OUTSOURCED MICROFINANCE MIS SYSTEMS—A DECISION GUIDE FOR MICROFINANCE INSTITUTIONS

microREPORT #115

OUTSOURCED MICROFINANCE MIS SYSTEMS—A DECISION GUIDE FOR MICROFINANCE INSTITUTIONS

microREPORT #115

Contract No. GEG-I-01-02-00011, Task Order No. 01

Alice Liu

CONTENTS

TABLES AND FIGURES

OUTSOURCING DECISION GUIDE FOR MICROFINANCE INSTITUTIONS

INTRODUCTION

Core banking management information systems (MIS) are the foundation upon which financial institutions worldwide run their business, serve their clients, and provide differentiated products and services to gain competitive advantage. Microfinance institutions (MFIs) in developing countries require the same foundation for the same reasons but have fewer vendor choices, more limited budgets, and sometimes unique requirements, leaving MFIs to build their own systems or make do with spreadsheets or even manual paper systems. In the last five to ten years, however, the success of the MFI model has become widely recognized and attracted the interest of the mainstream financial sector, development practitioners, and information technology (IT) solution providers. MFIs today have a new option as a few vendors have begun to develop outsourced core banking systems.

The choices for a resource-constrained MFI can be confusing. Outsourcing is based on a new business and pricing model in most developing countries, making it difficult for MFIs to compare against other solutions. The vendors are new, so it may be wiser to take the more traditional approach: build a system from scratch (custom development) or buy a commercial-off-the-shelf package (COTS). Custom development can easily take six to nine months, and COTS software requires a large up-front investment and may not meet all the requirements. MFIs may have already tried one of these approaches and were dissatisfied with the result, but outsourcing looks expensive and they are worried about security. MFIs driving through this roundabout of decisions need to know which road to take.

This Decision Guide seeks to help MFIs break through the "analysis-paralysis". It identifies the key decision factors to consider, the main reasons to choose each option, pricing models for outsourced solutions, and it explores in depth two key issues for core banking systems: total cost of ownership and data security. There is an extensive list of tips and recommendations to guide MFIs in the vendor selection and evaluation process, starting with developing a request for proposal (RfP), and ending with tips for managing the vendor post-implementation. For this research, DAI interviewed two vendors of core banking solutions, one who provides solutions for the largest to the smallest financial institutions in the developed world, and another, IBM, who has just embarked on an initiative to build shared "processing hubs" for MFIs in Latin America and Africa. The interview summaries can be found in the Appendix.

This Outsourcing Decision Guide is a companion document to "Microfinance Core MIS Systems – The Business Case for Outsourcing". The Business Case document provides a summary of the business case for MFIs to outsource their core banking system, describes the research objectives, and defines terminology, so the reader should review the Business Case document before this Decision Guide. The Business Case includes three other case studies profiling the experience of three small financial

institutions in the U.S.: one that outsourced from the first day in business, one that has a hybrid of in-house and outsourced systems, and one that chose to buy a package and host in-house.

DECISION FACTORS FOR EACH IMPLEMENTATION OPTION

Today MFIs have three main options to implement a core banking system: build a system from scratch ("custom development"), buy a software package (COTS), or outsource. To decide which option is best, the following are the main decision factors an MFI should consider:

- Implementation time/time to market and the opportunity costs

- Total Cost of Ownership (TCO), which includes both tangible and intangible costs as well as ongoing costs

- The breadth and depth of requirements the system must satisfy

- Need for frequent customizations and changes

- Availability of qualified, reputable, and viable software vendors and outsourced solution providers

- Skill and availability of IT staff and within the local IT sector

- Technology preferences

- System availability, performance, and security

- Regulations or government policy governing financial information, IT systems and electronic data

- Other priorities

Table 1 below summarizes the reasons to choose each option, the reason why the option may not be the right choice, and the keys to success for each option:

TABLE 1: SUMMARY OF DECISION FACTORS FOR EACH IMPLEMENTATION OPTION

| Implementation Option—Build from Scratch	
Reasons to Choose this Option	- Have unique or frequently changing requirements - Can build to meet exact requirements, processes, and policies - Have an IT team that can do the work - Want to host the system in-house - Vendor choices are limited
Reasons to Not Choose this Option	- Longest implementation time - Highest TCO - Most complex to manage
Main Success Criteria	- Stable, qualified, and experienced IT staff and management - Availability of qualified IT professionals in the local market - Stable and sufficient internal infrastructure for in-house hosting
Implementation Option—Buy a Software Package	
Reasons to Choose this Option	- Faster implementation time - Lower TCO - Less complex to manage

	• Want to host the system in-house
	• Don't have an IT development team to build the software
Reasons to Not Choose this Option	• Software packages on the market don't sufficiently meet requirements
	• Don't want to depend on the vendor for software changes
	• Implementation time is still too slow
	• TCO is still high, especially up-front costs
	• Still complex to manage
Main Success Criteria	• Stable, reliable software package that meets most of the requirements
	• Qualified, reputable, viable software vendor
	• Enforceability of contracts
	• Stable and sufficient internal infrastructure for in-house hosting
Implementation Option—Outsource	
Reasons to Choose this Option	• Fastest implementation time
	• Lowest TCO
	• Least complex to manage
	• Don't have an IT team that can build or host the system in-house
Reasons to Not Choose this Option	• Outsourced solutions don't sufficiently meet requirements
	• Don't want to depend on vendor for software changes and hosting support
	• Want to use a different technology than the vendor is using
Main Success Criteria	• Stable, reliable outsourced solution that meets most of the requirements
	• Trusted partnership with the outsourced solution provider
	• Explicit contracts and service level agreements (SLAs)
	• Enforceability of contracts
	• Stable network connectivity and sufficient network bandwidth with the off-site data center

OUTSOURCING IMPLEMENTATION PHASES

Before discussing total cost of ownership, it is important to understand the life cycle to implement and maintain an IT system, because the TCO is directly related to the tasks involved. Figure 1 below illustrates a hypothetical time frame to implement an outsourced core banking system. This is a screen shot from Microsoft Project, the de facto standard project management tool on IT projects. In the actual MS Project file, links between tasks and phases show the dependency of one task on another; that is, if one task is delayed, it delays the start or completion of another task.

Instead of a long software development phase, in which programmers are coding the application, there is an Application Configuration and Setup phase and a short development phase to implement customizations. Some time is allocated for Supplementary Software and Hardware Procurement for additional network equipment to connect to the outsourced solution provider's data center and servers, the potential need to increase the institution's own network bandwidth and Internet service due to the expected increase in network usage with the new system, and new or additional desktop PCs and printers. This is significantly less time than if the MFI intended to host the system in-house. The bulk of the software and hardware procurement, installation, and configuration work is left to the outsourced solution provider, who already has all the systems in place, fully tested and configured.

