International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

The Role of Site Reliability Engineering in Enhancing Customer Trust in Digital Banking Platforms

Riyazuddin Mohammed

Personal Investors Technology
The Vanguard Group, Inc
Malvern, PA, USA.
riazuddiinm0409@gmail.com

Abstract:
Due to the emergence of digital banking, customer interactions with the financial institutions have re-defined what success means, with trust and reliability as the pillars of the process. Disruptions, intrusions, and data breaches have a direct impact on customer trust, and will result in lost revenues and negative publicity. The role of Site Reliability Engineering (SRE) in building customer trust in the online banking systems is explored in this research paper. Google was the first to patent SRE, which is a combination of operations and software engineering to develop some of the most reliable, secure, and scaled systems. SRE (through the use of error budgets, observable events, blameless postmortems, and automated remediation) works on both human trust and technical reliability outcomes. The paper considers how the specificities of the financial industry, such as the strict compliance with the regulations, large amounts of transactions, and the real-time availability can be implemented through SRE practices. The SRE adoption in the traditional banks and fintech companies presented in terms of case studies show that the solutions cut down on downtime and enhanced security, as well as raised the levels of transparency. According to the findings, it appears that SRE is not just an operation type model but a strategic trust-forming mechanism to match engineering performance to the expectations of the customers. The article concludes that with the ever-increasing digitalizing financial role, SRE has to be integrated into digital banking to ensure customer trust over time.

Keywords: Site Reliability Engineering (SRE), Digital Banking, Customer Trust, Financial Technology (FinTech), Banking.

I. INTRODUCTION

Banking is no longer about branch services, but now about digital-first services, where a customer demands to be able to instantly access funds, handle a transaction, and secure themselves to the hilt. In a survey of the banking sector conducted by Accenture on an international level, more than 60% of clients expect mobile applications and internet resources over brick and mortar establishments [1]. This development has opened up possibilities of innovation on the part of the banks yet at the same time increased risks, with just a short cutting off spoiling the trust of the customers.

The two previous banking systems were based on mainframes and legacy IT systems, which showed stability at the expense of flexibility. Banks have become scalable with the use of cloud computing, APIs and micro services, but they have also acquired other system complexity issues, distributed failure point issues and new vulnerabilities to cyber-attacks [2]. These issues reveal the utmost significance of customer trust of the operational resilience and dependability.

Financial services are based on the trust of customers. In contrast to a retail or entertainment platform, where the obstructed service will be inconvenient, in the case of digital banking failure, the loss of access to funds, postponement in activities, or sharing of sensitive information are all possible outcomes. Research has shown that 45% of banking customers would change the service provider in case there are two major service failures [3].

Where digital banks and Fintech are concerned, trust is not merely a social agreement, but a quantifiable engineering value proving to directly influence customer loyalty and brand trustworthiness, as well as complying with regulations [4].

Site Reliability Engineering (SRE) which was initially pioneered by Google in the early 2000s views operations as a software engineering problem by incorporating concepts of automation, monitoring, resilience, and continuous improvement into the operations of systems. In its simplest form, SRE puts an emphasis on quantifiable objectives in the form of Service Level Objectives (SLOs) and Service Level Indicators (SLIs), which specify and evaluate system performance. It also brings in the notion of error budgets which enable teams to strike a balance between innovation and reliability by establishing controlled limits to failure toleration rates. The other pillar of SRE is to minimize toil, the manual, repetitive, operational work by automation, and allow engineers to concentrate on tasks of greater value. SRE fosters a culture of learning when an incident happens with blameless postmortems where the mistakes are seen as a chance to make things better and not blame them. In addition to these practices, chaos engineering is used to actively test the resilience of the systems facilitating the simulation of failures in controlled settings. These practices become particularly important in the framework of digital banking because this area directly promotes the confidence of the customers in the bank since the availability of the services is high, the integrity of the data is guaranteed, the security compliance is also adhered to, and the process of the incidents management is transparent and open.

II. PROBLEM STATEMENT

Although banks have invested significant resources in the digital transformation process, most of them experience massive outages and the consequent loss of customer trust. A typical example is the high-profile failure in handling an IT migration of TSB Bank issued in 2018, which had left the bank in a situation where it had no way of accessing their account over weeks without the ability to fix the situation. Besides the immeasurable frustration, the disruption brought the bank the regulatory fines and compensation claims of more than 330 million, which caused the disruption severe harm to the bank image. Such an eventuality underscores the quality of its inherent fundamental weakness, where traditional IT operations that would have been considered normal in the old days cannot think big, large and self-independent of the scope, complexities and dependencies of the new digital banking systems.

