Risks and Threats Arising from the Adoption of Digital Technology in Treasury

Johan von Solms(✉) and Josef Langerman

University of Johannesburg, Johannesburg, South Africa
jvonsolms@gmail.com, josef.langerman@standardbank.co.za

Abstract. The importance of Treasury management, within a commercial bank has increased significantly over the last couple of years. After the 2008 financial crisis the role and responsibility of a Treasury department has changed in terms of scope and strategic importance, evolving from a transactional cash manager to the guardian of the balance sheet. In order to meet this broader strategic mandate, Treasurers must therefore consider ways to become more effective and streamlined, while reducing time-consuming operational activities. Digitalisation can address many of the traditional Treasury challenges and provide a number of commercial and competitive benefits as well. However, to successfully adopt digital technologies and related digital innovations, Treasury requires a well-defined digital transformation plan. The Smart Digital Treasury Model (SDTM) was developed to provide a comprehensive roadmap to assist a Treasury's digital transition towards a next generation 'smart' Treasury department. This paper explores a key building block of the SDTM, which addresses the risks and threats that can arise from the adoption of new digital technology. The reason for focusing on this aspect is that many of the digital risks have no direct reference points with conventional banking activity or security measures. The result of this research is an approach that articulates Treasury specific digital risks and threats, as well as describes a risk management process that can be deployed as part of the digital transformation. The digital landscape is evolving the whole time; therefore, digital risk management activity in Treasury can't be seen as a once-off exercise, but needs to evolve in line with market developments.

Keywords: Digital technology · Digitalisation · Innovation · Smart treasury · Digital risks and threats · Evolution of treasury · Cyber security

1 Introduction

The Treasury department in a commercial bank plays a crucial role in managing a commercial bank's scarce financial resources such as capital and liquidity. The responsibility of the Treasury department has changed significantly over the last couple of decades and especially since the 2008 financial crisis. During this time, Treasury has evolved from being primarily focussed on transactional activities such as cash management to becoming the guardian of the holistic balance sheet, with an important role in setting the firm's strategic direction.

H. Venter et al. (Eds.): ISSA 2020, CCIS 1339, pp. 1–19, 2020.
https://doi.org/10.1007/978-3-030-66039-0_1

These changes in the Treasury mandate were driven by a combination of factors, including developments in regulations, technology, monetary policy and the altering of the competitive landscape. As the custodian of the balance sheet and manager of scarce and expensive financial resources, Treasury is under ongoing pressure on various fronts and therefore requires change and transformation to remain effective. On the one side, the regulatory requirements are becoming more onerous calling for greater granularity and precision, higher frequency of reporting and forward-looking analytical capabilities. On the other side, the Chief Executive Officer or Chief Financial Officer increasingly looks to the Treasurer, often in real-time, for strategic decision-making and holistic attestation that the balance sheet is efficiently optimised.

For many Treasury departments there are a number of obstacles in the way of achieving this broader strategic mandate, including: the complexity of a bank's business model, fragmentation of upstream systems, legacy technology not tailored for evolving Treasury needs and large amounts of data to process and analyse. Comprehensive digitalisation of Treasury can help address some of these challenges and can deliver a range of commercial benefits, for example: reduce operating costs, enhance Net Interest Income, improve risk management and optimisation of capital and liquidity buffers [17].

Leveraging appropriate digital technology solutions for core activities like risk management of Liquidity and Capital - which requires large amounts of data analysis, real-time decisions, and complex forecasting - can provide a number of advantages for Treasury. These benefits include:

- Deliver on its growing strategic mandate by automating manual processes to reduce operational activities and support better strategic decision making;
- Keep tread with digital transformation in the rest of the bank, which will increasingly put pressure on Treasury's legacy systems and processes, if no corresponding digital transformation takes place;
- Ensure an ongoing competitive advantage relative to developments in challenger banks and Fintech competitors; and
- Future proof Treasury against anticipated step changes in the financial markets for example open banking.

A problem is that Treasury tends to be a slow adopter of digital technology and often does not have a well-articulated digital strategy. A survey by the Boston Consulting Group of 44 banks revealed that most Treasury functions have relatively low level of digital maturity. The analysis shows that only 11pct of bank Treasuries made widespread use of advanced technologies and use cases, while about 70pct have yet to embrace digitalisation in any meaningful way [14]. The 2019 PWC Global Treasury benchmarking survey [12], found that the biggest roadblocks for implementing digital technologies in Treasury were inter-alia:

- lack of digital use cases/business cases;
- no mid to long term strategy; and
- lack of people skills.

There is thus a requirement for a Treasury specific digital transformation model which provides clear guidance for its digital transformation journey. The Smart Digital Treasury Model (SDTM) was previously developed with the objective to provide a Treasury a well-defined roadmap, in the transition towards becoming a more mature digital user. The logic and approach of the SDTM was researched and described by the authors in a prior paper [32] and comprises of four main building blocks namely:

1. Digital Maturity Assessment and identification of digital use cases;
2. Digital Technology evaluation and Business Case development;
3. Technology implementation plan; and
4. Management of Digital Technology Risks and Threats.

This paper will focus on the fourth building block of the SDTM, namely the identification and management of risks and threats that can arise in Treasury due to the adoption of new digital technology.

Section 2 looks at a literature review and the reasons why it is critical to identify, consider and mitigate any exposures that may arise as part of the digital transition of a Treasury. Section 3 briefly introduces the Smart Digital Treasury Model (SDTM) and describes its different building blocks. Section 4 explains the different risks and threats that a Treasury might face when adopting new digital technologies. Section 5 considers a holistic risk management solution to combat the new digital exposures.