FIGURE 1: HYPOTHETICAL TIME FRAME TO IMPLEMENT AN OUTSOURCED CORE BANKING SYSTEM
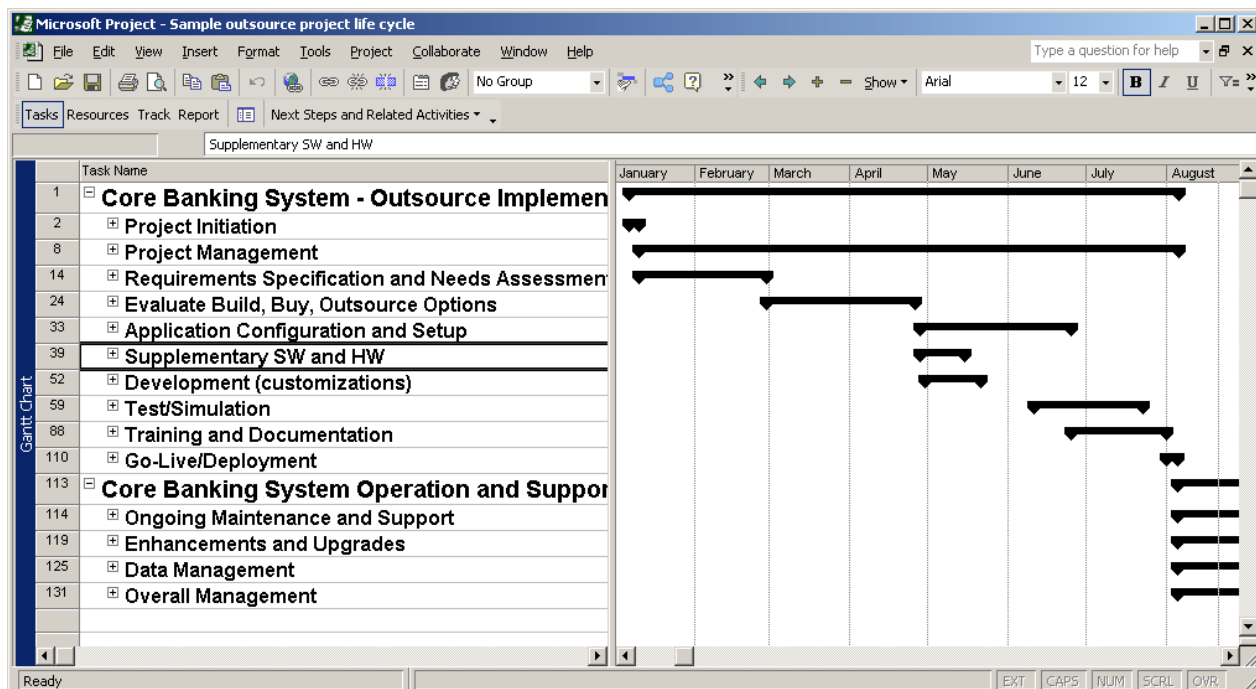
These are hypothetical implementation times. Other issues factor into the time for implementation, such as size of the MFI in terms of number of employees and branch locations, volume of data, number and complexity of business processes to support, user buy-in, and other issues which can result in a long implementation time regardless of the approach.

The table below provides another illustration of several complex implementation and maintenance tasks and the associated staffing and other costs that transfer from the MFI to the vendor in both a packaged software and outsourced implementation:

TABLE 2: TASK RESPONSIBILITIES FOR EACH IMPLEMENTATION OPTION

Phase	Responsible Party		
	Build	Buy (and host in house)	Outsource
Software Design, Development, Test, and Support	MFI	Software Vendor	Outsourcing Vendor
Software Enhancements and Upgrades	MFI	Software Vendor	Outsourcing Vendor
Server and Network Procurement, Support, Maintenance, and Monitoring	MFI	MFI	Outsourcing Vendor
System Security, Backup and Recovery, Disaster Recovery	MFI	MFI	Outsourcing Vendor

PRICING MODELS

There are different pricing models and combinations used by U.S. core banking vendors, some of which are illustrated here:

- Upfront installation fee

- License and maintenance fees

- Per account

- Number of accounts (could be based on tiers)

- Number of deposit and loan accounts; some related products based on a per-user basis

- Asset-based

- Low license fee and monthly charge based on asset growth

- Variable monthly fee based on number of accounts processed

Implied above in "number of accounts" is tiered pricing. Instead of a flat fee per account regardless of the total number of accounts, there is a "volume" discount where the fee per account is reduced the higher the total number of accounts at the financial institution. For instance, the tiers might be grouped and priced as follows (this is purely illustrative and not based on any vendor quotes):

Tier	Number of Accounts	Monthly Cost per Account
1	1-999	$1.00
2	1000-4999	$0.90
3	5000-9999	$0.85
4	10000+	$0.75

MFIs should closely scrutinize the price quotes from vendors and compare the different models based on their own circumstances (number of accounts, asset size, expected growth) to determine which model would be most cost-effective for them, and use the information to negotiate with the vendor.

UNDERSTANDING TOTAL COST OF OWNERSHIP

Some believe that buying a package or outsourcing is more expensive than building and maintaining an in-house system. In some cases, as mentioned with the "Credit Union Product B" from Vendor X in Vendor Case Study 1 (see the Appendix), that might be true. However, most people do not have a full understanding of the **total cost of ownership** (TCO) for maintaining an in-house system because they are unaware of what is involved in implementing an in-house system. It is important to understand the TCO because a core banking MIS system is a long-term investment, more likely to be used for five to ten years in most MFIs except for the smaller ones (fewer than 2000 clients). The main cost differences between maintaining a system in-house and outsourcing are in the up-front cost of IT hardware and infrastructure and the long-term (three to five year) cost of infrastructure and systems maintenance, application maintenance and support, and staff time and labor. These are the hidden costs that organizations typically overlook. What may look like the lowest cost approach could be the most expensive in the long run, and what may appear to be the most expensive approach initially could be the least expensive over time. For

some MFIs, however, other issues will trump TCO. Each MFI must determine its own priorities and "bottom line" decision criteria.

There are numerous articles focused on customer relationship management (CRM) systems that compare the TCO of in-house solutions versus software-as-a-service (SaaS). One article even makes their spreadsheet available as a template for the reader to build their own TCO estimate[1]. To better illustrate the total cost of ownership, the table below provides a partial list of implementation tasks, organized by implementation phase, and can be used by an MFI to create their own TCO spreadsheet. These tasks would be the MFI's burden to staff and execute if the MFI decided to implement a core banking solution in-house. Some of these tasks, and in some cases the entire task, would be the responsibility of the core banking solution provider if the system was outsourced to them. Software and Hardware selection, procurement, and installation, and Testing, as well as the ongoing Infrastructure and Maintenance support and Application management, and the staff for these tasks would almost entirely be the responsibility of the outsourced solution provider. These tasks are the variables that should be factored into a TCO calculation. This is not an exhaustive list of TCO variables because it cannot represent every possible type of in-house core banking system implementation. It assumes that the core banking system is a purchased commercial-off-the-shelf (COTS) package and not built from scratch.