The financial institutions will have the task trying to find the way to make trust visible and sustainable that they will practice systematic and recurring engineering practice. Its customers desire around-the-clock access, secure dealings and seamless online convenient, but in order to deliver them, more than conventional patterns of operation are required. Site Reliability Engineering (SRE) fits very well sometime here. The SRE approach of reliability as engineering problem provides a systematic method of improving consistency, limiting hazard parameters and predictable service execution. In the example of the banking industry it is not possible to introduce SRE as the transfer of the technology to such corporations like Google. It will inevitably be carefully diluted to serve the special requirements of a very constrained, risk-averse context, in which compliance, security, and accountability become pertinent as the availability and performances of systems.

III. RESEARCH OBJECTIVE AND SCOPE OF THE RESEARCH

This study aims to:

1. Improve the availability and reliability of digital banking by examining the impact of SRE Principles
2. Review the role of SRE security, compliance and transparency.
3. Find out how the metrics on SRE (SLOs, MTTR, error budgets) can be connected to customer trust perception.

This essay has been paying attention to the deposit banking products, such as mobile applications, web portals, and application programming interfaces (APIs), which have taken the main frontline where communication is done between a customer and a financial institution. These platforms are now the opening to the digital door of the modern banking business, and the reliability, availability, and smooth performance of such a platform become directly related to customer trust and satisfaction. In discussing the use of Site Reliability Engineering (SRE), the paper evaluates established banks, undergoing the process of legacy infrastructure modernization, and cloud Fintech firms, which are establishing digital-first platforms by means of ground-up construction. Such a twin-fold approach gives a holistic approach on the integration of the reliability practices in the spectrum of the financial institutions.

Although the study has a global focus, the majority of the case studies and examples used are based on the European, North American and Asian banking systems since these areas depict the highest evident and developed incorporation of SRE principles in financial services. The markets have been pioneering in realizing the concept of reliability as a strategic source of differentiation based on its high customer expectations, regulation factors and strong competition caused by it, due to Fintech disruptors. The results, in its turn, are particularly relevant to those institutions that operate in a similar digital setting where the central role in gaining trust with the customers will be played by SRE practices.

IV. FOUNDATIONS OF SRE AND TRUST IN DIGITAL BANKING

A. Principles of Site Reliability Engineering (SRE)

Site Reliability Engineering (SRE) is a field that was first invented at Google to cope with the issues of ensuring reliability of distributed systems on large scale. In its simplest form, SRE aims at making sure that the contemporary software systems are resilient, scalable, and efficient even in unplanned circumstances. Unlike the classical IT operation that is more of a manual operation, SRE organizes the operation as an engineering task, conforming to both software development and operations practice. The change assists the organizations to be focused on automation, proactive monitoring and controlled failure tolerance rather than using reactivity in troubleshooting only and manual intervention.

SRE has a range of principles that define the approach. Service Level Indicators (SLIs) are the metrics that show the quality of service i.e. system latency, service availability, or service error rates. Service Level Objectives (SLOs) are based upon this and they reflect the desired performance of these indicators. One such case is a bank which can establish an SLO which its mobile banking application has to be in the air 99.99% of the time, such that customers can have access to their bank accounts most of the time. The other important concept is the error budgets that, it determines the acceptable limits of unreliability. A small margin of failure can be used to curb the reliability against innovation dilemma where the development teams will be able to make quantifiable risk assessment without compromising the reliability of regular passengers.

Automation and monitoring are the premises of SRE practices. Automated testing, deployment circles and observability means that human error is minimized and can increase user demand on the system. Mistake studies are carried out by postmortem in case of failures by blameless analyses. Its reviews never aim at

other individuals; they facilitate transparency and education, in addition to continuous enhancement, that increases organizational measurability.
The principles are even more important in regard to digital banking. The account management and real-time transactions service as well as account authentication cannot simply be available and responsive but also resistant to cyberattacks, as well as stable when it comes to unexpected order surges. Banks can inculcate trust through an application of concepts of SRE and the services the customers face in an increasingly digital-first financial system have predictable performance, compliance, and reliability.