2 Literature Review

A bank's Treasury department has evolved significantly over the last couple of decades [3]. The discipline has its roots in the latter part of the previous century, with the introduction of Treasury specific management systems and software. Over the turn of the century many Treasury functions turned from a regional focus to a more global focus as banks consolidated and expanded internationally [23]. However, since the 2008 financial crisis, Treasury's role and responsibility has changed significantly. The evolution can be divided into distinct stages, driven by the developments in regulations [26], new technology [8], monetary policy [27] and competitor activity [16]. The high-level stages are:

Pre the Financial Crisis (prior to 2008) no comprehensive global regulations were enforced for certain key risks such liquidity and balance sheet leverage. One of the outcomes were that funding were readily available and relatively cheap and the Cost of Funds was therefore not accurately reflected in new asset origination, resulting in an increase in credit supply and low loan margins - with limited leeway to absorb future funding shocks [25]. Therefore, when the 2008 financial crisis hit, banks struggled to continue financing their bulky balance sheets on a profitable basis.

Post the Financial Crisis (2008 to 2015) a range of new regulations were introduced (i.e. Basel III accord, Dodd-Frank and others) calling for higher capital buffers, larger liquid asset portfolios, more granular and frequent reporting, stress testing etc. [28]. In order to meet these increasing prudential demands and ensure the regulations were implemented, different Treasury related activities [6] were centralised into a Group Treasury unit [24].

The new Regulatory regime (after c. 2015) meant the role of Treasury started to shift more towards becoming a guardian of the balance sheet, with responsibility for the holistic management of all assets and liabilities. One reason was that senior management needed to ensure the balance sheet was sustainable and profitable going forward, in light of all the prudential constraints that was imposed on scarce balance sheet resources like capital and liquidity.

In order to meet this broader strategic mandate Treasury must consider different technology solutions such as digitalisation to become more efficient and streamlined by reducing time-consuming operational activities. The problem is that Treasury management is increasingly faced with the difficult challenge of weighing the value of deploying new digital solutions to improve internal processes and ward of external competitors against the potential new risks that the technology potentially creates. The reality is that new technology often equals new risks. A 'tried and tested' technology infrastructure has a known risk profile; however, deploying cutting edge innovation creates a different kind of risk profile and therefore new technology is often far more vulnerable.

As an example, Volt a new online bank in Australia is one of first banks globally, that will perform all its processing and data storage in the cloud [20]. This approach has significant benefits compared to using old legacy banking systems, but comes with a totally new set of risks and exposures, which needs to be managed.

This increased risk is especially relevant for traditional Treasury functions which is used to operating in a centralised environment, where data and its activities are protected behind the external firewalls and security measures of the broader bank's defences. These risks have made many regulators hesitant to open the distributed computing field too rapidly. In a recent report the Bank of England indicated that it has ongoing concerns about 'concentration risk and lack of substitutability', pointing to lingering worries about the wisdom of putting critical financial applications on someone else's infrastructure, which has not been immune to resilience issues [30].

This reservation is also shared in some regard by market participants. In 2018 the Association of Finance Professionals (AFP) undertook a risk survey, where they found that Treasury and finance professionals are worried about emerging technologies even as those technologies provides increasing benefits [1]. The following findings were made:

- A majority of survey respondents cited Artificial Intelligence, Robotic Process Automation and Data Engineering as technologies that could expose their companies to additional risks;
- Treasury and finance professionals perceive new technology risks through a traditional cybersecurity lens. However, operational risks and business continuity risks are also cited as consequences from the introduction of new technologies;
- A majority of organizations has no Board approved risk-appetite policy;
- One third of organizations are unprepared for new risks arising from the implementation of new technology and only a small percentage are confident in their preparations.

It is therefore crucial that as part of the digital transformation journey of a Treasury function, all the potentially digital risks are identified and plans are put in place to address these additional threats. The European Banking Authority (EBA) published a report in

January 2020 on the impact of Big Data and Advanced Analytics [13]. It found that a data-driven approach is emerging across the banking sector, affecting bank's business strategies, risk, technology and operations. The report notes a number of fundamental challenges that needs to be sufficiently addressed. These risk factors include: Ethics, Explainability and Interpretability, Fairness and Avoidance of bias, Traceability and Auditability, Data protection, Data quality, and Security and Consumer protection. The AFP Risk survey [1] found that new or increased risks being managed as a result of increased digital technology are: Cyber Security, Operational Risk, Business Continuation, Error and omissions, Regulatory Risk, Cloud Risk, Reputational Risk and People Risk.

Since all these risk factors can have an influence on a Treasury department when it adopts new digital technology, it is crucial to study them in more detail. The reason is that Treasury is a significant user of data in order to interpret information for strategic capital and liquidity decision making purposes, leaving it exposed to arising digital threats. Academic literature often overlaps in terms of the main digital risks and concerns and importantly tends not to be Treasury specific. Therefore, this paper will study the risks and threats that can arise and requires attention in the context of a Treasury's digital transformation.

The research methodology underpinning this study takes the form of a Design Science research. The reason is that a Design Science approach works well for problems that reside at the intersection of Information Technology and deployment thereof in organisations. The digitalisation of a Treasury function fits well into this paradigm. The output of the research is to produce an Artefact (i.e. Smart Digital Treasury Model), which will have practical value to both a research and professional audience. The Risks and Threats component explored in this paper forms an integral part of this Artefact.

The next section will briefly introduce the Smart Digital Treasury Model (SDTM) to explain how the management of digital risks and threats fit into the overarching model. Following from that the digital risk and threat elements relevant for a Treasury will be identified and explored in more detail.

3 Smart Treasury Digital Model (STDM)

The emphasis on digital technologies and digital strategy in banks have increased significantly over the last couple of years. The development of digital applications in areas like: online banking, customer payments, credit scoring, fraud prevention and detecting money laundering has grown in leaps and bounds. The common denominator in most of these applications is often the customer interfacing dimension. The rationale is that it simplifies banking for clients, improves customer experience and leads to cost reduction, in that there is a reduced need for bricks and mortar branches.

