Core banking resilience

Time to grasp the nettle

How banks can make their core systems fit for purpose

Connected Banking
Connected Banking
Thought Leadership for the UK Banking Industry

Accenture’s UK Banking practice welcomes you to the Connected Banking thought leadership series.

Why Connected Banking?
To fulfil their historical core role, banks have always had to be connected to a wide range of stakeholders. And today more than ever, banks cannot operate in isolation. In a fast-moving and increasingly transparent environment, they are now part of everyday life – and connected to most things people do. To grow and build trust in such an environment, banks must connect in new, more responsive and more seamless ways – not just with customers, employees and other banks, but also with regulators, business providers and society as a whole.

Being a Connected Bank today means change is the norm. This change requires banks to have viable and profitable business models that are constantly enhanced through agile innovation. But as they develop and deliver this innovation, banks must also demonstrate continuously that they are aligned with – and committed to supporting – the interests of the wider economy and society.

Against this background, the Connected Banking series focuses on addressing banks’ challenges in three key dimensions:

The Future of Banking:
The move to Connected Banking will bring new rules, new economics and new customers. In response, banks have to design and create new business and operating models that enable them to connect in a frictionless way.

The Digital Revolution:
The need to connect intimately with the evolving customer requires banks to progress from being ‘utility’ providers of transactional banking services to becoming value-adding partners at the heart of their customers’ everyday digital lives.

Risk & Regulation: A well-connected strategic regulatory response can help banks switch from reactive survival mode to leveraging regulatory change in ways that support profitable growth.

‘Core banking resilience: Time to grasp the nettle’, the latest point of view in the Connected Banking series, focuses on the challenges that banks now face in their underlying core banking architectures – and presents some options for solving these challenges.

What’s next in the Connected Banking publication series?
Over the course of the coming months, we will be issuing points of view addressing different aspects of each of the three key themes identified above.

The recently released publications in the series are:
- Next Generation SME Banking
- Banking 2020
- Turning Switching to your advantage
- The challenge of Regulatory Implementation – a strategic approach
- Preparing for Growth – Banking Chief Financial Officers Look to the Future with Cautious Optimism

The forthcoming publications are:
- Remediation: robust service management
- Evolving the core – bite size chunks
- Replacing the core – game changing
- FATCA
- Tackling the ‘Too Big to Fail’ problem
- UKI Consumer Survey 2014

Contact Us
To find out more about the Connected Banking research, upcoming events or future publications please contact:

Robert Stubbs
Financial Services, Banking Research
+ 442078449845
robert.a.stubbs@accenture.com

Geetika Rai
Financial Services, Marketing
+ 442078445982
geetika.rai@accenture.com
What is the core banking challenge?

As the media and regulators continue to shine a spotlight on service outages among UK banks, the question needs to be asked: ‘What can be done to resolve these problems?’ This paper explores the challenges that banks now face in their underlying core banking architectures – and presents some options for solving these challenges.

Incidents rising in frequency and volume

The rising profile of bank service outages reflects more than just increased public interest. An analysis of news reports confirms that these incidents are also happening more frequently, with banks suffering a growing number of incidents where core systems become unavailable. Figure 1 illustrates the rising volume of reported technology problems experienced by UK banks between 2011 and 2013. For the banks involved – and indeed the industry as a whole – these outages are much more than operational glitches. The severe disruption they cause to customer service and experience can inflict lasting damage on customer perceptions, and can undermine confidence that has taken many years to build up.

Rising scrutiny from regulators

The rising frequency of service outages is attracting growing interest from regulators and other government agencies in connection with the performance and stability of banks’ core systems. This scrutiny is intensified by the recognition that these systems are part of nationally critical infrastructure.

The Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) underlined their concerns in 2012, when they asked all the UK’s top eight banks whether they had similar problems to those that had triggered a major outage at one of their number in June that year. The regulators’ worries were further highlighted in November 2013 by the FCA’s Director of Supervision, Clive Adamson, who commented in a speech to the Institute of Economic Affairs (IEA): ‘We know that trust in banks by consumers is low...and we know that many banks’ IT infrastructure is not sufficiently robust.’

