, pp. 24-28.

Horcher, K., (2005), "Managing Treasury Risks in the Real World", Journal of Corporate Accounting Finance, Vol. 17, No. 1, pp. 23-32.

HSBC. (2018). "HSBS Holdings plc: Annual Report and Accounts 2018".

IBM. (2018). "Basel III Summary"

Institute of Internal Auditors. (2013). "The Three Lines of Defence in Effective Risk Management and Control" [online].

Jack, A., (2019). "Blackstone Boss Hands Oxford Record £150m Gift" [online], Financial Times, June 19, available at https://www.ft.com/content/b0d0bc42-91da-11e9-b7ea-60e35ef678d2 : accessed 22 June 2019.

Jones, L., (2017), "Driverless when and cars: where? [Automotive Autonomous Vehicles]", IEEE Engineering Technology, Vol.12, No. 2, pp. 36-40.

JP Morgan Chase Co. (2016). "Annual Report 2016"

JP Morgan Chase Co. (2018). "Annual Report 2018"

Linthicum, D.S., (2017), "Making Sense of AI in Public Clouds", IEEE Cloud Computing, Vol. 4, No. 6, pp. 70-72.

Miles, D., Yang, J., and Marcheggiano, G., (2012), "Optimal Bank Capital", The Economic Journal, Vol. 123, No. 567, pp. 1-37.

Morris, K.C., Schlenoff, C., and Srinivasan, V., (2017), "Guest Editorial: A Remarkable Resurgence of Artificial Intelligence and its Impact on Automation and Autonomy", IEEE Transactions on Automation Science and Engineering, Vol. 14, No. 2, pp. 407-409.

Najmaei, N., and Kermani, M.R., (2011), "Applications of Artificial Intelligence in Safe Human-Robot Interactions", IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), Vol. 41, No. 2, pp. 448-459.

Naqa, I. E., Ruan, D., Valdes, G., Dekker, A., McNutt, T., Ge, Y., Wu, Q. J., Oh, J. H., Thor, M., Smith, W., Rao, A., Fuller, C., Xiao, Y., Manion, F., Schipper, M., Mayo, C., Moran, J. M., and Haken, R. T., (2018), "Machine Learning and Modelling: Data, Validation, Communication Challenges", Medical Physics: The International Journal of Medical Physics Research and Practice, Vol. 45, No. 10, pp. 834-840.

Nebauer, C., (1998), "Evaluation of Convolutional Neural Networks for Visual Recognition", IEEE Transactions on Neural Networks, Vol. 9, No. 4, pp. 685-696.

Noonan, L., (2018). "Barclays Signs up Artificial Intelligence to Aid Bankers"

Pattern, T., and Jacobs, P., (1994), "Natural-Language Processing", IEEE Expert, Vol. 9, No. 1, pp. 35.

Preece, A., Spasić, I., Evans, K., Rogers, D., Webberley, W., Roberts, C., and Innes, M., (2017), "Sentinel: A Codesigned Platform for Semantic Enrichment of Social Media Streams", IEEE Transactions on Computational Social Systems, Vol. 5, No. 1, pp. 118-131.

Quan, X.I., and Sanderson, J., (2018), "Understanding the Artificial Intelligence Business Ecosystem", IEEE Engineering Management Review, Vol. 46, No. 4, pp. 22-25.

Roberts, M.R., and Sufi, A., (2009), "Renegotiation of Financial Contracts: Evidence from Private Credit Agreements", Journal of Financial Economics, Vol. 93, No. 2, pp. 159-184.

Saunders, A., and Cornett, M.M., (2014), Financial Institutions Management: A Risk Management Approach, 8th Ed, McGraw-Hill Education.

Scherer, M.U., (2016), "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", Harvard Journal of Law Technology, Vol. 29, No. 2, pp. 353-400.

Srivastav, A., and Hagendorff, J., (2015), "Corporate Governance and Bank Risk-Taking", Review of Corporate Governance, Vol. 24, No. 3, pp. 334-345.

Stephenson, T.A., Doss, M.M., and Bourlard, H., (2004), "Speech Recognition with Auxiliary Information", IEEE Transactions on Speech and Audio Processing, Vol. 12, No. 3, pp. 189-203.

Stulz, R.M., (2015)., "Risk-Taking and Risk Management by Banks", Journal of Applied Corporate Finance, Vol. 27, No. 1, pp. 8-18.

Sudjianto, A., Nair, S., Yuan, M., Zhang, A., Kern, D., and Cela-Díaz, F., (2010), "Statistical Methods for Fighting Financial Crimes", Technometrics, Vol. 52, No. 1, pp. 5-19.

Tavana, M., Abtahi, A., Caprio, D., and Poortarigh, M., (2018), "An Artificial Neural Network and Bayesian Network Model for Liquidity Risk Assessment in Banking", Neurocomputing, Vol. 275, No. 1, pp. 2525-2554.

Tecuci, G., (2011), "Artificial Intelligence", WIREs Computational Statistics, Vol. 4, No. 2, pp. 168-180.

Tegmark, M., (2017), Life 3.0: Being Human in the Age of Artificial Intelligence, 1st Ed, Allen Lane.

Tran, S.N., and Garcez, A.S., (2018), "Deep Logic Networks: Inserting and Extracting Knowledge from Deep Belief Networks", IEEE Transactions on Neural Networks and Learning Systems, Vol. 29, No. 2, pp. 246-258

Wang, H., Hu, J., and Deng, W., (2017), "Compressing Fisher Vector for Robust Facial Recognition", IEEE Access, Vol. 5, No. 1, pp. 23157-23165.

Wilson, J.H., Daugherty, P., and Bianzino, N., (2017), "The Jobs that Artificial Intelligence will Create", MIT Sloan Management Review, Vol. 58, No. 4, pp. 14-16.

Weiß, G.N.F., Bostandzic, G., and Neumann, S., (2014), "What Factors Drive Systemic Risk During International Financial Crises?", Journal of Banking Finance, Vol. 41, No. 1, pp. 78-96.

Wong, A.K.C., and Wang, Y., (2003), "Pattern Discovery: A Data Driven Approach to Decision Support", IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), Vol. 33, No. 1, pp. 114-124.

Yeh, I., and Lien, C., (2009), "The Comparisons of Data Mining Techniques for the Predictive Accuracy of Probability of Default of Credit Card Clients", Expert Systems with Applications, Vol. 36, No. 2, pp. 2473-2480.

Yu, F., and Yu, X., (2011), "Corporate Lobbying and Fraud Detection", Journal of Financial and Quantitative Analysis, Vol. 46, No. 6, pp. 1865-1891.

Zhang, X.P.S., and Kedmey, D., (2018), "A Budding Romance: Finance and AI", IEEE MultiMedia, Vol. 25, No. 4, pp. 79-83.

Zhou, L., Shi, Y., and Zhang, D., (2008), "A Statistical Language Modelling Approach to Online Deception Detection", IEEE Transactions on Knowledge and Data Engineering, Vol. 20, No. 8, pp. 1077-1081.