TABLE 3: TCO FOR A COTS SYSTEM HOSTED IN-HOUSE

Phase and Tasks	Comments
Needs Analysis	
Server Room and Site Assessment and Testing	Evaluate whether existing hardware and network infrastructure can support the new system; whether physical space and security measures are sufficient; whether the cost of downtime and recovery warrants installing not just the typical redundancy in servers but also redundant network connections and power supplies; cost of floor space; estimate power consumption cost.
Detailed Design and Architecture	
Business Process Mapping and Re-engineering	With an outsourced system, the bank can choose to adapt some of its processes to the way the core banking system functions, rather than create new processes and business rules from scratch.
Create a more detailed functional specification	When buying a package or using an outsourced solution, the IT team and users still need some level of training on the software functionality, design, and architecture.
Create application design, data model, object model, physical database design, and system and network architectures	When buying a package and hosting in-house, the design and modeling needs to be done for customizations and the system and network architecture design still needs to be done. If outsourcing, the only effort required will be for customizations.
Implementation and Test	
Implementation	
Hardware Selection and Procurement • Firewalls, routers, and load balancers • Load balancers • Web servers	Includes the time to understand the expected system usage and performance requirements well enough to design the overall system and network architecture, develop the hardware specs, and to get multiple bids and negotiate with vendors. Also, since the system will be

---

[1] Andrew Conry-Murray, "TCO Analysis: Software as a Service – Same Dog, Different Fleas," *Network Computing*, March 5, 2007. http://www.networkcomputing.com/showArticle.jhtml?articleID=197700166.

Phase and Tasks	Comments
• Application/middleware servers • Database servers • Document management servers • Image servers/file servers • Racks, switches, and cabling	hosted in-house, the bank will need to create a test environment and procure test servers in addition to the production servers. If the COTS require customization, the MFI may also need to procure development servers and create a development environment if it does not have one already, or create a development area in the test environment.
Hosting Environment Upgrade	If the system will actually be hosted in the bank's own server room, the room may need modifications depending on the number of additional servers. More air conditioning, power, wiring may need to be installed. Need to have adequate backup power supplies and/or redundant power sources. May need to upgrade security systems such as security cameras, biometrics. Supervise any contractors, construction crews.
Software Selection and Procurement - Licenses and maintenance agreements for a complex software stack on the servers: • Application license • Operating systems • Network management software • System monitoring and notification tools • Backup and recovery software • Database engine • Application servers • Web server • Security software and monitoring (virus and intrusion detection) • Document management software • Fraud detection software • Software development tools and source code version control system (if building the system from scratch) • Bug/defect tracking database • User tools such as reporting software	Licenses need to be purchased for both the test and production environment. If any customizations are required, then software licenses for a small development environment must be purchased. If outsourcing, most of these licenses will be unnecessary, again only needed if the MFI IT staff will be building custom features to integrate with the software.
Hardware and Software Installation, Configuration, and Testing: • See list under "Hardware Selection and Procurement"	Includes integration with the corporate network, corporate email, etc.
Software Customization	Includes the user interface, reports, and database.
Documentation	Should include documentation of customizations, system and network architecture, system configurations, operational procedures, backup and recovery procedures
Test	
Application Testing	Encompasses testing the functionality and reports. Prior to this the team must develop a testing process and at least a rudimentary system (such as spreadsheets, ideally a database) for tracking new and resolved bugs.
User Acceptance Testing	Users test the system against a pre-defined set of acceptance criteria. If the system meets the acceptance criteria, the users accept the system and the system can go-live.

Phase and Tasks	Comments
Regression Testing	Must re-test the application after major changes have been made to the system, to ensure the changes have not broken any functionality that was working prior to the change.
Integration and Testing with other information systems the MFI may run or interact with	
End-to-end Testing	Test the system after it has been fully integrated, to test the system "end-to-end" by testing functionality that exercises every major component of the system, including integration with third party or other external systems.
Data Conversion and Testing	Create plan, define conversion rules, and create conversion scripts. May require multiple iterations to clean all the data before data can be successfully converted to the new system.
Performance, Stress, and Load Testing	Performance testing includes testing if the system can handle the required number of users, transactions per second, or volume of data. Stress testing tests the peak levels the system can handle. Load testing tests a constant load on the system to see if the system fails under this load (e.g. memory leaks that lead the system to run out of memory).
Security Testing	Both physical and electronic security systems should be tested. Includes testing of internal procedures to ensure that all staff understand and are following the procedures correctly
Failover and Redundancy Testing	Most mission-critical systems will have redundant systems; if one server fails, the other will take over the load. This needs to be tested and the associated performance degradation and impact to customer service and bank operations should be measured and evaluated relative to the financial and reputational risk and formally accepted (signed off) by management
Backup and Recovery Plan, Implementation, and Testing	Includes backup and recovery software and devices, contract with a remote tape storage facility
Disaster Recovery Plan and Testing	Depends partly on amount of downtime that is acceptable. For large institutions, this can be a complex solution and easily double the cost of an in-house implementation due to the need to create a mirrored system in another data center, preferably located a significant distance away from the primary location. Smaller institutions have less at stake and may determine that some downtime is acceptable and rely on the backup and recovery plan.
Independent IT audit	In highly regulated environments like the U.S., this is recommended.
Regulatory Review	In the U.S. this can be a several week process.
Training and Documentation	**For all training: If the training is held during work hours, there is an opportunity cost; while a person is at training, they are not performing their regular job duties.**
User and Staff Training	Includes the development of a training plan (approach such as "train the trainer" and designating certain users to be "super users"), training manuals, a training schedule, repeat or "refresher" training, and staff time spent in training versus doing their real job.
IT staff training	Training to support the COTS application and entire environment.