B. Challenges in Digital Banking Platforms

Digital banking is being implemented in the environment when reliability and trust are not only welcomed but also required. High availability does not compromise as a result since customers seek to reach their accounts and services at any time of the day. A less than temporary crunch would result in reputational costs, money side cost and loss of faith in the company among the customers. Along with availability, banks must survive within the closely managed regulatory environments, and fulfill the standards of such requirements as PCI DSS, GDPR and Basel III, and simultaneously they are crusading off an ever-growing list of cyber threats. The needs are fulfilled with the help of properly designed technical systems and intense operational practices [7].

In the meantime, the fast digital transformation [8] is transforming the banking services. The move towards the mobil-first platform and the use of artificial intelligence on custom experiences offers new opportunities and introduces an overwhelming level of complexity to pre-existing complex systems. These kinds of developments have the disposition of creating a platform that is fearful to breaking down causing the threat of a breakdown or sluggish performance. In addition, the customer expectations are ever rising. It is also demanded by the users that the communications of the site are swift, direct and transparent, such that even the occasions when transactions are not processed or interfaces loaded rather fast spoil trust. Such failures are particularly detrimental in the financial services industry, where the customers need to count on the trust and safety as the primary Keystones of the customer relationship [9].

What is even worse is that the banking system in the contemporary world is difficult to operate. The institutions are forced to contend with the integration of the latter systems into the cloud platform and, third-party APIs, and electronic payment networks. The spots of integration are all possibilities of vulnerability, or failure point, and hence resiliency engineering is a requirement [10].

The issues demonstrate why it is important to implement the concepts of Site Reliability Engineering (SRE) to the banking industry. By incorporating dependability into the design and workflow of digital services, SRE helps banks to address any possible risks in a proactive way, meet the regulations and deliver consistent performance. Last but not the least, SRE enables financial institutions to achieve reliability as a competitive advantage that will enable retention of the customers and remain competitive in a technologically volatile digital setting [11].

C. Trust Dimensions in Digital Banking

Digital banking sites also have difficulties that require reliability and trust of the clientele to prosper. There should be 24/7 banking services contrary to other fields because the customers would want to have access to their accounts and their financial systems 24/7 and with immediate access. Any form of disruption was however minor would result in huge reputational damage, loss of funds and customer dissatisfaction. In addition to access, the system should also include some of the strictest requirements assuming that banks adhere to such regimes as PCI DSS, GDPR, and Basel and the ability to defend against increasingly advanced cyberattacks [12]. That is why even reliability is a technical requirement, but a regulatory and reputational requirement due to this type of conflict between compliance and security.

It is complicated by the fact that this motivation of fast-digital transformation prompts the collaboration of various companies to appeal to international audiences. In the light of the introduction of mobile-first and personalization, which operates with the assistance of artificial intelligence, banks must act swiftly [13]. As much as such innovations can enhance customer experiences, there is also weakness associated with introducing them on board yet to already complicated systems. In the meantime, customer demands are on the rise. Customers now desire a user interface of smoothing and open digital communication that is instant, without delays and even the slightest non-responsiveness in processing or loading one will damage confidence [14]. There are more severe consequences of such lapses in financial services where trust is built based on the reliability and security compared to average other fields.

The digital bank systems are voluminous and can incorporate laggard infrastructure and the current cloud-based infrastructure and third-party APIs [15]. Each point of connection forms the risk of failure or performance difficulties, and as with resilience, it is always a challenge. It is here that Site Reliability engineering (SRE) comes in with great assistance. SRE ensures that banks are resilient and offer confidence to the banks by devising systems that help facilitate power to deal with risk and meet the necessary standards besides offer dependable performance providing that the service is regular. By so doing, SRE will change reliability into a proactive approach, rather than a reactive aspect, that would allow banks to remain trustful and competitive in a fast-paced digital environment [16].

D. Interplay Between SRE and Customer Trust

This ability of the SRE and customer trust to go hand in hand relates to the similarity of operational excellence and user expectations. For example:

- The direct relationship with customer expectations of reliability relates approximately by meeting SLOs.
- Error budgets would make sure that banks are innovative without compromising reliability levels so as to strike a balance between contemporary and trust.
- Monitoring and automation minimise the number of incidents, and postmortems help improve the level of transparency both to boost trust.
- This resiliency engineering via redundancy, and chaos testing informs customers that the system is resilient to any adverse events.

In a sense, SRE operationalises trust as it attempts to turn customer expectations (in their abstract form) into engineering objectives.