On the face of it many banks would therefore appear relatively advanced in the adoption of digital technologies or on a pathway to achieve digital maturity in the foreseeable future. However, the progress of digitalisation in a bank is not consistent throughout the organisation. One area specifically that has not kept up with wider digital development is the Treasury department. A recent survey found that most Treasury professionals (97pct) still use Excel as their primary tool, ironically while 28pct believes it is not a fit for purpose risk management tool [1].

Given the growing importance of bank Treasuries and its increasing strategic management mandate many departments, in line with the broader developments in banking, are looking at digital solutions to manage its activities more effectively. To achieve this objective, it is crucial to have a Treasury specific framework in place to measure the present digital maturity and provide guidance on the transitioning to a more advanced digital environment. The Smart Digital Treasury Model (SDTM) was developed for this purpose, namely to support and guide the evolution towards a next generation smart Treasury department fit for the 4th Industrial Revolution. In a paper entitled *'A Smart Treasury fit for the 4th Industrial Revolution'* the approach of how the model was designed and developed is described in more detail. In summary the main components that can impact a Treasury's digital transformation was identified and combined into an overarching model [32]. Figure 1 provides more insight on the underlying building blocks of the SDTM.

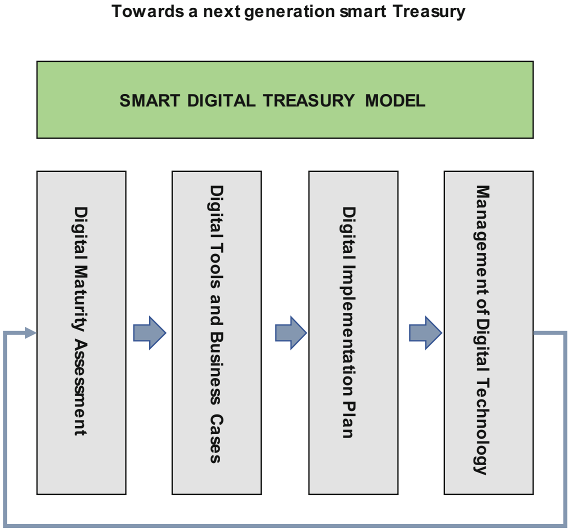
Towards a next generation smart Treasury
SMART DIGITAL TREASURY MODEL
Digital Maturity Assessment
Digital Tools and Business Cases
Digital Implementation Plan
Management of Digital Technology

Fig. 1. Smart Digital Treasury Model (SDTM)

The model comprises of four building blocks:

- **Block 1: Digital Maturity Assessment and Identification of Digital Use Cases** - measures the digital maturity of a Treasury against a specific set of criteria and scores the digitalisation level/readiness on a scale from beginner to advanced. It then identifies and describes digital use cases for the core Treasury activities and rank these for further development.
- **Block 2: Digital Technology Evaluation and Business Case Development** - digital use cases are mapped into the most appropriate digital technology tools. It is then build-out into more detailed business cases, that are prioritised based on defined requirements as well as performance hurdles like Return on Investment (ROI). This is

to ensure that any subsequent implementation will deliver the expected benefits and ensure the Treasury transition successfully to a more digitally mature state.

- **Block 3: Digital road map of Technology implementation** - this building block articulates the execution plan and approach applied to implement the new digital technology.
- **Block 4: Management of risks originating from Digital Technology adoption** - managing the risks and increased threats arising from digitalisation in Treasury is an important consideration. It therefore requires a dedicated approach to identify and mitigate these potential risks.

The contribution of the model is that it provides a unified and comprehensive approach, specifically to assist a commercial bank's Treasury department in its digital transformation. The adoption of digital technology can be a difficult and expensive endeavour. It is therefore imperative that a Treasury department has a well-articulated plan or roadmap in place that can guide its transition towards a smart function in an effective manner. For example, one of the key building blocks at the start of the digital journey is to perform a Digital Maturity Assessment. Von Solms [31] describes how a Digital Maturity Assessment (DMA) can be implemented specifically for a Treasury, that measures its existing digital maturity level and identify the gaps to focus on for future digitalisation.

The SDTM ensures that the subsequent digital technology evaluation and implementation thereof is done in an integrated manner. Also, that there are a pro-active awareness and focus on digital risks and threats through-out the adoption process, rather than as an after-thought once the technology has been deployed. This next section will focus on the fourth building block of the SDTM, namely the management of risks and threats that may arise due to the adoption of new digital technology.

4 Identifying Risks and Threats that May Arise from Adopting Digital Technology

Digital technologies like Artificial Intelligence, Machine Learning, and Advanced Data analytics have existed in some form or shape for the last couple of decades. However, the recent growth in processing power and the explosion of data available to 'learn from' mean innovative analytical tools are becoming far more useful and effective.

An area in the bank that can gain significant advantage from leveraging digital technology is the Treasury function. The reason is that there are a number of its activities, which fits well into a digital technology framework e.g. cash flow forecasting can be improved by Machine Learning; Payments and settlements can be automated through Artificial Intelligence; while Risk Management and Reporting of Capital and Liquidity exposures will greatly benefit from Big Data and Advanced analytics.

As a Treasury adopts more of these technologies it is important to identify all of the potential digital risks and how to mitigate them. A systematic search of academic literature finds a number of studies focussing on security awareness and training in general [5] and specifically within the banking domain [10, 22]. There are also a wide range of literature that covers the subject area of threat intelligence and provides policies and frameworks for the effective management in banking [4, 19, 29]. Although all very applicable for a Treasury department a consideration is that many of these are not focussed on Treasury. Another factor is that digital risks can also include more qualitative aspects - such as explainability of model decisions, fairness, regulatory risks - which are also relevant for Treasury activity. For example, the European Banking Association [13] identifies a comprehensive spectrum of potential risk and threats to consider when deploying Big Data, while the Association of Finance Professionals [1] highlights the main risk factors to manage with increased use of digital technology.