Phase and Tasks	Comments
Management training	To provide them with an overview of the system benefits, functions, and especially the reports and data available from the system.
Help guides, user manuals, operations manual	Help guides and user manuals will be provided by the software vendor. However, the MFI IT team needs to create its own operations manual which describes its system maintenance procedures, backup and recovery procedures, security procedures, etc. With outsourcing this task is the outsourcing provider's responsibility.
Go-Live/Deployment	
Establish an end-user help desk	
Release Management	Manage the process of pushing system modifications from the test environment to the production environment. Test that push to production didn't break the production system.
Make an image of the pristine database and code prior to go-live	
Run data conversion programs	
Perform a "smoke test"	To ensure that the release to production was successful – all files were copied, data was properly updated, configuration is correct, etc.
Staff Costs during the Implementation • Developers for any customizations • Report programmers • Quality assurance testers • QA manager • Configuration manager • System/network administrators • System/network architect • Database administrators • Database architect • Security specialists (network and physical) • Business analysts • Project manager • Team manager • IT director	With an in-house system, the bank will require more staff to manage and execute the various tasks listed, whereas with outsourcing the vendor would take responsibility for many of these tasks. One person may be able to take on multiple roles (such as both project manager and business analyst), if they have the skill and aptitude and the workload is still reasonable.
Ongoing Costs	**Calculate for next 3-5 years**
Infrastructure and Maintenance	
Facilities costs such as office space, server room or data center space, cooling systems, fire suppression	
Electrical power, backup power/fuel, lighting	
Network and Telecommunications costs	Internet connectivity and internal network traffic will increase with increased usage of the core banking system.
Annual support/license fees for core banking software and user tools	User tools include reporting software and software residing on a desktop or laptop PC.
Annual support/license fees for servers and server-level software	See server-level software list above
Staff-related costs (salary and benefits, training, recruitment, retention, management time, staff turnover/productivity loss).	For database and system administrators, suggested cost basis is one-third of a full-time employee.

Phase and Tasks	Comments
Configuration Management, including Upgrades, Updates, Patches, Bug fixes	This can be complicated – a patch for software X might run only on Operating System Y version abc service pack level 123 but Database Z has not been tested with this yet.
System monitoring, administration, and backups	Includes troubleshooting system performance issues, monitoring for disk usage and security issues, "ping" tests to test that the system is available, etc.
Scheduled maintenance (downtime)	Some maintenance tasks may require the entire system to be shutdown. The system should be designed such that most maintenance tasks can be done while the system is still online.
Hardware upgrades in Year 3, 4 or 5	Hardware warranties vary but typically last three years. After the warranty expires there will be an additional maintenance expense for each system out of warranty, replacement parts will be harder to find for older hardware, so there is significant incentive to replace the systems.
Application Management	
Integration with other systems	
Software customizations	Each customization will go through its own mini-implementation life cycle: requirements, design, develop, test, document, go-live.
Additional reports	Some new reports may come from the solution provider.
End-user support	
Data Management	
Define fields, valid values, and valid formats and set up data fields	
Define and enforce data standards	
Manage user access levels and permissions	
Support Data import/export needs	
Data cleanup	
Staff	
Other dedicated IT staff	Staff will vary, depending on how much customization and integration with other core banking system components is needed and the need for reports.
Recruitment, retention, management time, staff turnover/productivity loss	
Ongoing end-user and staff training	Training on new features in the core banking system, new reports, new business processes, new tools, etc. This task/cost may be shared with the COTS provider in the case of training about a new feature, release, or upgrade of their product. Include effort to create training documentation. Include opportunity cost if training is held during regular work hours.
Support from Procurement, Finance, Contracts, Facilities, Administration departments	Other departments contribute to the smooth running of the core banking system in some way, whether it is to process purchase orders and invoices, negotiate contracts, create budgets, etc.
Unplanned Costs	
Unscheduled Maintenance, Outage, Downtime, and Recovery Effort, Response to Security/Data Breaches	Unscheduled maintenance differs from an Outage in that it is not a sudden system failure that causes the system to shutdown, but an unforeseen maintenance task that must be done, such as applying a fix in response to a new virus that is infecting systems.

Phase and Tasks	Comments
Overall Management	
Management reporting, decision support tools, also known as "business intelligence"	The value from a transaction processing system is fully realized when advanced reporting is available for trend analysis and forecasting which management can use to make strategic decisions. The cost of these tools, the availability of pre-built and pre-tested reports, and consulting services from the vendor will vary.
Change management	Need to establish a change control process and change control board to manage and prioritize incoming change requests that will come from all parts of the MFI as well as from donors.
Vendor management	An IT manager is likely to be the person designated as the main contact person to liaise with the vendor.
Define policies and procedures	
Align the organization and establish organizational structure, roles and responsibilities	To manage the ongoing operations effectively and to provide ongoing management oversight
Oversee ongoing costs and budget	
Set strategy and vision for the application of IT in support of MFI strategic initiatives	This is the responsibility of the top level IT manager (CIO, VP, and/or IT director).
Evaluation of new products, services, and technologies	

This list will vary in scope and detail depending on the size of an MFI and therefore the complexity of its operations: number of clients/accounts, transactions per day, branches and other locations, staff. Some aspect of these tasks exists in even the smallest implementation, albeit on a much smaller scale and probably a small staff is performing multiple responsibilities. In large implementations, the financial institution will need dedicated IT staff for each responsibility area.

There are many variables to consider, cost-related and non-cost related, so a TCO calculation should not be the only criteria used when deciding whether to go in-house or outsourced. For example, the value an MFI might place on the ability to call the vendor when there is a system problem versus having to be responsible for resolving it themselves will vary. Conversely, the value an MFI might place in having servers on-site and under their direct control will vary.

The TCO should be calculated for the next three to five years. Three to five years is a rough timeframe as it is possible there is a break-even point in that time, but the break-even could be further out. The farther one looks out, however, the less reliable the numbers may be because the future is uncertain – the future technology costs, the future needs and growth of the MFI, the future technologies or systems available that the MFI will want to implement and integrate with the core banking system. Five years ago there was not as much discussion about mobile banking as there is today, for example.

DATA SECURITY

Security breaches are more common than one would think. Most cases are not publicized but they are a fact of life in today's increasingly electronic, wired world. No one is immune; JP Morgan Chase, Bank of

America, Wells Fargo, IBM, Hewlett Packard, AT&T, have all been breached, as well as many government and educational institutions[2].

An analysis of the data available from attrition.org[3], reveals that over all breaches tracked, the main source of data breaches was due to stolen equipment, followed by hacked systems. For financial institutions[4], the majority of the security breaches were due to stolen equipment. The table below focuses on the largest causes so these percentages do not add to 100 percent.

TABLE 4: CAUSES OF DATA BREACHES

Cause of Data Breach	Breaches Overall	Breaches at Financial Institutions
Stolen equipment (laptop, disks, tapes, documents, etc.)	36%	43%
Hacked systems	21%	13%
Unprotected web sites or accidental posting of data to the web	15%	5%
Lost equipment (laptop, disks, tapes, documents, etc.)	10%	15%
Fraud, scams, or social engineering (includes cases where an employee or contractor stole the data)	6%	10%
Improper disposal of documents	5%	6%

This suggests that financial institutions are doing better than other organizations regarding securing their web sites and systems, but are less successful when it comes to stolen and lost equipment and fraud/social engineering attacks. However, this data is collected through news sources and computer security lists, as mentioned earlier, so it is not comprehensive. Security breaches are likely to be under-reported for obvious reasons. Financial institutions in particular may prefer to quietly attempt to recover the data rather than make it public, as seen in the recent case of the UK tax office that lost two CDs containing sensitive information, including bank account numbers, on close to half the population of the country[5].

