HOW TECHNOLOGY DECISIONS CAN EXPOSE BANKS TO TECHNOLOGY AND STRATEGY RISK

Over the past three decades technology has had a profound effect on the way in which banks conduct their business, with technology decisions concerning bank legacy systems, technology outsourcing and financial innovation exposing banks and, in some instances, the wider financial system, to significant technology and strategy risks. The quality of early-stage planning, communication between management, and IT and systems implementation, can have a significant bearing on the level of technology and strategy risk to which the banks are exposed.

Legacy systems

The decision by banks to upgrade or replace their legacy systems is largely driven by a desire to grow the business, decrease costs and improve efficiency. Over the past five years, for example, Australian banks have invested billions of dollars in upgrading their core software systems just to stay competitive (King 2008).

As the banking industry has evolved, legacy systems have become increasingly sophisticated. This, in turn, has contributed to growing risks associated with undertaking core systems replacement, upgrade and integration. Consider how much more sophisticated modern banking has become since the 1990s. Key factors that have led to the development and complexity of legacy systems include: an increased diversity of products; use of technology to interact with customers; international expansion through globalisation; and growth in cross-border regulatory compliance.

Banks and financial institutions have traditionally structured their businesses around product offerings such as commercial or consumer lending, and retail or wholesale deposits. Industry rationalisation and growing competition have resulted in banks’ offering a wider range of products to customers, often delivered through new technology (e.g. online banking).

One credit card executive recounts that, ‘In 1994 and 1995, there were a couple of credit cards, one at 17 percent interest and the other at 19 percent interest. When I left [in 1999] there were 43,000 pricing combinations’.

These increased offerings required significantly more sophisticated computing power to deliver the product (Olazabal 2002, p. 2). Increased product variety and delivery methods have led to more elaborate systems design and sophistication.

Another important factor that has contributed to increased demands on bank legacy systems is how banks manage their regulatory compliance requirements across multiple banking jurisdictions and brands (e.g. Westpac and St.George). Globalisation of the banking industry has resulted in large banks operating in multiple jurisdictions with each subject to their own regulatory requirements. A survey carried out by the Economist Intelligence Survey Unit in 2006 found that banks are often required to operate multiple reporting systems to manage cross-border compliance and regulatory requirements. The report revealed that over one-third of all banks surveyed said that they report to 10 or more regulators, and over 75 per cent of all banks surveyed reported to four or more regulators (Metricstream, n.d.). This adds to the complexity of the banking business, placing further demands on core system requirements as information needs to be
The potential fallout from poorly executed core systems integration can range from frustrated customers through to a catastrophic loss of confidence in the bank, customers who walk, litigation and even multi-million dollar compensation payouts.

managed, channelled and aligned between systems to meet regulatory needs.

The quality of decision making at the planning stage of a system implementation can expose banks to risks surrounding their reputation, market positioning and operating earnings. Two well-documented system upgrade failures in the past 20 years have been the National Australia Bank’s integrated systems implementation, which in 2004 suffered a write-off of some $200 million, and Westpac Banking Corporation’s (Westpac) $200 million CS90 project in the 1990s.

Upgrading legacy systems

In 1987, Westpac launched its Core System 90 (CS90) integrated legacy system at a total budgeted cost at the time of $120 million. By 1992, the still-incomplete CS90 had cost the bank over $200 million, with the final cost never being acknowledged publicly. The system promised to link Westpac’s huge network of branches through a central computer which would be capable of integrating all key areas of the bank while providing improved efficiency to keep operating costs down. The project failed to deliver many of its original promises; it cost the bank significantly more than originally budgeted and was eventually abandoned (Carew 1997).

In her post mortem of Westpac’s CS90 failure, Carew indicates that ‘a combination of technical complexities and deficiencies, and management enthusiasm based on inadequate analysis, contributed to the death of CS90’ (p. 307).

The system vendor, IBM, considered Westpac’s inability to concisely define the business requirements of the system as being the biggest risk to the project (Carew 1997, p. 307), however, as system vendor, IBM also played a role in the CS90 failure.

Notwithstanding this, other commentators with an insider’s view of what went wrong cite Westpac management’s poor decision at the outset in entrusting system design and implementation to IT ‘academics’ that had little real world knowledge of banking, the industry and, most importantly, the business drivers for systems integration (Glass 1999).

Poor planning decisions at the early stages of the systems upgrade exposed Westpac to technology risk through interruption to business as usual, crystallising in the significant cost over-runs and delays incurred. The project was eventually abandoned by the bank and the entire cost written-off. The bank faced strategy risk as the issues with CS90 distracted the board’s attention from other issues facing the business at the time, namely, the problems surrounding asset quality with its troubled subsidiary AGC.