This section attempts to evaluate the various risks and threats identified from academic literature into a dedicated Treasury focussed framework. The basis for proposing the following risks were validated through structured interviews with Treasury experts. The key risk factors identified for consideration in a Treasury department is shown below in Fig. 2.

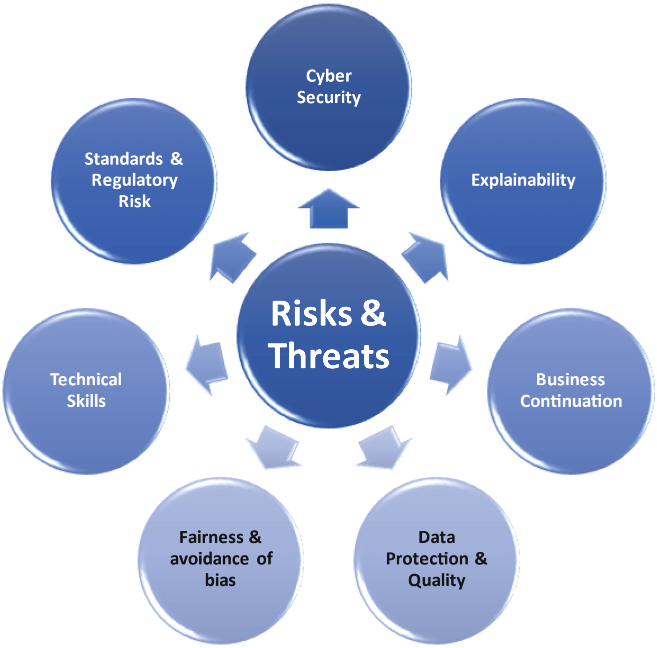
Cyber Security
Standards & Regulatory Risk
Explainability
Risks & Threats
Technical Skills
Business Continuation
Fairness & avoidance of bias
Data Protection & Quality

Fig. 2. Risks factors related to adopting digital technology in Treasury

Each of these seven risk factors are discussed in more detail below:

4.1 Risk Driver 1 - Explainability

The use of digital technologies including Machine Learning, Big Data and Advanced Analytics can quickly lead to untransparent ‘black box’ systems. This can make it very difficult to always understand, the internal behaviour or logic and verify how the model has reached a certain conclusion or result.

Opaque systems stand in direct opposition to explainability. Transparency is about being able to describe, inspect and reproduce the mechanisms through which the digital solution derives an outcome and having the appropriate governance in place. In different terms it means explaining the rules that the algorithm uses in a way that can be easily understood by humans [13].

Lack of explainability represents a serious threat for digitalising a Treasury. The reason is that Treasury is the gatekeeper of the bank's balance sheet and the manager of the scarce resources including capital and liquidity. It therefore has an important fiduciary duty to report and explain these balance sheet constraints to regulators, senior management, businesses and external shareholders in a clear manner. The capital and liquidity numbers can influence a wide range of aspects, from impacting on business growth to raising regulatory concern around the viability and financial robustness of the bank.

When a Treasury adopts digital technology it therefore needs to ensure that all the steps and decisions made through-out the entire analytics process are clear, transparent and traceable to enable oversight. In essence this translates to auditability, which is the ability for an outside entity (e.g. the regulator) to review how Treasury developed its algorithm, without compromising the bank's intellectual property.

4.2 Risk Driver 2 - Cyber Security

Banks as the custodians of money have been under attack for hundreds of years. In the beginning, it was the physical theft of monies from 'brick and mortar' branches. Then it moved to computer fraud using technology. Today, it's not just cyber theft of money, but also the hacking of bank systems to obtain personal information on customers. This is why cyber security in banking is of utmost importance [7]. Treasury has access to a vast amount of bank data because it has links into a wide range of banking systems inter-alia:

- Customer Product systems used for Loan and Deposit Pricing;
- Risk Management systems used for Interest Rate Risk management;
- Trading Systems containing trading strategies; and
- Finance and Accounting systems holding all bank's financial information.

The reason Treasury requires this myriad of data is in order to construct a holistic picture of the balance sheet to manage the funding, liquidity, and capital positions as well as the banking book risks (e.g. interest rate and currency).

Furthermore, it normally integrates this fragmented data and transforms it into valuable management information e.g. capital demand, contingent liquidity requirement and interest rate risk exposure. This management information is used in senior management committees for example the Asset and Liability Committee (ALCO) to support strategic decision making [15]. This centralised and strategic function makes Treasury somewhat unique in the organisation and therefore it has always been open to a range of specific computer security risks e.g.

- Theft of important confidential information like the ALCO report and supporting analysis;

- Hacking into Treasury Management Systems such as the payment and settlement systems to influence payments and/or commit payment fraud; and
- Viruses infecting systems that drives trading decisions and hedging.

Treasury has a number of defensive security measures in place, that are normally aligned with the bank's wider security policy. This can include biometrics, authentication and authorisation, firewalls etc. One of the major defensive techniques for a Treasury is that its data, models and systems are usually on bank owned infrastructure and maintained centrally.

The adoption of more advanced digital technology can impede these traditional protective measures and generate additional risks, normally due to the higher connectivity to the internet. Using distributed cloud computing functionality can open up Treasury to widespread attacks on its sensitive management information. Also, it could involve potential hacking of its 'intelligent' proprietary digital models (i.e. Big Data and Advanced analytical models). This type of model attack could entail model theft (e.g. stealing intellectual knowledge) or model poisoning (e.g. influencing the model's behaviour/output in a known or unknow manner).

It is therefore important for a Treasury to pro-actively enhance and strengthen its security measures as it adopts digital technology. This could include maintaining a technical watch, and regular updates on progress on security attacks and related defence techniques.