How attractive are MFIs to hackers and others with criminal intent? MFI core banking systems may be more vulnerable than the systems of large banks, due to the fact that they have fewer physical and electronic resources available to protect their systems, but MFI clients are not rich, so accessing an MFI database is not necessarily going to open a wealth of opportunity, both literally and figuratively, to hackers. Some regions, however, such as in Latin America, do give sizeable loans and have a more advanced IT sector, so in those regions the risk may be higher that access into an MFI's core banking system could lead to access to other database systems and greater repositories of wealth.

---

[2] Attrition.org, "Data Loss Archive and Database Open Source (DLDOS)," http://attrition.org/dataloss. This has now migrated to Open Security Foundation, "OSF Dataloss Database beta," http://datalossdb.org/.

[3] Data was retrieved on May 31, 2008 from attrition.org/dataloss/dataloss.csv. This is a comma separated value file that can be easily imported into Excel as well as various flavors of relational database. The attrition.org data goes back to 2000 but most of the data tracked begins in 2005 and is kept current. The data includes the number of records at risk and whether an arrest or prosecution was pursued.

[4] Financial institutions listed in the csv file include banks, credit unions, community banks, credit bureaus, stock brokerages, money transfer companies, financial data processing centers, mortgage companies, and insurance companies. Financial institutions fall under the category of Business, with Government, Education, and Medical institutions being the other broad classifications of organizations that reported data breaches.

[5] http://www.politics.co.uk/issueoftheday/opinion-former-index/economy-and-finance/hmrc-security-breach-$481844$481844.htm.

MFIs may face a greater risk from "insider" breaches, that is, employee-caused breaches, than from hacking or other external sources. Employees may find ways to create false accounts and false payments to funnel money to the desired recipient. A recent report from the Verizon Business RISK Team on over 500 forensic investigations conducted by Verizon[6] found that while insider breaches accounted for just 18 percent of the data breaches (external sources accounted for 73 percent and 39 percent involved partners[7]), insider breaches were the most damaging. The median number of records compromised during an insider breach exceeded that of external breaches by a factor of ten and was twice that of partner breaches[8]. Only 14 percent of the cases in Verizon's data set were financial services firms; the largest groups were retail firms (35 percent) and food and beverage companies (20 percent).

Partner breaches were not necessarily malicious but more likely to be due to lax security in the networks and information systems of the partner. The numbers due to malicious intent are still higher than one would like:

- 57% were due to weaknesses in their systems or networks

- 21% involved the partner but no individual was identified

- 16% were due to malicious intent of a remote IT administrator

- 6% were due to malicious intent of a remote or on-site partner employee

Technology can go a long way towards thwarting and identifying breaches. Referring to the case of the top ten core banking solution provider profiled in the Appendix, their core system products (as well as the core system products from other vendors) produce audit reports. These audit reports track data access in detail (date and time of access, by whom, terminal used, files or data elements accessed or updated, the data value before and after the update). It is possible to not only detect mishandling of data but also security access that may have been inappropriately granted to an employee (which could indicate collusion between employees). The major core banking systems available today have transaction level security that prohibits an employee from conducting a transaction they are not authorized to do. In addition, filters and edits are available that for example detect unusual account activity, which might indicate fraud. The problem with these types of tools is the amount of false positives they produce. Through fine tuning, the top ten vendor believes that these tools can prove quite effective in detecting external and internal fraud or account manipulation.

Policies and procedures are just as critical to ensuring the security of the core banking MIS. Creating the policies and procedures is not enough; the MFI must follow them, enforce them, and measure compliance. If the MFI's core banking system has tools such as audit reports, it is imperative that they use and actively analyze these reports. If they do not make this a required practice, they defeat the purpose of the tool and a key benefit of the core banking software. If audit reports or logfiles are not available, MFIs can consider a variety of other means to ensure that they have the right policies and procedures in place and that they are being followed, such as hiring an independent auditor to perform periodic audits similar to the SAS

---

6 Wade H. Baker and others, "2008 Data Breach Investigations Report," Verizon Business Risk Team, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

7 The percentages add up to more than 100 percent because multiple causes were suspected in some breaches.

8 Partners are any third party sharing a business relationship with the organization, such as vendors, suppliers, and contractors. Typically their systems are connected to each other to allow for the transmission of orders and invoices and other typical business transactions.

70[9] to examine the controls and safeguards in place, or an independent network security auditor to specifically evaluate the security of the computer software, systems and networks.

The data shows that many breaches are preventable through tighter controls over data replication and transport, and also shows that both insiders and partners are to blame for many breaches. The issue is not *if* a data breach will occur, but *when*, so the question becomes, who is more capable of recovering the data and closing the security hole? MFIs should be concerned but should consider whether they have more resources, both human and financial, than an outsourced solution provider, who generally has these resources, to prevent security breaches, and weigh this against the risks and their tolerance for the risks and consequences.

---

[9] American Institute of Certified Public Accountants (AICPA). "Statement on Auditing Standards (SAS) No. 70, Service Organizations," *SAS 70*. http://www.sas70.com/about.htm. A service auditor's examination performed in accordance with SAS No. 70 ("SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes. Service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

TIPS AND RECOMMENDATIONS FOR VENDOR SELECTION AND SYSTEM IMPLEMENTATION

These tips and recommendations are based on the researchers' interview with Catalyst Consulting Group[10], a consulting firm founded in 1998 to provide strategy and implementation consulting services to the banking and credit union industry. The firm's experts come from all sectors of the financial services industry, having served as senior managers or consultants at de novo banks to credit unions to the top 20 banks, technology service providers, international consulting firms, and the Federal Reserve Bank. The firm operates out of eight locations in the U.S. but has clients worldwide. Their clients range from $100 million to $100 billion in assets.

Jim Godish, the consultant interviewed, has over three decades experience, starting at Burroughs and Unisys. He has been involved with banking IT from both the application and hardware perspective, with his first 24 years focused on core and payment systems as well as branch automation, and became a consultant 11 years ago.

As Catalyst's clients are financial institutions, Mr. Godish provided the banker's perspective. He shared his experiences and insights about the outsourcing decision, evaluation and selection process, outsourcing perspectives, and advice and recommendations.

The next two tip sections are applicable to both buying a software package and outsourcing.

TIPS FOR THE REQUEST-FOR-PROPOSAL (RFP) DEVELOPMENT PROCESS

- Consultants may add value in this process because they use their past experiences and existing documentation as the basis to customize an RfP addressing the identified needs of their client, whereas an MFI would have to develop an RfP from scratch and have less experience developing RfPs.