V. REAL-WORLD APPLICATION OF SRE IN DIGITAL BANKING

A. Implementing SRE in Banking Environments

Although SRE began in the technology industry, its application in banking needs to be contextually adapted because of regulation, security and customer-focus constraints. Banks are already in a risky environment where services are not only prone to failure but also inspections by the authorities and damages to the reputation of the bank [13]. Hence, the practice of introducing SRE includes adjusting the practices that include:

- Monitoring that is Regulatory Controlled: Systems based on observability should be connected with compliance reporting to comply with audits conducted by the regulators such as FCA, SEC, or Basel committees [14].
- Auto Response: Automated rollback systems, failover switching and disaster recovery should systematically satisfy advanced financial industry resilience specifications [15].

- Data Privacy-Sensitive Techniques: Data monitoring and data-logging should not violate the GDPR or any other data protection laws, and the increase in reliability should never justify the further loss of confidentiality [16].
- Collaboration on Cross-Functionality: SRE practices promote the participation of both the developers, operations teams, compliance authorities and cybersecurity experts to provide reliability and trust [17].

Such modifications would make sure that the banks are able to take full advantage of SRE principles but not violate the regulation or ethical standards.

B. Case Studies in SRE for Banking

1. Monzo Bank (UK)

The largest digital-only challenger banking service, Monzo, is based on cloud-native infrastructure. Using the principles of SRE, Monzo has created:

- Live monitoring of transactions in terms of latency and failure.
- Innovation cycles based on error budgets, finding a tradeoff between introducing new feature and reliability.
- Report Blameless incident reporting, Blacklisting outage reports by publishing them publicly to keep the customers transparent [18].

Being open during down times in Monzo has not only been commended by customers and their regulators, but it has also demonstrated the power of open communication in the face of failure to inspire trust rather than distrust.

2. JPMorgan Chase

Being one of the largest banks in the world, JPMorgan has heavily invested in the modernization of its IT infrastructure on the basis of DevOps and SRE. They emphasize:

- The capability to do hybrid cloud failure over between consulate and the public cloud resilience.
- Anomaly predictive analytics: high-frequency trading systems.
- Logging of compliance that is automated and helps in the minimization of regulatory fines [19].

This has led to a major decrease in the down time, a better regulatory reports and an increase in the customer confidence in the digital products such as Chase Mobile.

3. DBS Bank (Singapore)

DBS bank has positioned itself as a Digital to the core bank, which uses SRE and Devops at scale. Key features include:

- Chaos engineering to exercise resiliency of banking applications to unexpected traffic.
- Between-the-lines/top-down visibility between customer applications and APIs and the back-offs.
- Accountability through SLO, business teams setting goals to have a customer-centric goal related to engineering KPIs [20].

Operational excellence and the possibility to build customer trust through open and trustworthy digital services ranked DBS among the best digital banks in the world.

C. Frameworks for Operational Trust

Customer trust in digital banking built upon Site Reliability Engineering (SRE) can be achieved in many different ways that go beyond ensuring system availability. This involves inclusion of working trust

systems that translate technical dependability and customer facade dependability. Some of the most significant aspects include the adoption of the Zero Trust Security in the context of which every user and communication between various devices and systems is evaluated on an ongoing basis. Reliability is not possible without security in the epoch of a loose cyber environment, and a zero trust model may ensure that the list of customer information and transfers is not violated, and the access to the services may remain uninterrupted.

Customer experience monitoring is important too and it is not available only to technical levels of latency or errors. The indicators of experience level (XLIs) must be added to the banks and, they encompass the degree of success of the logins, the speed of the accomplishment of the purchase, and the receptiveness of the mobile application since they will directly determine how confident the customer is towards the bank. By following through on what matters most to the end users, the banks can be able to identify the issues that do most to diminish trust by effectively handling them.

This is the combination of redundancy, distributed architectures and geo-replication with banking systems so as to ensure that services are not lost in case of failure or when there is a sudden surge in demand. Customers that have been able to gain continuous access even when the back-end has problems tend to have confidence with the bank.

Lastly, ethical transparency is important in the development of trust. In case of outages or incidents, it proves to be accountable, open communication with customers regarding the nature of the problem, the timeframes of its resolution, and what was done right, and trustworthy, even in unfavorable conditions.

