Aite PARTNER. ADVISOR. CATALYST.

Modernize to Digitize: Three Challenges for Banks to Overcome

MAY 2018

Prepared for:

avanade

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

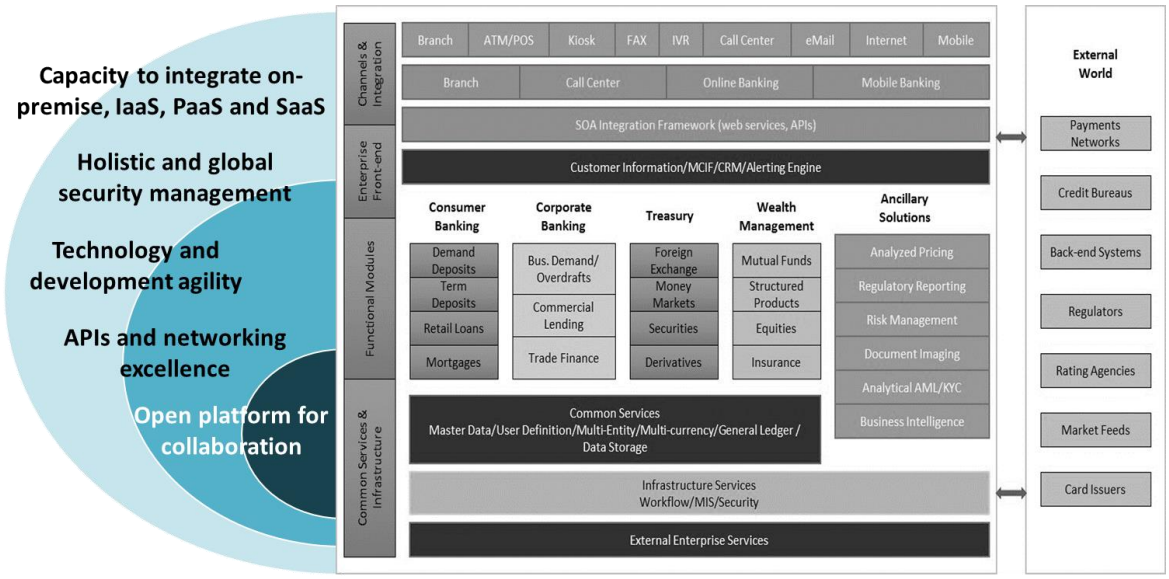
Modernize to Digitize: Three Challenges for Banks to Overcome, commissioned by Avanade and produced by Aite Group, explores what banks should consider while striving to modernize their IT and better respond to digital business demands. This white paper explores what banks must do to truly modernize and become **fit for digital**:

- **Reduce risk**. Legacy technology means a higher exposure to risk, especially due to extensive and unique levels of customization and the declining lack of knowledge within the business as to how such complex systems work. This is particularly the case in the areas of operational risk and security.
- **Increase agility.** Banks need to be more responsive to changing market conditions and digital demands from the business. Setting up their third-party networks to increase innovation will be particularly effective. Banks need to gain more expertise in agile development and operations (DevOps) skills as well as to leverage the opportunities presented by application programming interface (API) management.
- **Generate insights.** Banks need to cope with increasing amounts of data in a variety of formats. An effective data management approach is essential to delivering compelling insights at scale. Banks should leverage regulations such as General Data Protection Regulation (GDPR, which is starting in Europe but is rapidly expanding globally) as an opportunity to fund technology that will enable deeper customer understanding.

REDUCE RISK

Most bank architectures consist of a mix of technology types as a result of banks building their own solutions, merging with and acquiring other firms, and failing to replace and upgrade a multitude of vendor-built solutions and components. It is common to find many disparate legacy systems in place, leading to multiple risks—in particular, operational and security risks (Figure 1).