- Consultants also do not need to delve into the micro-elements and develop a 500-item requirements document, because they know what the core banking system choices are, they have clients using solutions of all major vendors, and the software must meet regulatory requirements and has been vetted by regulators hundreds of times (these conditions may not exist in all countries).

- The corollary from this is that if a developing country's regulations are based on the U.S. or European standards, that U.S. or European software may work for them too. The software may conform to more regulations than necessary for the MFI, however, given the different scale and scope between the countries and between commercial banks and MFIs.

---

[10] More information is available at http://www.ccg-catalyst.com.

- Depending on the MFI's availability, it can take three to four months elapsed time (not level of effort) from issuance of the RfP to selection of the vendor. Core banking systems usually require a little more time.

TIPS FOR THE EVALUATION AND SELECTION PROCESS

- When using a consultant, the MFI should be open to the consultant's advice but ultimately the MFI knows its needs best.

- Create selection criteria to narrow down the list of vendors to about five that will receive the RfP.

- The evaluation and selection process could require only five to ten days of an executive's time depending upon the sophistication of the MFI's requirements.

> "At the original presentation, we say believe everything they say. But when you whittle it down to two (vendors) we say don't believe anything they say."

- Involve staff throughout the entire process as part of the educational process, at the times appropriate information is presented[11], so that they can learn from the experience and apply it at the time the vendor is selected.

- MFIs should weigh the facts and data learned during the evaluation process against their gut reaction, to see if the metrics are in sync with what their gut is telling them. For instance, is the MFI getting the sense that this vendor is truly committed to their success, to a long-term partnership (beyond the recurring revenue stream)? Will the vendor be easy to work with (possibly measured partly by how cooperative and responsive they were during the evaluation process)? Is the MFI getting the sense that the client references are truly representative of the experience of most of the vendor's customers?

- During the reading of the RFP responses and original vendor presentation, MFIs can "believe everything the vendors say". After whittling the list down to two finalists, however, "don't believe anything they say". The MFI should ask for case studies and demos – the "show me" test. They should do site visits and call the references.

- Anything that gives the MFI manager sleepless nights should be included in the selection criteria, negotiated, and addressed in the contract.

- Evaluate the vendor's viability by examining the vendor's financial position and asking the vendor for its most significant wins and losses over the last 12 months.

- The authors of this paper also recommend that during the evaluation and selection process, the MFI should ask the vendor the number of past major product releases, when they became available, and what they contained, as well as the vendor's schedule of product releases for at least the next two years. There should be some sort of product roadmap.

- An MFI should select the alternative that best supports its long-term business plans.

---

[11] For instance, loan officers would be involved in the review of the loan processing module, but not in the system architecture review. IT system administrators would be included in the system architecture review but not in the loan processing module review.

TIPS FOR MANAGING VENDORS DURING THE EVALUATION PROCESS

- Some vendors may prey on an MFI's lack of understanding of the core banking MIS market. Some vendors may try to teach the MFI how to buy their product and take advantage of the MFI's lack of knowledge. They may try to go around the consultant if the MFI is using one.

> "The adage which applies here is a verbal contract is not worth the paper on which it is written."

- Make sure the vendor is conveying information that is important to the MFI, not what is important to the vendor. Sometimes the vendors' objective is to teach the MFI what is best for the vendor and not necessarily what is best for the MFI.

- The MFI's concerns are different from what the vendor is thinking.

- Vendors can be too optimistic about their product's capabilities, leading an MFI to select a solution based on inaccurate data or worse yet altering its business plans in such a manner as to render them unobtainable.

- Outsourcing vendors will argue that with outsourcing, clients will always be on the latest technology, but this is not necessarily true. Customers with in-house solutions are kept-up-to-date also. They pay an annual maintenance fee which includes periodic product updates and upgrades in addition to hotline support.

- The goal is for the MFI to have control over the vendor selection process. If an MFI controls the way the vendors pitch their service, the MFI will be safer.

- The MFI can give the vendor a time limit on their presentation, no more than x hours or only ten minutes on the corporate background, for example.

- The MFI should explain the evaluation process step-by-step to the vendor and give the vendor a spreadsheet to fill out. They should define exactly how the vendor should respond and counteract optimistic responses by defining the answer choices and the meaning of the answers: "yes" means the functionality exists now; "no" means it does not exist; "maybe" means the vendor would be willing to provide it if paid to do it. Otherwise the vendor may try to indicate that features exist that do not actually exist yet.

- There can be a separate section for the vendor to expand on their answers and say anything they want about the product, such as a description of features due in the next release.

- Everything should be in writing.

TIPS FOR MANAGING VENDORS AFTER THE IMPLEMENTATION

- Vendors can become complacent by not improving their product.

- Vendors may start raising their prices solely for their own financial benefit.

- The authors of this paper recommend that when a vendor announces a price increase, the MFI should request and receive a detailed statement from the vendor describing what they will receive for the price increase, whether it is new features, increased levels of security, etc.

SUMMARY OF ADVICE AND RECOMMENDATIONS

- MFIs need to decide if technology is their core competency or not, where they are willing to invest capital and resources, and their TCO and expected return on investment.

- A financial institution must manage the vendor by controlling the selection and implementation process. An MFI should steer the vendors to respond to its needs and questions the way they want them to. By doing this, the institution is laying the groundwork with the vendor and asserting its position. The vendor's response during the selection process will be a good indicator of the vendor's level and quality of service after the institution becomes a customer.

- After implementation the MFI must continue to manage the vendor. An MFI can outsource the task to a core banking system provider, but it does not outsource the responsibility. It should never outsource the management of the system, that is, the manner in which it is used, or the MFI's institutional knowledge.

- A system adopted by an MFI needs to be able to grow in sophistication as the MFI does. The MFI should pick a product that will establish a good foundation for future products or services.

- If an MFI is considering outsourcing, they should try to select a system that they can eventually take in-house, to give themselves as many options as possible. Part of the evaluation process must then include an evaluation of the technology and architecture of the outsourced core banking system, to ensure that the MFI's IT staff is familiar with the technology and can support it.

RECOMMENDATIONS FOR MFIS BASED ON THE CASE STUDIES

- If an MFI has plans to grow, or offer a more complex suite of services, they should consider outsourcing.

- With outsourcing, an MFI may still need to scale up its Internet service, as more traffic will be going over their Internet connection.

- IT staff should be an integral part of the evaluation and selection process and the management oversight of the outsourced solution provider.

- Select a system with a track record, a history of positive customer references and a well-established base of customers.

- Pricing models vary from vendor to vendor and MFIs may be able to negotiate a better price or a more beneficial pricing model. Ask for tiered pricing or whichever pricing model you want if the vendor does not offer it.

- An MFI should ask the vendor for an independent security audit report (similar to the SAS 70 in the U.S.).

- Setup is a lot of work, so an MFI should plan to have enough staff and time for the setup.