The Parliamentary Commission on Banking Standards has also become involved in the debate, commenting in its conclusions in June 2013 on the benefits of ‘encouraging banks to make much-needed investment into their patchy and outdated in-house IT systems.’ And as recently as January 2014, PRA director Sam Woods told the House of Commons Northern Ireland Affairs Committee: ‘I feel we are a very long way from being able to sit here with confidence and say that the UK banks’ IT systems are robust.’

Figure 1. Reported technology incidents in UK banks’ core systems, 2011–13

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>6</td>
</tr>
<tr>
<td>2012</td>
<td>8</td>
</tr>
<tr>
<td>2013</td>
<td>12</td>
</tr>
</tbody>
</table>

Sources: Factiva, © 2013 Dow Jones & Company, Inc.
What's the problem with core banking systems?

What is ‘core banking’ and what do we mean by ‘resilience’?

These differing perspectives all reflect underlying misgivings over a lack of ‘resilience’ in ‘core banking systems’. A deeper discussion in this paper demands a clear definition of what these terms actually mean.

By ‘core banking systems’, we refer to the systems – both hardware and software – that hold master customer account balances for savings and current accounts; that process the debits and credits and calculate interest and fees; and that then make this information available to customers via a growing array of channels, ranging from branch to phone, internet and mobile services. As Figure 2 shows, these core banking systems do not include the payment systems that connect them.

While core banking systems are central to banks’ service offerings and play a pivotal role in their customers’ experience, these are typically the oldest systems in most banks. In some cases they have been in place for 40 years or longer.

‘Resilience’ has a specific meaning in the context of core banking systems. The concept of resilience is often associated with the ability to spring back, or recover from a shock. This capacity to recover quickly when difficulties occur is certainly important.

However, from the viewpoint of regulators and customers, an arguably more vital aspect of resilience is the ability to avoid difficulties arising in the first place, thereby preventing any loss of availability.

While 99% availability may sound like decent performance, customers (especially those using mobile services) may feel otherwise – and it is only when outages occur that the speed of fully restoring the service becomes an issue.

Experience shows that, when this takes hours or even days, the resulting media coverage and reputational damage can be substantial.

Figure 2. High Level Core Banking Systems Architecture
Why is the resilience issue escalating up the agenda?

Remote and digital banking multiply the pressures

Given that many of today’s core banking systems were originally designed and built for a world that consisted mostly of branch-based banking and overnight batch processing, it’s hardly surprising that they are now coming under strain. The demands on these systems have increased beyond recognition since they were commissioned, with the headlong expansion in real-time channels – ATMs, contact centres, interactive voice response (IVR), internet, mobile – leading to massively increased line volumes.

As Figure 3 illustrates, this growth is showing little sign of slowing down, with real-time payments having roughly doubled since 2004. Over the same time period, we estimate that the impact of new channels has increased balance enquiries by a factor of 10 at least. The way in which today’s core banking systems were originally designed means that coping with these rising volumes is much more than a matter of simply adding new servers, and demands a deeper transformation.

As the pressures on core banking systems continue to intensify, the impacts and implications of failure are also multiplying. In the pre-digital world, a ‘run’ on a bank focused on whether it had enough physical cash in its branches to enable customers to withdraw their money. But today, managing a bank run is no longer about having enough cash, tellers and ATMs – but about having enough capacity to handle vastly increased online traffic.

The queues that formed outside Northern Rock’s branches in September 2007 often consisted of people who had tried and failed to withdraw their savings overnight via the bank’s website, a situation that added to their concerns over its financial stability. And across the industry, the challenge of having enough server capacity to maintain services and confidence has been exacerbated by the ongoing concentration of customers into fewer banks.

---

Figure 3. Real Time Payments Growth

**Volume growth of UK Batch and Real-time Payments to 2013 – Number of Payments (000s) by Type, Quarterly 2004–2013**

<table>
<thead>
<tr>
<th>Year</th>
<th>Batch</th>
<th>Realtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: “Batch” = Standing Orders, BACS Direct Debits & Credits & Cheques / “Real-time” = Faster Payments, CHAPS, Debit & Credit Card Transactions

Source: Payments Council and The UK Cards Association.