Figure 1: Hybrid Banking Environment as a Result of Legacy Technology



Source: Aite Group

HANDLING OPERATIONAL RISKS

As a growing number of banks look to re-evaluate their technology strategies and determine whether their service offerings remain aligned with the rapidly growing digital environment, they have to address the following operational risks associated with legacy systems:

- **Lack of flexibility:** One of the key issues with a legacy system is that it does not provide the flexibility required to carry out day-to-day tasks and to change how the system works when business needs change.
- **Lack of IT resources and dependency on a diminishing set of individuals:** Legacy systems often require specific IT skills, mostly in older or obsolete programming languages. Typically, legacy solutions incorporate extensive and unique customization, and the employees who have managed these customizations are the

only people who understand the complexity of the system. Supporting the legacy applications therefore becomes increasingly difficult.

- **System downtime:** One of the biggest operational challenges associated with legacy technologies is handling the downtime needed by these systems. Planning for the ideal time slot in today's global real-time business environment (and ensuring prompt recovery for mission-critical systems) is challenging.
- **Incremental updates:** Incremental changes to legacy systems often require code changes and even workarounds, which in turn require significant regression testing to ensure compatibility and reliability.

Many of these operational risks can be either completely resolved or at least mitigated by migrating to a modernized IT base (Table A).

Table A: Solving Operational Risks by Migrating to Modernized IT

	Legacy and conventional banking	Modernized IT
Architecture	20- to 40-year-old technology	Industry standards
	COBOL	Java, .NET, Visual Basic
	Mainframe-dependent	Flexible and open
	Monolithic applications	Cloud-based
	Hardware-dependent	Software based (such as software-defined networking)
Development	Heavy customizations to meet specific banking requirements	Extensive use of parameters and large number of configuration options
	Highly inflexible	Minimal need for customizations
	Substantial regression testing needed	Incremental testing only
	Uncompetitive time to market (long lead times and high costs)	Speed to market for new products meets business objectives
	Waterfall as the preferred development method	Agile as the preferred development method
Customer view	Account-centric architecture	Native 360-degree customer views
	Fragmented and siloed transactional data	Total view of accounts and services
	Additional software layer needed for single customer view	Enterprise customer relationship management (CRM) capabilities and referral tracking

	Legacy and conventional banking	Modernized IT
Operations	Separate systems for deposits and loans Separate name and address files Reactive cross-selling IT-driven organizational alignment Basic reporting	Single system for deposits and loans Integrated name and address file Proactive cross-selling Business-driven organizational alignment Advanced analytics and business intelligence
Support	Limited vendor support Diminishing pool of resources	Extensive vendor support Readily available pool of resources
Processing	Batch	Real time
Deployment	Thick client	Virtual environments, smart browser-based client, and cloud-computing infrastructure
Total cost of ownership	High cost due to extensive support	Lower cost to operate and maintain due to standard software development tools and flexibility

Source: Aite Group

COPING WITH SECURITY

Amid increased data breaches, security has become a paramount concern for all banks. But it's rapidly becoming clear that banks won't be able to shore up their defenses until they tackle the vulnerabilities caused by legacy technology. In a recent survey of over 170 senior U.K. financial crime professionals, respondents cite that legacy systems create specific technological obstacles to fighting financial crime:[1]

- Forty-one percent of respondents say they're worried their legacy systems can't respond in a timely manner to new forms of financial crime as they arise. This is probably because most banking systems in the U.K. were installed between 25 and 40 years ago, and are highly inefficient at processing data in real time. In addition, these systems were designed with much a lower volume of data.
- Fifty-three percent of respondents say they were frustrated by the difficulty with transferring data between their disconnected systems. These siloed systems segregate data according to specific banking divisions, making it hard to derive a higher-level picture, including the bank's own risk profile.

1. "Future Financial Crime Risks 2017," LexisNexis Risk Solutions, accessed May 1, 2018, https://risk.lexisnexis.co.uk/insights-resources/white-paper/future-financial-crime-risks-2017-wp-uk.

- Ninety-two percent of respondents are concerned that their organizations' legacy technology will become an obstacle to combating financial crime in the next two years.