- An MFI must allow time to learn the system. No system is "turnkey". Cutting training to save costs is self-defeating.

- It is important to fully analyze the TCO of any solution under consideration, whether it is a COTS that will be hosted in-house or an outsourced solution. The TCO must include the ongoing costs for the next three to five years, as often this is where the savings is seen in outsourcing.

- Vendor selection can be a complex decision. Consultants can help if an MFI can afford one. If not, there are other resources to help make the decision, create RFPs, etc. The Charles Waterfield document about an effective MIS, written in 2002, is still applicable[12]. CGAP and the Microfinance Gateway are excellent resources. Other studies of outsourcing, such as for "on-demand" applications of "Software-as-a-Service," have good examples to help calculate TCO. See the Bibliography at the end of this guide for more information sources.

---

[12] http://fieldus.org/Publications/index.html#mis.

APPENDIX:
CASE STUDIES OF VENDOR SOLUTIONS

This section presents summaries of the interviews with the vendors to hear their perspectives on their core banking system implementation experiences. *These summaries express the point of view of the interviewee and are not meant to represent the opinions of the research team, except where noted.* In some cases the interviewee commented on the draft of their summary and those edits were incorporated to provide clarification or corrections.

VENDOR CASE STUDY 1: TOP TEN PROVIDER OF CORE BANKING SOLUTIONS

(Note: to allow this vendor to speak more candidly, the vendor is not named and references to the vendor's products are in generic terms, as in "product X")

BACKGROUND AND PROFILE

Vendor X is a leading provider of core financial institution processing, card issuer and transaction processing services, mortgage loan processing and related information products and outsourcing services to financial institutions, retailers, mortgage lenders and real estate professionals. Vendor X has processing and technology relationships with the top 50 global banks, including the top 10. Vendor X maintains a strong global presence, serving over 9000 financial institutions. Their products support a range of financial institutions, from thrifts and credit unions, to community banks, to mid and large tier banks.

> **A Top 10 Vendor**
>
> **Type:** Vendor of information products and outsourcing services to financial institutions
>
> **Client Range:** Over 9000 financial institutions, from churches to the top 10 global banks
>
> **Key Points for MFIs:**
>
> - Involve IT people in the system selection
> - Do not be the first customer of a product
> - Invest in staff; do not cut back on training during the implementation
> - Do not neglect system documentation, especially if running an in-house system
> - Data security is more of a "people" problem, less a "system" problem

The research team met with a commercial product manager of Vendor X, focused on product development for one of their core banking solutions. He has been in and around the business for over three decades in various capacities—de novo and community banking, mortgage lending, regulatory oversight, and mergers and acquisitions. He was responsible for numerous data conversions and in the process saw every core system in the market and every perspective. His background is in accounting and data processing and he has served in executive level positions.

The product manager provided a vendor's perspective about in-house versus outsourcing, key decision factors, data security, data control and access, as well as a description of some of the product offerings including their implementation timeframes, hosting options, and regulatory conformance.

PERSPECTIVES ON IN-HOUSE VERSUS OUTSOURCING

The first question Vendor X asks banks is their preference for in-house or outsourcing. In his view, everyone has a bias and very few institutions are open-minded in their evaluation process in his opinion. In the interest of full disclosure, the product manager's bias is towards outsourcing. For him, the issue is that institutions need to focus on their core competency and for commercial banks that is usually not the IT aspect of their operation.

Vendor X offers both in-house and outsourcing options. They sell the software to a bank to host and maintain in-house, or Vendor X hosts and maintains the entire system for them. Vendor X can also do a variant of these two models by providing "facilities management" services, defined as hosting and running the bank's servers and mainframes for the bank. Vendor X provides the personnel and the expertise. The bank owns the equipment. For the bank, the benefit is that they do not need the personnel to support the systems and the equipment, and they feel they have more control because their data is on their own devices versus being shared with other banking clients on the same hardware.

The product manager cited several reasons why banks may prefer the in-house approach. A bank will tend to know its system better and feel they have more control because they are less dependent on a vendor. For the banks that have staff with the ability to program the system, they have more flexibility because they can design a product at night and release it the next morning (theoretically). On the other hand, an outsourced service provider could take two weeks to deliver the functionality, due to their need to consider the impact of the change on other client installations and their more formal processes to document and implement the change.

However, as technology advances, it becomes more difficult for staff to remain up-to-date, staff may not be willing or able to learn new technology, and the new technology may require new capital investments which a bank may not want to make. Outsourcing becomes more and more appealing for these banks.

The idea of having more control with in-house systems is a bit of a fallacy, in the opinion of the product manager. With outsourcing, a bank has a contract with a vendor, establishes service level agreements (SLAs), and holds the vendor to the terms. With in-house support, bank managers do not have as much control as they might think with respect to their own operations team. People are not truly available on a moment's notice. IT staff will leave for other jobs and leave behind poorly documented or undocumented code and procedures, making it more difficult for the person taking over that function. Managers and staff interact not only on a professional level but also on a personal level, so when a member of the team is frequently calling in sick or the team's performance is declining, it is more complicated for the managers. The team is not meeting the operational SLAs. The bank runs the risk of not achieving the gains in productivity they predicted because they are setting the rules and holding themselves accountable. With a vendor, the bank has a financial and SLA relationship, not a personal one, eliminating one of the limitations of managing an in-house team.

Generally it is better for Vendor X to receive a steady revenue stream from outsourcing than from a one-time sale for an in-house system. For the financial institutions, outsourcing has a lower up-front cost because the cost is spread out over time.

DECISION FACTORS WHEN CHOOSING IN-HOUSE VERSUS OUTSOURCED SOLUTIONS

The product manager observed that ten years ago in the U.S., most financial institutions made their own selection decision. Nowadays, the majority makes the decision with the help of a consultant. The institutions do not have the time or resources to keep up with the industry consolidations and technology changes, so they rely on the consultant. It is too big of a challenge and the interpretation of the choices and information is difficult.

Consultants also understand what the key decision factors should be. The bank does not always know what the best or highest priorities should be, whereas the consultants are more knowledgeable based on their experience with numerous banks and vendors, the product manager argued. Consultants can also be more objective. Banks should start with the environmental factors such as availability of resources, or having people who know how to maintain the servers or mainframe. Banks need to be clear about how much initial capital they have to spend on the solution. They need to recognize their business focus and model: are their operations simple and will stay simple, or do they plan to grow but not offer any unusual products or services?   Is much of what they want to do not available in the market so they will need to create it themselves, and therefore own the source code and have a skilled programming team to build and maintain the system?

Financial institutions need to consider the impact on their infrastructure; with outsourcing there will be more network traffic between the bank and the outsourced service provider than there would be with an in-house system, so the amount of increased traffic needs to be estimated to determine if the bank's existing infrastructure needs to be enhanced and what the associated short and long term costs would be.