Along with the frameworks, the technical resilience of the engineering work is changed into the fulfilled customer benefit, which grants the fix to the discrepancy between the technical and the perception of reliability. With security grouping, experience-based base monitoring, resilient-based design, and explicit interaction, SRE enables digital banks to turn trust into a practical concept in a manner that their customers not only trust their services, but they are comfortable with them.

D. The Trust Dividend in Banking

Then those banks successful in applying Site Reliability Engineering (SRE) practices gain what can be called a trust dividend, a cascade of tangible and intangible benefits going far beyond the level of technical performance. Among the short-term impacts, one can mention the improved customer retention. During the digital age, it is simple to change banks and consumers will not be afraid of transferring to rivals in case they have frequent outages or unreliable services. Banks improve loyalty and create a long-term relationship with their clients through the provision of uninterrupted and uninterrupted digital experiences. The other great advantage is lesser regulatory fines. Financial institutions are highly regulated and failure of systems can easily result in violation of regulation. Banks can reduce these risks by exploiting high observability, continuous observation and compliance conscious reliability practices so that in addition to meeting technical standards, legal requirements are also satisfied. Not only does this save them the tonnes of fines but it also empower them with the officials controlling and other interested parties.

Competitive advantage is the other crucial outcome of an effective implementation of SRE. The majority of the online-only banks, which are typically competing to the existing incumbents, state their superior uptime and open nature of their functioning as the common advantage in the market. The concept of operational excellence is one of the factors utilized in positioning the market as clients are becoming more and more circumspect of the providers who are not only innovative, but also reliable.

The other effect that is highly imperative is the brand reputation. Operation reliability, is a reputational capital in an industry where confidence and trust are a crucial factor. Banks which are able to perform their services with an accurate and strong way instil a strong reputation of reliability that is translated into broader assurance amongst customers, investor and partners among others.

Lastly, SRE is not about the availability of systems or even indicators of performance. It enhances social contract between the banks and the customers by ensuring that banks are trustworthy, answerable and that there are transparency. It is one of the most significant assets that a financial institution can be likely to build under the modern digital economy setting.

VI. RESULTS AND DISCUSSION

A. Literature and Industry Empirical Findings

As it has turned out, application of the notion of Site Reliability Engineering (SRE) to the architecture of digital banking brings the clarified and quantifiable value of the nature of reliability, security, and trust among the customers. The research and industry reports have reported that in case banks adopt the principles of SRE, high rates of service availability are always available and normally the uptime rates are in the range of above 99.95. This is unlike the outdated IT operations where availability is less than a 99.5 percent will actually result in more noticeable disruption to the customer.

The other significant improvement is the incident response. The automation and advanced monitoring and observability tools enable the banks to detect and resolve the issues at a much faster rate. An indicator such as mean time to detect (MTTD) and mean time to resolve (MTTR) has been shown to enhance the rates up to 40 per cent in eliminating the impact of a service interruption and to recover customer trust in an efficiency that is more efficient.

The other advantage of SRE implementation is transparency. Monzo, a digital-first bank that acts to make incidental reports and recoverys publicly available to the clients, has seen fewer complaints in case the bank KS encountered an outage than managing similar in other cases, for which no reports were relayed to the client. The culture of open and proper communication enhances the responsibility and helps to continue the trust even in the circumstances of inevitable inconveniences.

In addition to this, SRE operations increase the levels of regulatory alignment through harmonizing compliance with everyday operations. It minimizes the possibility of an audit violation and fines and ensures the technical reliability of banks and their adherence to the law.

Taken together, these results demonstrate that SRE does not bring only technical performance. It aids in maintaining the standards of customer trust which are dependability, transparency and accountability directly and hence serves as a significant framework to the modern digital bank. These values can be applied to all operations of the financial institutions who are struggling to provide services at a better scale, and also gaining trust over time in an increasingly competitive digital world.

B. The Trust-Performance Nexus

The digital banking is weak in the aspect of customer trust that is directly related to service performance on day to day basis. The findings of the research report that reliability transparency and automation play a direct role in establishing that trust. The customers interpret the stability of the services as a competence and in most cases they associate technical stability with the economic stability. This is particularly true when it comes to those banks, which are digital-only where the platform itself constitutes the primary icon of the trustworthiness of the enterprise.

An openness also contributes to building trust. Whenever failure takes place with the banks being communicative with customers, the latter are more positive about it. Immediate information concerning the incidents, clarifying of the root causes and describes the corrective measures would enable to maintain the trust and develops a loyal relationship in the long-term. Real-life experience of Monzo where detailed reports of outages are published demonstrates that aggressive communication may transform what can be considered as a crisis opportunity to build stronger relationships with customers.