* Batch processing is the execution of a series of programs (‘Jobs’) on a computer without the need for manual intervention. Jobs are set up so they can be run to completion without manual intervention generally outside of working hours. An example of batch processing is the way that credit card companies process billing. The bill is created through batch processing, where all of the data is collected and held until the bill is processed as a batch at the end of the billing cycle.*
Layers of complexity

To date, these rising demands on banks’ IT – and the related need to engage customers through new channels – have been met by adding new layers to systems built in the 1960s and 1970s, rather than by replacing them. This has resulted in ever-increasing complexity – a problem compounded by the age of the core technology, which means there are fewer and fewer people who possess both the required technical skills and knowledge of how the systems were built to help them recover from incidents.

This situation means banks seeking to address problems often need people who understand mainframes and batch processing – skills that are now in increasingly short supply. It’s been reported that one recent incident required the recall of an employee who had retired some time ago. And even when banks can bring the required knowledge to bear, the tangled layers of interdependent systems and interfaces make it hard to understand how the various technologies all fit together end-to-end.

This makes it very difficult to prevent bugs by testing all the components and interactions together; to detect bugs by tracing issues through multiple systems; and to recover from bugs when they arise.

In recent years, all these issues have intensified – to the extent that we have even seen bank CEOs admit that ‘decades’ of underinvestment have resulted in ‘unacceptable’ failures.

This historical lack of investment is mainly a reflection of the enormous cost and high risk of failure for the IT programmes required and the personal risk for any CEO or CIO undertaking a multi-year investment of this scale; and the strain on the capital budget required when the existing asset was fully depreciated long ago.

These barriers to IT spending have existed for decades. And, as indicated by former Barclays CEO Martin Taylor in a comment published in the Financial Times on 29 January 2014, IT has historically occupied a paradoxically low status within banking organisations.5

It is important to stress that not all banks are still wrestling with outdated core banking platforms. A significant minority – including some established majors and a handful of new entrants – have invested in making their systems less complex and easier to manage. But while the scale of the challenge varies between banks, improving the resilience of core systems is clearly a priority for the industry as a whole.

Insiders took the computer staff as much for granted as outsiders did.

Martin Taylor, former chief executive of Barclays

For anyone with an understanding of banks' IT systems, none of what we’ve said up to now will come as a surprise. Indeed, much of it has been said every five years or so since the late 1980s, usually by technology vendors seeking new business. Each time, despite the dire warnings, the banks have managed to cope.

So, why are things so different now? For five main reasons.

1. **We’re now in a truly digital world** – Today’s world is one in which customers demand the same real-time, always-available experience from their banks as they get everywhere else in their lives. When their interactions with their banks were limited to the occasional phone call or internet session, it was possible to hide the limitations of the underlying core systems. Now that customers are connected all day through their phones or tablets, it’s impossible to paper over the cracks. Meeting their digital wishes also means that banks need new capabilities in their core systems – the ability to develop and launch new products more quickly (days rather than months) and a much richer set of context data to drive highly tailored interactions.

2. **Many of the people that understand the legacy core systems have already retired** – Today, banks are reaching the endgame in terms of relying on knowledge and support from the generation who built many of these systems. As that generation leaves the workforce, maintaining these systems is becoming ever harder.

3. **Cost pressures demand simplification, not greater complexity** – Banks are under ever greater cost pressures, and can no longer afford the additional costs generated by adding further layers to core systems.

4. **Regulators will not tolerate continued fragility in systems** – Banking regulators are fully aware of the shortcomings in core systems, and are taking a much more direct interest in them than before. This reflects both their mandate to protect the customer, and also the need to improve the resilience of the banking system as a whole as part of the national economic infrastructure.

5. **Some banks have demonstrated that while core banking transformation is difficult, it is not impossible** – Banks’ IT departments should be given credit for their skill and dedication in accommodating so much innovation in channels and products within creaking infrastructures for so long. Until relatively recently, these efforts partly reflected the view that core banking transformation was like changing the engines of a 747 in flight: simply impossible. However, programmes such as Lloyds’ integration of HBOS, Santander’s integration of its UK acquisitions, and Nationwide’s implementation of SAP have now shown that – while expensive and difficult – core banking transformation can be achieved. These projects have given all bank Boards a clearer idea of the practicalities, opportunities and challenges involved.

In combination, these five factors represent a call to action for banks to tackle their core system challenges as a matter of urgency. The question is how.
What are the options?