4.3 Risk Driver 3 - Fairness and Avoidance of Bias

A number of regulators have raised concerns that digital technology like Artificial Intelligence may unintentionally exclude customers from access to banking if it introduces bias against certain new customers or those seeking loans. For example, the Hong Kong Monetary Authority (HKMA) has put directives in place seeking to ensure customers and their data are treated fairly [18].

Bias can be introduced into the process through either the data or the algorithm being used. In the former, the outcome might be impacted by the way the data is collected or selected for use. In the latter, the models may be trained on data containing human decisions or on data that reflect second-order effects of social or historical inequities.

This a crucial element for a bank Treasury, since it is the 'bank within the bank' and effectively functions as a clearing house for capital and funding, which is often driven by the underlying behaviour of customers. For example, one of the key Treasury activities is Funds Transfer Pricing (FTP), which assigns an internal price for funding sources like deposits and charges out the cost of funds to assets, like loans which require funding. FTP is rooted in the behavioural science of clients i.e. in terms of how long the funding remains with the bank (i.e. stability), or how quickly customers pay-back their loans. This behaviour is driven by many factors including: geographical location, income, access to different banking channels and others. Treasury therefore has to be aware of these elements and how they can influence its decision-making ability, when using more advanced digital technologies.

This awareness can be achieved by ensuring processes are in place to maximize fairness and minimize bias created by technologies like Artificial Intelligence (AI) e.g.

- Identify where there is a high risk that AI could exacerbate bias or help correct for the bias;
- Establish processes and practices to test for and mitigate bias in AI systems;
- Recognise that potential biases in human decisions exist and how this can flow into models; and
- Invest more in bias research and make more data available for research (while respecting privacy).

Fairness also relates to ethics. The development, deployment and use of any intelligent solution should adhere to some fundamental ethical principles such as respect for human autonomy, prevention of harm, explainability and guarantee that the outputs are free from unfair bias and prejudice, whether conscious or unconscious.

The risk for a Treasury is that if it does not address these considerations upfront, it could lead to Legal, Operational and Reputational issues down the line.

4.4 Risk Driver 4 - Data Protection and Quality

Data is a very valuable commodity and therefore it must be well protected. Data has always been the cornerstone of finance - from primitive ledgers to today's hyper-connected markets.

As mentioned, Treasury has a somewhat unique position in the bank since it holds a lot of data, ranging from customer level data to risk management data.

The first consideration for a Treasury is that it is critical that this information is well defended against internal and external threats. In a traditional set-up, it is normally protected by the banks centralised security measures, but this challenge can magnify significantly if data/information is moved to distributed cloud computing. This is one of the reasons why central banks historically were hesitant to fully endorse aspects like cloud-based computing [30]. However, this is not stopping new banks to venture down this route. Volt a new Australian online bank will only use cloud-based computing. While potential Volt customers are largely unaware of the distinction between public and private clouds, they are concerned about their data and how it is used. Volt is therefore developing a data policy for distributed data, that will be overseen by independent committees and that it hopes will be adopted by other Australian banks [20].

A second consideration is that when managing customer data, e.g. for behavioural profile of clients, a digital technology solution like Big Data and Advanced Analytics needs to comply to current regulation on data protection. This means the bank should have a lawful basis for processing the personal data. In addition, customers have the right to demand human intervention and not be subject to a decision based solely on automated process e.g. profiling, if the outcome impacts the customer in a significant manner [13].

Another issue for a Treasury is that the quality of data it uses might not always be that robust, since it can originate from fragmented bank systems which is not always aligned in terms of format or standards. Therefore, there is an obligation on Treasury to check the data quality and discard any low-quality inputs before it feeds into the digital models. An important point is that digital technology is not a panacea to fix bad quality data (meaning garbage in equals garbage out); using bad quality data to drive Big

Data and Machine Learning, can magnify the errors and lead to wrong decisions being made. Therefore, a Treasury needs to work very closely with upstream data providers to confirm the data quality, scrub the data and discard any data sources which do not meet its defined checks and balances.

4.5 Risk Driver 5 - International Standards

Treasury driven solutions are increasingly becoming more advanced and offering clients improved and real-time access to information and payments. As an example, HSBC has recently announced the launch of a Treasury Application Programming Interface (API) covering payments in 27 markets in a bid to offer business clients a faster and more seamless way to transfer funds [2]. Using HSBC Treasury APIs, Treasurers can make payments from their own workstations, without logging into a proprietary bank platform. Clients receive confirmation that a payment request has been received and can track payments from their accounts to the beneficiary, improving visibility over transactions.

APIs are facilitating a key shift towards more open banking by removing barriers between applications and systems and enabling seamless interaction between these different platforms. However, to ensure a level playing field for all competitors including well-regulated bank Treasuries and loosely controlled Fintech challengers, common standards are required. Data standards and protocols are the bedrock of a robust and dynamic financial system. They can enable innovation and competition and reduce the cost of finance. However, standards need to be consistent for all participants as it pertains to privacy, security, trust, resilience etc.

The risk for a Treasury is that in the absence of clearly defined standards around the deployment of digital technology, it either does nothing and thereby lose touch with wider market developments or proceed and implement solutions, which does not meet future requirements. Consistent data standards could bring several benefits to many different banking areas that Treasury interacts with:

- Innovations in retail payments, built-on common data standards and protocols, can enhance the understanding of client habits and transform deposit product developments;
- Access to wider data sets could allow more tailored and accurate decisions about lending, opening new borrowing opportunities for customers and small businesses;
- Big Data can help provide an in-depth understanding of business models for credit assessment; and
- Transferring data through APIs could give households and businesses better information about and access to financial products.