Systems integration

It is widely believed that as banks grow in size, the potential scale and array of technology increases (Saunders and Cornett 2003). This argument can also be turned around, such that major investments in technology can often lead banks to engage in a strategy of growth, typically, by merger or acquisition. The economics of this are based on the notion that a bank will want to spread the high cost of technology investment across the largest possible business and/or customer base.

Large initial investments in technology have given rise to new economies of scale in the provision of banking services. This, in turn, has driven the large consolidations in the banking industry over the past few decades (Lapavitsas and Dos Santos 2008). For example, ANZ Australia’s decision to upgrade its internal enterprise-wide systems in 2009 was driven by the strategic goal of growth (Bajkowski 2009).

In late 2009, Toronto-based TD Bank (TD) attempted to integrate its core systems with North American Commerce Bank. TD purchased Commerce Bank in 2007 for US$8.5 billion, with the deal more than doubling TD’s presence in the United States, making it North America’s seventh-largest bank, as measured by bank branches (Dealbook 2007). In her discussion of the deal, Amanda Taylor of West Chester University outlines a multitude of reasons for the merger, all of which point to two compelling motives: cost cutting and improved efficiency. However, when the systems integration project went ‘live’ in September 2009, something went very wrong, resulting in customers losing access to their bank online accounts. There were also delays in overnight processing for customer account balances which caused significant frustration for all affected, including the bank.

As a result of the widespread disruption to customer banking arrangements, rival banks staged a targeted campaign to acquire unhappy Philadelphia-area TD Bank customers. While the exact reasons for the integration problems have not yet been publicly aired, this case highlights how a lack of business disruption and recovery planning can expose banks to the risk of competitors stealing customers and thereby eroding the market share of the ill-fated bank.

Careful planning and preparation, coupled with business continuity and disaster recovery plans, must be carefully considered to mitigate the fallout from system failure throughout the ‘go live’ phase.

The potential fallout from poorly executed core systems integration can range from frustrated customers
through to a catastrophic loss of confidence in the bank, customers who walk, litigation and even multi-million dollar compensation payouts, the latter being the ultimate repercussions when Mizuho Bank was launched in Japan on 1 April 2002.

One of the biggest bank system failures in history, the amalgamation of Dai-ichi Kangyo Bank, Fuji Bank and Industrial Bank of Japan into the newly formed Mizuho Bank, is a first-class example of how poor technology decisions can expose the bank to significant technology and strategy risk. As part of a finance industry reorganisation, Mizuho Bank’s launch on 1 April 2002 was flawed from the very start. On ‘go live’ day, an incredible 105,000 automatic debits failed to be processed and customer ATM debit transactions were processed despite customers not having taken the cash from the machines.

Further erroneous transactions occurred in the days immediately following the ‘go live’ date and it took more than a month until the banks’ operations were returned to normal (Nakao n.d.). Having been reprimanded politically and publicly, Mizuho was ordered by Japan’s Financial Services Agency under Provision 26 of the Banking Act to take improvement and response measures and identify those responsible for the failure (Nagaoa and Takemura 2009). The threat of litigation followed, with corporate customers being compensated for significant losses. Tokyo Electric was paid approximately ¥9.8 billion (USD$74.7 million) in compensation for late payments and penalties (Reference for Business n.d.). In his analysis of Mizuho Bank, Masayuki Nakao of the University of Tokyo suggests that the systems failure can be attributed to the following causes:

**Technical systems factors**
- a failure to modify the incumbent system (previously the Dai-ichi Kangyo Bank system) to meet the requirements of the newly formed bank;
- an insufficient testing period and lack of interrogatory testing of operations and loads under the newly formed system;

**Business factors**
- poor planning and a lack of a master system architecture including electing a ‘go live’ date on one of the busiest days of the year for all three merged banks; and
- data integrity issues within status reports and a severe disconnect between the technical requirements to ‘go live’ and management’s expectations.

The above decisions exposed the bank to technology risk, which was crystallised through false transactions being generated and legitimate transactions not being processed. This failure to carry on business as usual undermined public confidence in the bank which, in turn, caused considerable damage to the bank’s reputation, also severely impacting the bank’s ability to execute its desired strategy. The implications of the failure were wide-reaching in that the failure of Mizuho caused ‘immeasurable damage to the society and highlighted some of the problems of the information society. It also proved how much benefit the Japanese economy receives from information technology’ (Nakao n.d., p. 7).