There are several actions that banks can take – either individually or collectively – to make their core systems fit for the future. In light of the clear need for change, we’ll now examine the pros and cons of each approach.

**Individual actions**

The actions open to individual banks seeking to improve their core systems are summarised in Figure 4. While these approaches are all different, they are not mutually exclusive. We plan to explore each of these in more detail in future papers, and have set out our high-level assessment in Figure 4.

- **Remediating the existing platform** represents the bare minimum that banks must do to stay in the game. Remediation will normally involve both changes to the existing platform and changes to the way the platform is managed. Careful review of the current application and infrastructure architecture can identify weaknesses (e.g. single points of failure) and present opportunities to improve resilience, often by taking advantage of the technological advances made since the original architecture was designed. Improvements to management of the platform include steps to prevent incidents through more proactive monitoring, improved ‘offline’ processing to create operational contingency, more effective change control and testing, more thorough back out plans, better documentation, improved incident management, and enhanced disaster recovery planning and testing.

- **Simplifying core systems through evolutionary transformation** involves a gradual migration to a simpler and more resilient architecture. This is focused on modernising and standardising the layers that have grown up around the original systems. A phased approach should bring the benefit of being less risky than a ‘big bang’ migration, and a number of major banks globally are currently undertaking such projects, with timescales between four and seven years. Success requires maintaining a consistent and disciplined approach across multiple years and, historically, this is something that many banks have found extremely difficult to do.

Figure 4. Possible responses in core systems
Replacement of core systems is a further option, and comes in many forms. The first is the 'classic' approach of wholesale replacement with a new platform, generally through a major implementation of packaged software. However, these are massive projects with costs – and, if things go wrong, massive write-offs – running into hundred of millions of pounds. Even when these are successfully implemented, there will be a period of lower resilience while the platform settles down before improvements are achieved. As a result relatively few COOs, CIOs or Boards have an appetite to undertake them. Nevertheless, there are examples such as Nationwide in the UK and Commonwealth Bank in Australia where this approach has been implemented successfully.

One alternative to replacement with a new platform is migration to an acquirer's platform as a way to replace the legacy core systems. This is less risky because the target platform has been proven, and recent experience in the UK shows this can be achieved successfully. However, competition requirements mean it can only be part of the solution for the industry as a whole.

A more attractive replacement option may be to build a new platform around a new 'bank within a bank'. This enables the bank to start from scratch, unburdened by legacy systems and processes. Risk can be reduced by running the old and new systems in parallel and migrating customers across only when the new platform's functionality and capacity are proven to be sufficient. However, this 'dual running' also adds further cost.

Finally, a bank can outsource its core systems to a third-party provider and pay it to run them as a utility. Many banks in the UK would adopt this approach enthusiastically as it offers a relatively quick and lower-cost migration path. However, the supplier marketplace for core bank outsourcing in the UK is currently relatively small and underdeveloped, especially for any larger players considering taking this route. This is noticeably different from the US where a broad market for mid size banks has allowed a number of providers to develop.

Overall, the easiest decision among all these options is to invest in strengthening the delivery of services from the existing platform. In contrast, the other options all present tough choices.

Could new entrants show the way?

Looking across the banking industry, one possibility is that new entrants may be better positioned to identify the optimal way forward by building or buying a better solution from scratch, and using it to take a significant slice of the market. This approach has the benefit of being unconstrained by legacy. However, building or implementing a new platform is costly, and it takes time to achieve scale – meaning it’s unlikely to be an option for the whole industry.

These considerations point towards outsourcing as the answer, but as indicated above this is an option that’s relatively immature and unproven. On balance, while new entrants to the banking market may have some influence on industry resilience, they will not be able to fix the problem across the entire sector.
Better incident management...

Alongside actions that individual banks can take to improve their core systems, resilience can also be improved through joint industry initiatives. One option is for banks to team up to improve their ability to manage major individual incidents collectively – an objective highlighted by the British Bankers’ Association (BBA) in its UK Retail Banking Sector Summary Report on Retail Resilience Exercise 2013. This report was based on an initiative in April 2013, when UK retail banks participated in the BBA’s Retail Resilience Exercise (RRE), the first of a new form of sector-based ‘market wide exercise’ (MWE) designed to test the UK’s finance sector. The RRE was rated a success, having identified the core sector-based information flows, tested the interaction with the authorities in the event of a significant IT event, and confirmed the importance of effective and proactive media management across the industry.