4.6 Risk Driver 6 - Business Continuation

A bank's Treasury normally has a number of activities that needs to be executed daily or even intraday, for example payment and settlements [11]. This real-time management and reporting requirement make it challenging for a Treasury to implement any new technology, given the potential impact on business continuation. A further difficulty for a typical Treasury function is that it operates in a technology environment that often comprises of largescale legacy systems, like cash management systems, which uses older technology which is not very adaptable for new requirements. Also, Treasury normally does not own the upstream data systems like product and pricing platforms, which makes it very difficult to implement any major changes. The reality is that Treasury is very intertwined with many different business divisions within the bank; therefore, making implementation of digital technology tricky, given the significant repercussions on business continuity if something goes wrong.

The one thing a bank cannot allow is to go offline, it is truly a 24/7 business, where even in the middle of night, batch operations run to process the previous day's transactions. Treasury digitalisation therefore, at least initially, needs to identify business cases to target which are more controllable or can be run separately as prototypes, before switching off life bank systems. Examples of these Treasury applications areas are:

- Big Data and Advanced Analytics used for financial planning and forecasting purposes,
- Machine Learning deployed to identify customer behaviour, and
- Robotic Process Automation implanted to automate certain Treasury owned processes.

As Treasury becomes more comfortable with digital technology deployment and proof its feasibility to senior management, it can be expanded to larger scale projects across the bank's wider technology infrastructure.

4.7 Risk Driver 7 - Technical Knowledge and Skills

The conundrum with digital technology implementation is that the required digital skills often resides in the technology department or some of the client-facing business areas and not in Treasury.

Treasury personnel's expertise often tend to be in disciplines such as capital management, liquidity management, portfolio management, which are specialised banking or finance skills. The business and technology skillsets in terms of training and education more often than not do not overlap. This is one of the key reasons, why digital technology adoption in Treasury is relatively low [1]. Treasury also do not have the same push-pressure to upskill, compared to other client interfacing business areas in the banks (e.g. mobile banking and fraud detection units).

Therefore, Treasury must emphasise upgrading its skills and employing new digital expertise instead of just focusing on traditional finance, tax and accountancy skillsets. If it does not expand its technical knowledge and expertise it will not be able to effectively reap the benefits of rolling out digital technology. Or it will implement digital solutions that it will struggle to maintain and manage going forward.

To be successful in an increasingly digitalised environment it must combine the right technology with the right talent. At a strategic level this will require that Treasury management build a digital vision and put together teams that are able to:

- understand the impact of digital technology on Treasury;
- articulate and champion the value of digital solutions to old Treasury problems;

- develop a strong business/technology foundation for digital transformation;
- partner and collaborate with other digital technology developments and teams in the bank; and
- implement and manage the required changes.

This section identified a range of risks and threats that a Treasury department should consider when implementing new digital technology. It is not an exhaustive list, but focused on the main challenges, which can impede the successful deployment of new digital technology. The next section will look at how these risks and threats can be managed in a holistic and integrated manner.

5 Managing Digital Risks and Threats in Treasury

It is important to manage the various risks and threats that can manifest from the adoption of new digital technology effectively. For a bank Treasury digitalisation often entails moving away from manually controlled processes, where the interpretation of results is based on personal experience and can be overridden if need be. Automation of processes and the introduction of intelligent algorithms can make many Treasury activities more effective, quicker and cost efficient, but it requires additional safeguards throughout the process to ensure the output is fair, explainable and unbiased. Also, leveraging technology like cloud computing have advantages, but it can move Treasury outside the security of its traditional defensive wall, which is often centralised and well protected behind the bank's wider computer security protocols.

There are various academic articles which looks at digital risk management in a digital economy such as [9] and within banks specifically [17, 21]. The section below tailors and refines these different risk management frameworks and approaches for a Treasury department. Figure 3 depicts the primary steps that can underpin a Treasury's digital risk management approach.

The next section looks at a risk management cycle that can be used in Treasury to manage the threats and risks in a more integrated manner.

5.1 Step 1 - Develop a Board Approved Risk Appetite Policy

As identified in the AFP survey [1] many banks do not have a board approved policy for digital risks. In cases where a digital policy does exist, it is often focussed on the client interfacing business activities, and not specifically on functions like Treasury.

As mentioned, Treasury has an important role and responsibility within the bank because it interacts with a lot of external counterparts and internal businesses and are involved with various transactional systems.

It is therefore crucial that the Treasurer works with the Board and the Risk Management division to ensure that a digital risk policy is formulated and that it includes Treasury activities [30]. This is required to define a formal digital risk appetite for the firm and provide guidance to Treasury on what digital technologies it can focus on. It will also ensure that the right governance and oversight is in place for any future implementation.

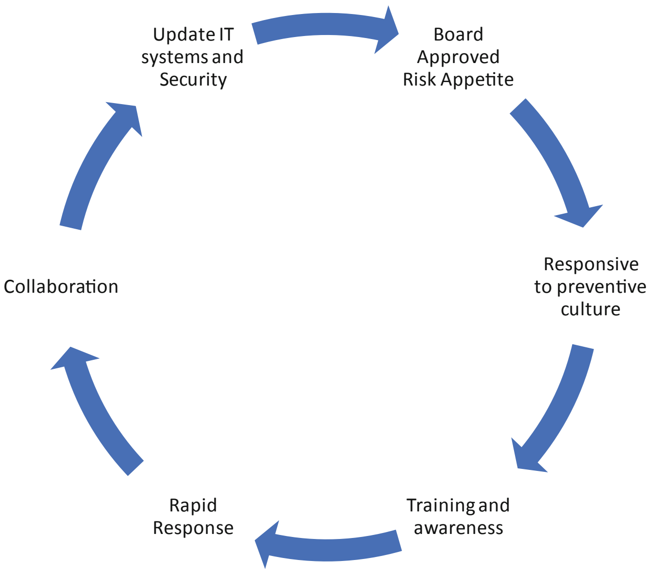
Update IT systems and Security
Board Approved Risk Appetite
Responsive to preventive culture
Training and awareness
Rapid Response
Collaboration

Fig. 3. Managing digital risks and threats in Treasury arising from digital technology adoption

5.2 Step 2 - Evolve from a Defensive to an Offensive Environment

Digital technologies often expand the footprint of the bank. This opens up a lot more avenues of attack that can be used to hack into the bank's or Treasury's systems to steal valuable data and/or smart models. This digital expansion requires that security measures must evolve from being primarily defensive to becoming more offensive in nature. This means that policy, systems and the culture need to be reengineered, not just to protect the bank's 'valuable assets' against cyber-attacks, but also to pre-emptively identify and eliminate threats before it occurs.