**Mitigating systems integration risk**
Handled well, core systems integration can bring significant upside benefit to the newly merged entity without the downside risks and repercussions discussed above. The question therefore follows, how might banks look to ‘de-risk’ the system integration process and what benefits might follow as a result? Heap, Israelit and Shpilberg (2003) cite the benefits that can arise out of well-orientated and executed systems integration. They also state three key rules to assist legacy systems integration. These are:

> **Follow the money**: What is the purpose of the integration? Is it to achieve cost savings (economy of scale)? Is it revenue growth through cross-pollination of databases to extract cross-sell value and deeper product penetration (economy of scope)?

> **Speed over perfection**: The time taken to implement, and interruption to business, can be a massive resource drain on the bank. It is often more desirable to select one system over a hybrid/best-of-breed structure.

> **Keep the base business running**: The base business is at the heart of the value which is being merged and it is vital that this is given priority to avoid costly errors leading to competitors stealing customer accounts and eroding the banking business.

A relatively recent example of a well-planned systems integration project occurred when Great Britain’s Abbey National was acquired by Spanish bank Banco Santander in 2004.

The Abbey National acquisition was large, even by international standards, and at €13 billion, was Europe’s biggest cross-border acquisition. Before the acquisition took place, Santander went on record asserting that it would trim approximately £307 million from Abbey’s business by successfully applying its banking systems to the British bank (Nuttall 2004).

While the integration process did incur minor glitches such as errors made in processing customer account transactions, the integration is widely heralded as a success by modern-day bank merger standards.

In referring to the Abbey National acquisition, Parada, Alemany and Planellas (2009) suggest that it was Santander’s ‘success in transferring its superior operational, technological and marketing capabilities to its British target that was critical in creating that value. Value that was created in integrating Abbey arose from economies of scale and scope, especially in IT and training activities’ (p. 667).
This ‘socialisation of risk’ has exposed banks to increased technology risk as there is a loss of soft knowledge about credit counterparties, process or business model, instead replaced by heavy, myopic reliance on cutting edge technology to model complex quantitative equations. The increasing reliance on technology to enable banks to manage large positions on their banking book presents new elements of vulnerability to the banks and the wider financial system.

Obsolescence and failure to upgrade
The capital investment required to upgrade or replace a legacy system is significant and often a significant hurdle for many banks. Legacy system upgrades may be delayed for budget or funding reasons. As discussed above, the consequences of not doing anything can often be more significant than the risks arising out of poor implementation.

Often, the upside benefits are difficult for the board and management to quantify, particularly when new and ‘untried’ technology are being proposed.

In August 2010, Singapore’s DBS Group Holdings was ordered by the Singapore Monetary Authority to improve its computer systems after its automatic teller machines, internet banking and electronic payments failed for seven hours in July 2010 during maintenance by IBM Corp.

The Singapore Monetary Authority concluded that ‘DBS Bank did not exercise sufficient oversight of the maintenance, functional and operational practices and controls employed by IBM’. This incident has revealed weaknesses in DBS Bank’s technology and operational risk management controls’ (AP Associated Press 2010, para. 3).

In addition to being instructed to improve its systems and over-reliance on one IT systems provider, DBS Bank was forced to set aside around $230 million Singapore dollars of regulatory capital to cover operational risk. The decision to rely on a single provider for an essential area of the banking business exposed the business to technology risk. Whether the network failure was due to ageing technology is uncertain, however, given the seriousness of the failure, it is reasonable to assume that the systems were not up to standard and further investment and improvement was required. The bank is now exposed to additional strategy risk in that the requirement to carry additional capital presents an economic and lost opportunity cost to the business.

As a result of under-investment in reliable systems technology, the bank now faces other strategy risks including reputation risk and the risk of competitors capitalising on DBS Bank’s failure.

Technology outsourcing
Other technology risks include the logistical reliance on a third-party provider that may be located a considerable distance from the bank. Studies have shown that the geographic distance from the function and timing lags in reporting heighten the potential risk exposures (Swartz 2004).

Outside of the banking sector, the failure of Telecom New Zealand’s XT Network in early 2010 is a good example of technology risk in the form of over-reliance on a third-party vendor without the necessary local support to maintain critical technology infrastructure. It took several weeks for Telecom’s XT network provider Alcatel Lucent, who were flown into New Zealand from around the world, to properly diagnose and fix the systems problem. During this period, Telecom ‘XT’ customers were adversely affected by arbitrary network outages which came under the public spotlight through national media coverage.