...or an industry utility?

A second industry-wide option to enhance the resilience of core systems is joint investments in a shared utility solution. The utility would hold customer balances centrally and be managed as part of the payments infrastructure, while leaving individual banks free to run their own systems to undertake activities such managing products, applying interest and calculating fees. The option of a shared utility solution attracted support from the UK Payments Council in its June 2013 paper The Payments Roadmap – An Initial Report, on the grounds that it would not only boost resilience but also lower the barriers of entry to the industry, aid switching, and make it easier to migrate customers elsewhere when a bank fails. Also, as the final report if the Parliamentary Commission on a Banking Standards notes, the benefits of a common utility platform would include “raising the general levels of transparency in the money system, improving bank resolvability in the case of bank failure, and encouraging banks to make much needed investment into their patchy and outdated in-house IT systems.”

As with most other options, joint investment in a shared utility brings both pros and cons. On the upside, it would open the way to the creation of a standardised, modern and highly robust platform that would undoubtedly transform the resilience of core banking services across the industry. In a blog written in January 2014, BBC business editor Robert Peston commented: ‘When I talk to those running banks big and small, they say that the competitive playing field could be levelled in a significant way, if the payments system became an independent, price-regulated utility, available to be used on equal terms by all authorised banks, whether big or small.’

However, the cons of trying to move to a utility solution are also substantial – including enormous cost and risk, and the competition issues that inevitably arise when an industry seeks to act in concert.

Regulators weigh up their options

While UK regulators are expressing growing interest and concern over the resilience of banks’ IT systems, they have to date introduced relatively little regulation on IT. This light-touch approach is in contrast to that being taken in markets such as Singapore, Hong Kong and Australia, where more prescriptive rules have been put in place.

Given these contrasting approaches, what steps might regulators take that would be helpful for banks wrestling with core system resilience? Actions to consider might include making availability of systems a key part of assessing the bank’s operational risk. Such a step would probably require mandating standardised availability reporting, since this is currently an area where it is very difficult to identify and compare different banks’ performance.

Other possible actions for regulators to think about might include setting more prescriptive IT guidelines. In Singapore, for example, the Monetary Authority of Singapore (MAS) published IT guidelines that set out risk management principles and best practice standards to guide financial institutions. For example, it will soon be compulsory to notify all outages of critical systems within 30 minutes.

A further step that regulators might consider is to become more closely involved in facilitating industry cooperation to deal with major incidents. However, this is likely to require very different kinds of expertise and skillsets from those that most regulators currently possess in-house.
A substantial part of the core banking systems still in use today in the UK were designed and developed when British Leyland was producing the Austin Allegro. In the intervening decades, the car manufacturers invested in completely new production lines, driving productivity and quality up and costs down. In contrast, the banks built layer after layer on top of their original systems.

Despite these contrasting approaches the past forty years have seen both banks and carmakers innovate massively in their end-customer offerings. So it’s hardly surprising that legacy core banking systems are running out of road. In fact, the really surprising thing is that banks’ IT departments have succeeded in keeping them on the road for so long.

Put simply, more of the same will no longer do. It’s time to seize the nettle – and create core banking platforms fit for the 21st Century.
References

1 http://www.publications.parliament.uk/pa/cm201314/cmselect/cmniaf/uc650-viii/uc65001.htm
5 http://www.ft.com/cms/s/0/b18894c4-88d6-11e3-bb5f-00144feab7de.html#axzz2xrZcHNJY
8 http://www.publications.parliament.uk/pa/jt201314/jtselect/jtpecbi/27/2704.htm

Authors

Kashif Khan
kashif.khan@accenture.com

Matthew Edwards
matthew.edwards@accenture.com

Emily Farrimond
emily.farrimond@accenture.com

Nick Badger
nicholas.badger@accenture.com

Ashish Mehta
ashish.d.mehta@accenture.com

Auraelen Guia
auraelen.guia@accenture.com

Robert Stubbs
robert.a.stubbs@accenture.com

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 289,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$28.6 billion for the fiscal year ended Aug. 31, 2013. Its home page is www.accenture.com.