5.3 Step 3 - Training and Awareness on Digital Technology Risks

As mentioned previously it is crucial that training and awareness of digital technology risks takes place in Treasury. The reasons are two-fold:

1. Digital technology utilisation can often create new risks and threats that has limited reference points with traditional banking activity. For example, cyber theft of money or data sounds straight-forward, but the ways and means hackers can attack the bank can vary significantly (in contrast to an old-style bank robbery). Furthermore, the use of intelligent models for decision-making purposes can create outcomes, which is not anticipated.
2. Normally personnel in areas like Treasury and Finance do not have a technology background. It is therefore crucial that they are educated on the use and risks of digital technology and that teams are expanded to include individuals with technology experience.

5.4 Step 4 - Real-Time Threat Monitoring

Digital technology offers many benefits, one being that it can improve the frequency of certain Treasury activities to almost real-time e.g. intra-day liquidity management [11], or client API payment execution [2]. This means protective measures need to evolve to become more rapid responsive. If something goes wrong or a threat materialise it needs to be identified and addressed immediately. This is a paradigm shift for many Treasuries that are used to operating on a slower timescale.

5.5 Step 5 - Collaboration and Information Sharing

The real success of digital technology implementation and combatting digital threats reside in taking a unified approach across the firm. Many banks are relatively digital mature as it pertains to client facing applications like online banking and fraud detection and therefore have the relevant digital skills and experience in place. However, digital maturity is not always uniform across the organisation. As indicated, Treasuries tends to be slow adopters of digital technology. Rather than re-invent the wheel and starting from scratch, it can really benefit from collaborating with other business units and through the sharing of information. This will ensure the bank's digital strategy is integrated and consistently implemented.

5.6 Step 6 - Update/Revise IT Systems and Security

Implementing any new technology including digital technology may require an update to existing IT systems and security measures. These can include inter-alia: preform a security audit to reveal the strengths and weaknesses of the existing setup, strengthen the existing firewalls, update anti-virus and anti-malware applications and consider enhanced authentication like biometrics, too obtain access confidential data and/or models.

6 Further Development and Research

This paper studied the risk and threats that can arise from the adoption of Digital Technology in Treasury. Identifying and protecting against digital risks cannot happen in isolation, but needs to form part of a unified digital transformation plan that inter-alia includes elements such as business case development, selecting appropriate digital technology and its implementation, as well as protective measures against new digital threats.

Therefore, the management of digital risks and threats described in this paper forms an integral part of the overarching Smart Digital Treasury Model (SDTM). The intention is that once completed the SDTM will be tested with a number of bank Treasuries to validate the feasibility and robustness of the model. This user acceptance phase will include evaluation of the risk management building block as well. Based on the market practitioner feedback it will either move forward for adoption or if required further research and modification will be undertaken.

7 Conclusion

The role and responsibility of a Treasury department within a commercial bank has changed significantly over the last couple of decades and especially since the financial crisis. During this time, a bank's Treasury function has evolved from being primarily focussed on activities like cash management to becoming the guardian of the holistic balance sheet.

Comprehensive digitalisation of Treasury can help support this expanding mandate and can deliver a range of commercial benefits, for example reduce operating costs and enhance Net Interest Income. The problem is that Treasury tends to be a slow adopter of digital technology and often does not have a well-articulated digital strategy. The Smart Digital Treasury Model (SDTM) was developed with the objective to provide a bank Treasury a well-defined roadmap to transition towards becoming a more mature digital user.

As part of digital transition, it is important to identify and manage any risks and threats that may arise due to the adoption of new digital technology. For a bank Treasury it often entails transitioning away from manually controlled processes, where the interpretation of results is based on experience and can be overridden. Automation of processes and the introduction of intelligent algorithms can make many Treasury activities, more effective, quicker and cost efficient, but it requires safeguards throughout the process to ensure the output is fair, explainable and safe. Also, leveraging technology like cloud computing have a range of benefits, but it moves Treasury outside its traditional security defence, which is often centralised and well protected behind the bank's wider computer security protocols.

The contribution of this paper is in researching an approach that identifies the main threats and risks that a Treasury should take cognisance off, when adopting new digital technology. It also describes a risk management framework to assess and manage these digital risks in a holistic manner across Treasury. The digital landscape is evolving the whole time; therefore, this digital risk management process can't be managed in isolation or seen as a once-off exercise, but needs to be part of an integrated digital transformation plan.