Cybersecurity risk to enterprises is top-of-mind from the C-level down, and with good reason. Escalating attacks by organized crime rings and nation states have resulted in 9.7 billion data records breached in the past five years.[2] Data breach notification laws in various jurisdictions dictate that these breaches are often embarrassingly public and costly. In addition to the expense associated with remediating the breach, the more significant and long-term impacts are often associated with the erosion of brand trust and customer attrition.

Banks that rely on legacy technologies make it easier for cybercriminals to succeed:

- **Patch and vulnerability management is overly complex.** When vulnerabilities are discovered, either in homegrown or vendor-supplied software, they need to be fixed. This process is neither quick nor easy, however, especially when customer-facing applications are involved. On average, it takes over 60 days for a software vulnerability to be fixed from the time it is discovered or the patch is received.[3] Equifax is the poster child for this risk; a midlevel manager at Equifax decided to postpone applying a security patch, resulting in the largest breach of personally identifiable data in U.S. history.[4]

- **Devaluing data is difficult.** With the continued rise of breaches, the acknowledged best practice among firms handling sensitive data is to deploy technologies, such as tokenization and encryption, that devalue the data. Tokenization replaces sensitive data at rest with a proxy value that is used as a surrogate, while encryption protects data in transit. While these technologies are highly effective and increasingly widespread, tokenization in particular is often difficult to deploy within rigid mainframe-based environments. This is another driver for banks to move to more modern technologies that can devalue data.

2. "Breach Level Index," Gemalto, accessed March 12, 2018, http://breachlevelindex.com.

3. "2018 Vulnerability Statistics Report," edgescan, accessed May 2, 2018, https://www.edgescan.com/assets/docs/reports/edgescan-stats-report-2018.pdf.

4. Russel Brandom, "Former Equifax CEO Blames Breach on a Single Person Who Failed to Deploy Patch," The Verge, October 3, 2017, accessed May 2, 2018, https://www.theverge.com/2017/10/3/16410806/equifax-ceo-blame-breach-patch-congress-testimony.

INCREASE AGILITY

To implement new growth strategies, banks must first focus on core transformation and on replacing their legacy systems. In doing so, banks are aiming to easily access real-time, accurate, consolidated global information to achieve cross-selling success and better meet customer demands. Their customers are looking to them to provide easier access to data to enable more accurate forecasting and cash position reports. Here are two typical examples:

- In a 2017 Aite Group survey, one bank IT executive mentioned that his institution has significant integration issues and that its information is not as real-time as he would like it to be because many mainframe systems are more than 10 years old.[5] The bank spends too much money and effort on integration with its core, and lengthy product launch timelines put the bank at a competitive disadvantage.
- Another large global bank blames many of its legacy challenges on mergers and acquisitions, too much internal customization, and past practices of building business processes around system limitations. It is not uncommon for a large global bank to be running multiple core systems simultaneously as well as running multiple instances of each system in different countries.

These factors, coupled with systems that have been in place for more than 30 or 40 years, are holding back many banks from growing, operating efficiently, and meeting new customer and regulatory demands. One approach that banks are taking up in this area is agile development.

GAIN EXPERTISE IN AGILE DEVELOPMENT

Software companies around the world have been utilizing an agile development methodology to incrementally release products that focus on a satisfying customer experience.

According to a 2016 Aite Group survey of treasury management product managers, the benefits of migrating from waterfall to agile development fall predominantly in the following areas:[6]

- **Time to delivery:** Most respondents agree that the use of agile development can improve time to market, with many finding they can now have two to four releases a year, while with waterfall development some of these large complex systems would have annual or biannual releases. “With agile, we are able to adjust what is included in the release; with waterfall, everything is included, and it all has to be defined in the beginning, with no changes,” says one respondent. Time to market is important, because the chances of the release meeting the customer’s expectations are diminished the further away the release is from the gathering of requirements.
- **Quality:** Continual, incremental testing has improved product quality—testing is now a normal daily activity rather than an event. As one respondent comments,

5. See Aite Group’s report *Large Banks and Technology Buying: An Evolving Mindset*, July 2017.
6. See Aite Group’s report *Agile Development From Product Management’s Perspective*, April 2016.