It is also the automation which counts in ceasing customer mistrust. The proactive system of monitoring, detection and recovery eliminates human intervention in order to reduce the likelihood of human error thus creating efficiency in reliability of the services. Besides the technical benefits, automation serves as a pointer of organizational maturity and therefore, sends information to both the customers and regulators to show that the bank is committed towards good forward-looking operating behaviors.

All these evidence that it is not the implicit inclusion of the systems that are operational that leads to the creation of the confidence in digital banking. Instead, it is clearly developed where such practices are included like Site Reliability Engineering (SRE). With the introduction of reliability, transparency, and automatization of its work, banks are able to actively establish a new base of trust that will enhance the stability of customer relationships and assist in overcoming competition in the digital economy in the long-term perspectives.

C. Trade-Offs in SRE Adoption

Although the advantages of Site Reliability Engineering (SRE) are self-evident, the application of Site Reliability Engineering to digital banking is also linked to the trade-offs that should be mulcted over. One of the biggest problems is to strike a balance between innovation and reliability. Error budgets are designed to take calculated risks, but taking it too far and risking systems by neglecting to employ adequate safety would lead to the destruction of customer confidence and stability.

The alternative trade between supervision and automation. In as much as automation is central in the removal of human error and the improvement in efficiency, its excessive implementation can give rise to what can be referred to as black box systems in the loss of responsibility when the process goes wrong. The banks must ensure that the automated processes are lucrative and visible in order to retain the trust as well as the regulatory compliance.

The issue of price is very crucial also. SRE attributes lead to huge investment in infrastructure, redundancy, excessive levels of monitoring equipment and a high level of specialized engineering skills. These act as a prohibitive expense on the minor banks. These expenses however would tend to recoup themselves in the long term as they are normally used to cushion against the regulatory fines, enhance reliability and offer what can be named as a trust dividend in the form of greater customer loyalty.

And finally, it has risks of transparency. Even though the transparency in the event of outages or occurrences is a good communication, the disclosures that were not dealt with appropriately can destroy the reputation instead of protecting it. The banks should come up with the ideal balance of being open to failures yet offer an element of hope and demonstrate that they can manage recovery operations.

The presence of these trade-offs shows that SRE cannot be the process of adoption of financial services in all cases. Instead the banks must carefully tailor the way they take the routes based on the situations of operation; the regulation environment and what their customers expect them to provide so that there is increased trust through the same but without subjecting the bank through unnecessary risks.

D. Comparative Insights: Banks with and without SRE Practices

Comparing industries, one cannot avoid noticing clear differences:

- Banks (e.g. Monzo, DBS, JPMorgan): These have a high level of reliability, higher rates of announcement in their incidents, are very commanding, and their brand is appreciated as a differentiator of their offer.
- Banks without SRE (smaller regional or traditional banks): Banks have higher downtime rates, and their level of communication with customers is low upon outages, and depresses digital trust perception.

The above comparative understanding ratifies the fact that the concept of SRE is not an option in contemporary digital banking rather it is strategic.

E. Broader Implications for the Banking Sector

The findings reveal that Site Reliability engineering (SRE) is changing reliability beyond being a component of technical norm to a corporate property. The critical distinction in the situation with digital banking is trust, as the client can be subjected to minimal switching costs and high demand is always

found in quality experience delivery. There is no doubt the banks that build such trust through trustworthiness will obviously gain in various cases.

First of all, the trust which is attained as a result of reliability influences customer retention and growth directly. By having reliable service which would not fail, chances of keeping the customers are high and the lifetime value and relationship of the customers increases. Second, a market pie has an upper hand with regards to operational excellence. Good message of competent bank will be to be a stable and reliable bank and this will be attractive to digitally inclined customers who may be more keen to smooth and reliable financial services.

There is also proactive resilience by banks in which regulatory positioning is better. Based on its incorporation of SRE practices in the operations, the institutions are more aligned with the standards of the international assignments such as the operational resilience framework as outlined by the Basel Committee. This reduces risks of fines that the regulator may look to impose besides increasing confidence to the supervisors and stakeholders.