References

1. AFP. AFP Risk Survey Report. Treasury Risk Survey Report. Association of Finance Professional (2018). https://www.oliverwyman.com/our-expertise/insights/2018/jan/2018-afp-risk-survey-report.html
2. Ashar, J.: HSBC Launches Treasury APIs for Payments in 27 Markets (2020). https://www.theglobaltreasurer.com/2020/01/15/hsbc-launches-treasury-apis-for-payments-in-27-markets/
3. Association of Finance Professionals: AFP Strategic Role of Treasury Survey. Association of Finance Professional Library (2017)
4. Barrigar, Z.: Examining the Current Threat of Cybercrime in Mobile Banking and What Can Be Done to Combat It - ProQuest. Utica College: ProQuest Dissertations Publishing (2020)
5. Bauer, Stefan, Bernroider, Edward W.N.: From information security awareness to reasoned compliant action: analysing information security policy compliance in a large banking organization. ACM SIGMIS Database DATABASE Adv. Inf. Syst. **48**(3), 44–68 (2017). https://doi.org/10.1145/3130515.3130519

6. Bragg, S.: Treasury Management: The Practitioner's Guide. Hoboken, N.J. (2010)
7. Camillo, Mark: Cybersecurity: risks and management of risks for global banks and financial institutions. J. Risk Manage. Financ. Inst. **10**(2), 196–200 (2017)
8. Ceren, J., Montegelli, S.: Trends in technology: how web 2.0 will impact the next generation of online treasury tools. J. Corp. Treasury Manage. **1**(1), 78–82, 5 (2007)
9. Chernyakov, M., Chernyakova, M.: Technological risks of the digital economy. Корпоративные Финансы **12**(4) (2018). https://cyberleninka.ru/article/n/technological-risks-of-the-digital-economy
10. Daniel, W.K., William, K.F., Ling, M.L., Lai, S.M., Tevanotai, A.: Awareness in E-banking security and usage. In: 2014 International Conference on Information Science, Electronics and Electrical Engineering, vol. 2, pp. 1176–1150 (2014). https://doi.org/10.1109/InfoSEEE.2014.6947856
11. Davies, A., Wheaton, M., Stambaugh, T., Wilson, M.: Intraday Liquidity Management|Accenture. Accenture Consulting (2019). https://www.accenture.com/gb-en/insights/financial-services/intraday-liquidity-management
12. Di Paola, S., Cohen, E., Farrar, I.: Global Treasury Benchmarking Survey 2019. PwC 2019 (2019). https://www.pwc.com/gx/en/services/audit-assurance/publications/global-treasury-benchmarking-survey-2019.html
13. EBA. EBA Report Identifies Key Challenges in the Roll out of Big Data and Advanced Analytics. European Banking Authority, 13 January 2020. https://eba.europa.eu/eba-report-identifies-key-challenges-roll-out-big-data-and-advanced-analytics
14. Elgeti, C., Schäfer, R., Vogt, P., Broemstrup, I., Lai, C., Granzer, M., Strauch, T.: Creating a Digital Treasury in Banking. Boston Consulting Group (2019)
15. FSA: Senior Asset and Liability Management Committee Practices. Financial Services Authority Library (2010)
16. Harrison, T., Estelami, H.: The Routledge Companion to Financial Services Marketing. Routledge Publishing, London (2014)
17. Harvey, David: Digital transformation in banks: the trials, opportunities and a guide to what is important. J. Digital Bank. **1**(2), 136–145 (2016)
18. HKMA. High-Level Principles on Artificial Intelligence. Hong Kong Monetary Authority (2019)
19. Mbelli, T.M., Dwolatzky, B.: Cyber security, a threat to cyber banking in South Africa: an approach to network and application security. In: 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 1–6 (2016). https://doi.org/10.1109/CSCloud.2016.18
20. Mistry, D.: Banks with Their Feet on the Ground Should Have Their Heads in the Cloud. International Banker (2019). https://internationalbanker.com/technology/banks-with-their-feet-on-the-ground-should-have-their-heads-in-the-cloud/
21. Moloi, Tankiso, Iredele, Oluwamayowa Olalekan: Risk management in the digital era: the case of nigerian banks. In: George, Babu, Paul, Justin (eds.) Digital Transformation in Business and Society, pp. 229–246. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-08277-2_14
22. Pattinson, Malcolm., Butavicius, Marcus., Parsons, Kathryn., McCormac, Agata, Calic, Dragana: Managing information security awareness at an australian bank: a comparative study. Inf. Comput. Secur. **25**(2), 181–189 (2017). https://doi.org/10.1108/ICS-03-2017-0017
23. Phillips, Aaron L.: Treasury management: job responsibilities, curricular development, and research opportunities. Financ. Manage. **26**(3), 69–81 (1997). https://doi.org/10.1111/%28ISSN%291755-053X/issues
24. Polak, P.: Centralization of Treasury Management in a Globalized World. SSRN Scholarly Paper ID 1702687. Rochester, NY: Social Science Research Network (2010). https://papers.ssrn.com/abstract=1702687

25. Ramskogler, Paul: Tracing the origins of the financial crisis. OECD J. Finan. Market Trends **2014**(2), 47–61 (2015). https://doi.org/10.1787/fmt-2014-5js3dqmsl4br
26. Sarkanova, B.: The Impact of Selected Financial Regulations on Corporate Treasury Management. vol. IV. QUAERE 2016 (2016)
27. Schmitz, S.W., Wood, G.: Institutional Change in the Payments System and Monetary Policy. Routledge (2007)
28. Sironi, A.: The evolution of banking regulation since the financial crisis: a critical assessment. SSRN Scholarly Paper ID 3304672. Rochester, NY: Social Science Research Network (2018). https://doi.org/10.2139/ssrn.3304672
29. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. **72**, 212–233 (2018). https://doi.org/10.1016/j.cose.2017.09.001
30. Van Steenis, H.: Future of Finance: Review on the Outlook for the UK Financial System (2019). https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report.pdf?la=en&hash=59CEFAEF01C71AA551E7182262E933A699E952FC
31. Von Solms, J.: (Forthcoming) Digital Technology Adoption in a Bank Treasury and Performing a Digital Maturity Assessment (2020)
32. Von Solms, J., Langerman, J.: A Smart Treasury Fit for the 4th Industrial Revolution. FEMIB 2020 (2020). https://www.insticc.org/node/TechnicalProgram/femib/2020/personDetails/00e65df0-5615-4a51-809b-60a49ef97d3f