"Sprint cycles showed less defects than average waterfall releases." These incremental sprints allow correction of defects to be completed in weeks, compared to the months it might take with waterfall.

Apart from speed and quality, banks are also looking for flexibility around innovation. API management is a new market driver that offers banks a major opportunity to create a new business model, focused on providing new services for customers.

LEVERAGE API MANAGEMENT

The idea of APIs is not new within the banking industry: They have been used for connecting with vendors for some time. However, banks are now looking for new ways to leverage APIs to deliver and share information within their own organizations, with partners, and even with customers.

To date, banks' API activities are dedicated to regulatory requirements (e.g., Europe's revised Payment Services Directive [PSD2]) or to industry-led initiatives (e.g., U.S. banks' Business Payments Coalition). The PSD2 mandate is forcing banks to share information through APIs. Other drivers for banks to create an API strategy include the ability to build once and use many times and the belief that it will lead to greater operational efficiency across the organization (i.e., common taxonomy, common infrastructure, common security, reusability).

Banks need to assess their role in the overall API ecosystem and champion the development of new products and services. Otherwise, they will be disintermediated from their customers and risk being relegated to providing back-end utilities. API development plans must be part of the bank's strategic agenda, and certainly not limited to the information and technology officers. By infusing API management into their strategic agenda:

- Banks can focus on reacting quickly to increasing customer expectations. APIs provide banks with the flexibility to be able to connect to new systems and new data that can help them react to changing consumer needs for products and services.
- Banks can focus on collaborating with third-party providers to deliver new products and services. Given the large number and variety of new technologies available, banks will be hard-pressed to continue to have the internal skills needed to implement it effectively. APIs open the door for banks to partner with fintech companies and other solution providers to gain access to systems they do not have the in-house experience to build.
- Banks can focus on moving toward a more modernized IT stack. APIs open the door for banks to be able to slowly modernize various components. A phased approach will provide the most flexibility and help move the bank to a modernized IT stack over the next few years.

GENERATE INSIGHTS

The massive explosion in data is creating serious management issues for banks. This is due to expanding customer touch points (with the rapid growth of digital structured and unstructured data associated with new customer engagement platforms and social media) and the real-time data processing that is necessary to provide timely insights and improve decision-making.

IMPLEMENT EFFECTIVE DATA MANAGEMENT TO DELIVER INSIGHTS AT SCALE

Meeting these new data-volume challenges can be costly. Legacy technology involving multiple data warehouses and transactional systems not only adds up to a high total cost of ownership but also is unsustainable in this new environment. Increased regulations and compliance have increased banks' responsibility to maintain data and provide greater transparency to the regulators.

Banks need effective data access standards coupled with a nimble infrastructure built around new delivery models (such as cloud) and the management of unstructured data (using technologies such as Hadoop). With such imperatives in place, banks will be able to shift their focus from dealing with the complexity of data analysis, governance, and distribution to actually harnessing the data and using it to their advantage to deliver compelling insights. A 2017 Aite Group survey of senior fraud and data analytics executives highlights that the vast amount of data now available to inform machine-learning analytics is a key reason for its success. But it is a challenging journey to bring it all together: 55% of the banks interviewed are only using structured data today, while 45% are using both structured and unstructured data. [7]

USE GDPR TO DEVELOP DEEPER CUSTOMER UNDERSTANDING

The European Union has created headlines around the world with the publication in April 2016 of the new GDPR.[8] The regulation became effective on May 25, 2018, and it replaces the Data Protection Directive (adopted back in 1995). It aims to bring EU law in line with the technology revolution that has fundamentally changed data processing and to further harmonize data protection regulation in EU member states. The regulation strengthens the rights of natural persons and introduces new obligations for data processors. It also gives supervisory authorities the means to impose hefty fines for noncompliance. With GDPR, data protection has entered the board room.