Lastly, SRE will assist banks to overcome survival following technical failure. They can create trust into their system and processes designs and hence they are prepared to contest in the dynamic electronic market. Trust-by-design will not only provide a defensive barrier against outages but also act as a forward looking approach that will set the banks apart in an increasingly active financial ecosystem.

VII.CONCLUSION AND FUTURE DIRECTIONS

A. Conclusion

The paper has thoroughly examined how reliability, resilience, and transparency as an area of study contribute to customer trust in digital banking platforms, as sometimes viewed as being just technical goals, reliability, resilience, and transparency are fundamentally used to create trust in financial services. Customers in the age of digital banking are no longer drawn to the interactions with the bank in the form of visiting the branch or receiving in-person assurances, instead, they depend on the performance, availability, and security of the system that forms their trust. This paper demonstrated that SRE activity types like the definition and enforcement of Service Level Indicators (SLIs), Service Level Objectives (SLOs), and error budgets are bringing reliability to life in a way that is quantifiable, enforceable and customer oriented quality assurance [1]. In this manner, the banks will be able to transfer the abstract concept of reliability to reality engineering objectives that will directly influence the customer trust. Also, the level of transparency became one of the keystones of the new trust-building because such transparency features as blameless postmortems, incident publication, and open communication in the event of an outage solidified trust, in spite of the cases when service issues went on. Rather than mistrust, well-handled incidents have the potential of strengthening relationship due to accountability and progressive improvement portrayed.

Another issue that was identified during the review is that operational excellence has proven to be reputational to banks. The case studies of Monzo, DBS, and JPMorgan have demonstrated that resilience and reliability are now differentiators in the market, but not the necessary technical properties. In the Darwin of battle, where digital-first banks take on long-established rivals, great reliability and capacity to quickly recuperate in the number of any malfunction has become a key determinant in customer attachment. Furthermore, it is important that the research was devoted to the manner in which SRE balances innovation and risk. Institutions can use error budgets to seek innovation one day and implement new functionality without compromising reliability of the base. This assists in compromising the common trade-off between high rate of innovation and the steadiness of the service level in such a way that the alteration of the service do not occur at the expense of the customer trust.

Besides this, the regulatory facet of reliability was brought out in the paper.

In addition to this, the paper highlighted the regulatory aspect of reliability. The harmonization of SRE frameworks with regulatory principles on a worldwide level including the principles of operational resilience, proposed by the Basel Committee, will guarantee compliance alongside the principles observed

by banks in terms of customer expectations [6]. Such comeliness between technical reliability and regulatory trust enhance the generality of the ecosystem, so reliability is not only an internal engineering objective but also the responsibility of the people. The implementation of compliance based observability by the banks will enhance both trust by customers and institutions. However, there are still restrictions. There is minimal publicly available data about the application of SRE in banking, and it is hard to determine the maturity of SRE application in the sector. The case studies are also threatened by bias because it has only been successful companies funded by such large amounts of money and might not reflect the real life of smaller banks with small levels of funds. Furthermore, the metrics of technical reliability are well defined but the literature shows that there are no strong models of customer-perceived trust direct measurement, which implies a research gap that should be addressed in future research.

The combination of the findings supports the conclusion that it is impossible to dispel the trust in digital banking without the reliability of the system. SRE offers the roadmap to introduce reliability and transparency within the organizational and technical structure of a digital banking company.

B. Future Recommendation

Site Reliability engineering (SRE) is an architecture that will be exponentially growing in the banking industry in the future because of the algorithm in technology, the growing demands by the customers, and also the more complex regulations. One of the most exciting ones is the introduction of artificial intelligence (AI) and machine learning to the world of reliability. With regards to the benefits of AI-based SRE, banks can change the decision making process to predictive monitoring or put differently, the potential anomalies will be detected prior to the interruption of network transactions and, consequently, the involved one can be prevented. Such forewarned to anticipative resilience modification would be employed to minimize the outburst and deliver near-enduring dependability that enriches consumer confidence. However, having engaged into the procedure of implementing AI into observability pipelines, one will be required to be highly careful with the concept of transparency and explain ability as an assurance of passing ever the regulations and ethics appeals.

The other notable direction is the reliability measures developing customer orientation. The classic SRE models put emphasis on the engineering metrics of the latency, availability, and throughput, but they do not necessarily reflect the real customer experience. The gap that will be dealt with by new theories is the Experience Level Indicators (XLIs) that will be used to measure the following variables: the rate of successfulness of logins, time taken to complete a transaction or customer satisfaction, which followed an outage. This would render XLIs more noticeable and involuntary by bringing the operation priorities near what the customers appreciate most, hence integration of XLIs in the SRE practices would help the banks to set their priorities straight.