Telecom suffered considerable reputation damage and lost market share as a result of the XT network failure. The company was immediately exposed to strategy risk, which was realised when it lost out on selection to tender for the first stage of the government-funded rollout of ultra-fast internet network across New Zealand. Indeed, Telecom is still recovering from the failure of its XT Network.

Another technology risk resulting from outsourcing is the impact of incompatible or corrupt technology from a third-party provider on a bank’s incumbent system.

Recently, America’s second-largest US bank, Chase, experienced first-hand the seriousness of system failure when its internet banking service failed for two days, affecting millions of its customers (Gogoi 2010). Chase cited the key reason for the failure as being software issues resulting from a third-party database company which had corrupted information in its systems and prevented users from logging on. This meant that millions of Chase customers could not get online access to their accounts to transact ordinary, everyday payments.

Decisions that failed to address the terms of engagement, and, in particular, the necessary precautions to protect the bank, exposed the bank to technology risk.

Significant financial cost was incurred to reimburse customers. In addition, there were additional costs involved with repairing and testing the system with the full extent of the failure yet to be fully determined.

Financial innovation
The availability of enhanced and affordable computing power has allowed banks to engage unequivocally in ‘financial market’ mediation, while transforming their techniques of risk management. By way of example, the development and subsequent increased use of
mortgaged-backed securities was a result of increased investment in computing power (Lapavitsas and Dos Santos 2008).

Lapavitsas and Dos Santos assert that banks’ appetites for these derivative arrangements have led to a move away from relational assessment of credit risk using technology to undertaking complex computational assessments of quantitative elements. This has resulted in banks exercising less managerial judgement on credit risk.

Allen and Santomero (1998) believe that a similar argument can be mounted in that banks’ increased volume of derivatives indicates a shift in risk management by banks away from traditional balance sheet liquidity and maturity management towards hedging with derivatives assets using advanced computer modelling technology. This ‘socialisation of risk’ has exposed banks to increased technology risk as there is a loss of soft knowledge about credit counterparties, process or business model, instead replaced by heavy, myopic reliance on cutting edge technology to model complex quantitative equations. The increasing reliance on technology to enable banks to manage large positions on their banking book presents new elements of vulnerability to the banks and the wider financial system.

Strategically, this risk is accentuated when the quality and quantity of data is limited, thereby exposing the bank to risk positions that, arguably, were at the heart of the 2007 global financial crisis (GFC).

Lapavitsas and Dos Santos also assert that the enormous growth in residential mortgage lending would not have been possible without the widespread adoption of sophisticated ‘computationally intensive inference based techniques of credit analysis’. As mentioned above, the adoption of such technology innovation has changed the ways in which banks manage credit risk; the use of derivatives has grown concomitantly.

The advent of such new and untested financial innovation carries risks that have yet to be fully identified in some areas.

For example, the risks and characteristics of collateralised debt obligations were not fully appreciated by credit ratings agencies (Risk Magazine 2010) until after the GFC. Technology and financial innovation provided the means for banks to develop these synthetic risk management instruments; all the while, they were unknowingly exposing themselves to untenable risk positions. The decisions to rely on these new financial innovations exposed banks to technology risk through the lack of knowledge, in dealing with these products, about the implications for the banks’ business.

Furthermore, banks could be assuming riskier positions than contemplated, the result of which exposes the institution to strategy risk through having to manage the impact of unexpected risks and shocks on the business, when considered against the corporate strategy.

Summary

This paper examines the ways in which technology decisions can expose banks to technology and strategy risk. Particular attention is given to technology decisions regarding legacy systems, technology outsourcing and financial innovation.

The analysis highlights common decisions such as cost management and outsourcing, and instances where banks’ failure to understand how a project can expose them to technology and strategy risks. A key finding is that the quality of early-stage planning, communication between management, and IT and systems implementation can have a significant bearing on the level of technology and strategy risk to which the banks are exposed.

After examining a wide range of examples in which technology decisions by banks have exposed those institutions and, in some instances, the wider financial system, to technology and strategy risks, a common thread emerges in which significant risk exposures have resulted from an extreme reliance on technology to manage the banking business.

References


Carew, E. 1997, Westpac, the bank that broke the bank, Doubleday.

THE JASSA PRIZE

All original articles published in JASSA are eligible for the JASSA Prize of $1,000 awarded annually for the article judged as making the best contribution to the financial services industry.

If you are interested in submitting articles or for further details, email: JASSAcontent@finsia.com