GDPR compliance is a major exercise that many companies have not yet completed. The principles do not differ from existing data protection regulations in Europe and abroad. However, the accountability and transparency requirements bring data protection to a new level.

7. See Aite Group's report *Machine Learning: Fraud Is Now a Competitive Issue*, October 2017.

8. This refers to Regulation (EU) 2016/679. See "General Data Protection Regulation," intersoft consulting, accessed April 29, 2018, https://gdpr-info.eu.

Given the global nature of data processing, companies will find GDPR restrictions on data transfers outside of the EU some of the most challenging. Other regulations, such as GDPR, are rapidly expanding globally: Australia and Canada are following suit. GDPR is creating a shift in how companies manage customer identity so that they can facilitate the right to be forgotten and the portability of data. This compliance effort is spurring investments that modernize how banks manage their customer identity data.

Companies should review their processing contracts—not only contracts with external vendors but also relationships with group companies that process personal data on behalf of a customer-facing entity.

Consent is a very important concept in GDPR, and companies will have to rethink their approach to customer consent management. As companies must document what personal data they hold, where the data came from, and with whom the information was shared, they must also indicate the lawful basis for processing that data. Because GDPR raises the bar considerably to obtain customer consent, companies should rely on consent only when no other lawful basis is available to process certain personal data.

Anonymization, pseudonymization, and encryption are important techniques to reduce the risk of disclosure and breach of personal data.

NEXT STEPS

As a growing number of banks look to modernize their IT base in order to respond effectively to digital business demands—"modernize to digitize"—Aite Group recommends the following:

- **Doing nothing is not an option.** Legacy systems increase the level of risk in the business, restrict agility, and limit innovation. They are a major cost in terms of operations and maintenance. Critically, they make it difficult to respond to the digital demands of both the business and your customers.
- **Develop a compelling business case.** This should cover both business and IT benefits resulting from an IT modernization program. This will also drive senior executive sponsorship and provide specific goals for the program. Use cases can be complex to develop, however, and cross-business support is essential. Use independent ROI approaches to validate benefits delivery.
- **Ramp up DevOps and agile ways of working.** These modern software engineering approaches will be critical to helping you deliver the benefits quickly. This will probably require an investment case. Banks have expertise in this area, but it needs to be more widespread.
- **Evaluate your cloud options.** This needs to be tailored to your specific requirements. Many banks are moving to IaaS or performing application migrations to get away from end-of-support platforms. The real value comes when applications are adapted to changing digital business needs and are made more cloud native with higher-level platform services. This dramatically speeds up development time and therefore time to market.
- **Assess your apps portfolio**, but with a view to making legacy apps future-ready and adding net new future-ready apps. Decommission based on business value.
- **Be realistic.** There are operational risks in migrating to a cloud environment. Look for ways to mitigate risk by adopting a phased/incremental migration approach. Consider hybrid options where appropriate. Be honest about what skills you have in-house and where you need external help. Assess your service management and security expertise.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

ABOUT AVANADE

Avanade is the leading provider of innovative digital and cloud-enabling services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation and has 30,000 professionals in 24 countries. Visit us at www.avanade.com

AUTHOR INFORMATION

David Albertazzi
+1.617.398.5036
dalbertazzi@aitegroup.com

Tiffani Montez
+1.617.338.6045
tmontez@aitegroup.com

CONTACT

For more information, please contact:

North America
818 Stewart Street
Suite 400
Seattle, WA 98101
Phone: +1.206.239.5600
America@avanade.com

Europe
30 Cannon Street
London EC4M 6XH
Phone: +44.20.7025.1000
Europe@avanade.com

Growth Markets
250 North Bridge Road
#30-03 Raffles City Tower
Singapore 179101
Phone: +65.6592.2133
AsiaPac@avanade.com

For all press inquiries, please contact:

Avanade PR
Tom Barton
eupress@avanade.com