The hardiness of cybersecurity is also getting to be a matter of concern. As the level of threats increases, SRE will be forced to approach security practices, in particular, the Zero Trust models. With total integration of security in the reliability practice, the banks will be in a position to extend protection to their customers against both not only down time, but also cyber incursions, which shall earn the confidence of the customers on two critical fronts.

Meanwhile, it is the challenge of international banks to have an encounter with numerous regulations in different regions. The future Sundown SRE architectures must be adaptable to accommodate various standards such as GDPR in Europe, OCC in the U.S. or MAS in Singapore and be dependable across the globe.

Finally, quantum computing has some long-term dangers particularly on cryptographic security. SRE will also need to evolve into quantum-safe resiliency to have post-quantum cryptography protocols, as part of monitoring, recovery and reliability planning.

In conclusion, the future of SRE in digital banking will be concerned with pressing technical reliability to new levels of trust resilience in the holistic meaning. Reliability is a strategic asset that the banks can achieve with the help of AI to become curse-centric, improve the level of cybersecurity, confront the rules

worldwide, and be prepared to withstand the quantum risks. This way, SRE will remain the basis of innovation, compliance, and long-term customer confidence in the digital era.

REFERENCES:

1. Accenture, "Banking On Trust: Enhancing Customer Confidence In Digital Banking," Accenture Research Report, 2021.
2. T. Limoncelli, S. R. Basile, And C. J. Hogan, The Practice Of Cloud System Administration: Designing And Operating Large Distributed Systems. Addison-Wesley, 2014.
3. Deloitte, "2022 Global Digital Banking Survey: Winning And Retaining Trust," Deloitte Insights, 2022.
4. A. L. Mcknight And C. Chervany, "The Meanings Of Trust," Misrc Working Paper Series, University Of Minnesota, Wp 96-04, 1996.
5. B. Beyer, C. Jones, J. Petoff, And N. R. Murphy, Site Reliability Engineering: How Google Runs Production Systems. Sebastopol, Ca: O'reilly Media, 2016.
6. Bbc News, "Tsb Bank Faces It Meltdown," Bbc Business, Apr. 2018. [Online]. Available: Https://Www.Bbc.Com/News/Business-43907382
7. B. Beyer, C. Jones, J. Petoff, And N. Murphy, Site Reliability Engineering: How Google Runs Production Systems. O'reilly Media, 2016.
8. J. L. Fisher, "Defining Slis And Slos For Modern Services," Ieee Internet Computing, Vol. 24, No. 6, Pp. 46–53, 2020.
9. P. Garraghan Et Al., "Reliability In Cloud-Scale Systems: A Survey," Acm Computing Surveys, Vol. 53, No. 1, Pp. 1–37, 2021.
10. N. Murphy And B. Beyer, The Site Reliability Workbook. O'reilly Media, 2018.
11. L. Hochstein, "Automating Operations In Financial Services," Journal Of Financial Innovation, Vol. 12, No. 3, Pp. 112–124, 2021
12. J. Allspaw, "Blameless Postmortems And A Just Culture," Communications Of The Acm, Vol. 62, No. 6, Pp. 48–54, 2019.
13. B. Beyer, C. Jones, J. Petoff, And N. Murphy, Site Reliability Engineering: How Google Runs Production Systems. O'reilly Media, 2016.
14. Basel Committee On Banking Supervision, "Principles For Operational Resilience," Bank For International Settlements, 2021.
15. A. Jain And V. Kumar, "Ensuring High Availability In Financial It Infrastructure," Ieee Trans. Eng. Manage., Vol. 68, No. 4, Pp. 987–995, 2021.
16. R. Stallings, Information Security For Financial Institutions. Crc Press, 2020.
17. N. Murphy And B. Beyer, The Site Reliability Workbook. O'reilly Media, 2018.
18. Monzo Bank, "Monzo Status And Incident Reports," [Online]. Available: Https://Monzo.Statuspage.Io/.
19. Jpmorgan Chase, "Technology Modernization Initiatives," Annual Report, 2022.
20. Dbs Bank, "Digital Transformation Journey," Dbs Insights, 2021.
21. R. Stallings, Information Security For Financial Institutions. Crc Press, 2020.