> "I came to a de novo financial institution. …. They bought an in-house computer system before I got there. … The banking application was … supposed to be a national product. Within three months I was running all of our loans on an Excel spreadsheet because the system couldn't do accruals correctly. Basically, you had non-IT people running an IT product."

Lastly, time to market could be an issue. It is much faster to implement an outsourced solution than to implement it in-house because the core solution provider already has all the infrastructure, hardware, and people in place. In addition, vendors that serve the U.S. market have refined their implementation processes over the course of hundreds, even thousands, of customer implementations, whereas the bank staff may have participated in at best one or two implementations. All of these issues affect which vendor to select in addition to which approach to take, in-house or outsource.

DATA SECURITY

Anecdotally data security is often cited as a major reason for not outsourcing. The product manager's security concerns centered more on the human element rather than on technology or system weaknesses in the outsourced solution provider's environment that leave files open to unauthorized view. He would have to dig pretty deep to find a problem with customer data being co-mingled with other customer data on the servers. The product manager is more concerned with breaches such as accidental exposure of other people's data because an employee left a customer list on the desk at night before the cleaning crew arrived. This can happen at a financial institution or the outsourced solution provider. Another major concern is with a customer or a business being duped into disclosing account information to someone.

Vendor X has passed every SAS70 examination, yet even with all the proper controls and procedures in place, total control over employees is not realistic. A disgruntled employee can still figure out a way to take sensitive information to a competitor or the highest bidder.

DATA CONTROL AND ACCESS

Audit reports are produced by every core system. They include time of access, files accessed, employee or terminal that accessed the data and often before-and-after changes. The product manager states that it is imperative that the financial institution access and analyze these reports. It is possible to not only detect mishandling of data but also security access that may have been inappropriately granted to an employee. In terms of of a bank requesting data dumps, these would be produced in an encrypted format and delivered to the financial institution through a number of means depending on the size of the files – ftp, web vault, tape, etc. Most core systems today have gone to transaction level security that prohibits an employee from conducting a transaction they are not authorized to do. In addition, filters and edits are available that detect unusual account activity, for example, that might indicate fraud. The problem with these types of tools is the amount of false positives that are produced. Through fine tuning, these tools can prove quite effective in detecting external and even internal fraud or account manipulation. Vendor X offers a host of fraud control and security options to their customers.

PRODUCTS AND IMPLEMENTATION

Vendor X offers several different core processing solutions targeted at different types of financial institutions. Commercial bank product A is targeted at de novos to banks with $40 billion in assets. Commercial bank product A is a mainframe database system utilizing Unisys hardware and can be run in-house or outsourced.

A sister product of Commercial bank product A, (call it Credit Union Product B), is targeted at credit unions with $50,000 to $400,000 in assets, but has become popular with churches who lend to their congregations and take deposits. It is a "credit union in a box" and performs basic lending and deposit functions. It runs on one PC, based on Microsoft Windows and Access for the database, written in Visual Basic and C. Vendor X offers this only as an in-house solution. They did consider offering it as an outsourced service but determined that it would be more expensive for their customers than running it in-house.

Small Bank Product B is the equivalent product to Credit Union Product B but is for banks. According to the product manager, approximately 47 percent of de novo banks in the U.S. opened their bank with Small Bank Product B, so it has been very popular with new financial institutions in the U.S. Most of the implementations are outsourced and implemented "out of the box", with little customization.

Implementation time is easiest and fastest for de novo banks, because there is no data to convert. With Small Bank Product B, a bank can be live and functional in two months from signing of the contract. Part of that time is spent waiting for the infrastructure setup, hardware installation, and training. For Commercial bank product A, which runs on Unisys equipment and a proprietary operating system, the actual conversion to the system can take 7-13 months. Banks also need to allow time to review the contract at service renewal time. Some take over one year to review the contract.

Vendor X aims to be a solution provider, not simply a provider of software and hardware. They have started offering business intelligence solutions that help banks with decision-making, that is, helps them

analyze large volumes of data, see trends and patterns by multiple dimensions such as time, product, business unit, or region. They felt that banks need this support and they can help them through these processes.

Governance has become the leading system requirement as all systems contractually agree to comply with Federal Regulation. Product development is driven first from the financial sector regulations. The Commercial bank product A product team has monthly regulatory reviews. They gather information from a variety of sources including a technology advisory board, industry experts, new business requests, their customer enhancement request database, and technical support cases. New customers have a greater influence on this type of product than on a mass consumer application like word processing.

Pricing varies on either number of accounts or asset size depending on the particular system.

THE PRODUCT MANAGER'S LESSONS LEARNED

- **Too often non-IT people are selecting and running an IT product.** Non-IT people can be more easily swayed by "eye candy", a glitzy presentation or demo. The evaluation team should be a multi-disciplinary group representing the banks's needs and functions – IT, bank operations, lending, account manager, sales, senior management, etc.

- **Banks should avoid being the first customer to use a vendor's solution**. Be sure that the vendor has a track record of success and satisfied customers.

- **Banks need to invest in their staff when implementing a core banking solution. They should not skimp on training.** Vendor X has seen that often the first item to be cut to save on the implementation cost is training and this is the last item that should be cut. If the bank needs to save on the implementation cost, it would be better to cut back on the hardware than cut back on training. It cannot be delayed until after the installation; by then it will never happen because the customer is up and running and has less time for training, yet probably needs it even more.

- **System documentation is critical, especially if the bank is running their system in-house.** Staff turnover is inevitable so the documentation, such as system configurations and customizations, business processes and procedures, data definitions, workarounds, and service level agreements with vendors, will be critical to the person taking over the job. Even in an outsourced environment, the staff still needs to understand how the system works and how it is configured or customized, so the documentation is still crucial.

VENDOR CASE STUDY 2: MFI CORE BANKING PRODUCT EXAMPLE FROM IBM

BACKGROUND AND PROFILE

While the IBM processing hubs are not yet online and serving MFIs, the purpose of profiling this initiative is to understand how a large multinational corporation made both the business and social case to provide an outsourced core banking platform for MFIs in developing countries, and learn more about the business model and planned services and features for MFIs.

In December 2007, IBM and CARE issued a press release announcing their plans to build an "Africa Financial Grid" which would provide a shared platform—comprised of the core banking software

applications, hardware, and necessary infrastructure—to serve MFIs' core banking MIS needs in Africa. Their "shared services and infrastructure model" is "designed to help MFIs reduce operating costs, streamline lending processes, scale rapidly, and integrate with other resources such as credit bureaus, financial institutions and international payment networks. The Grid will also eventually be able to flexibly link with telecommunications companies or other mobile payment providers in Africa to enable customers to repay loans or carry out money transfers via mobile phones or other devices"[13].

According to IBM, an MFI would need only an inexpensive PC and Internet access to connect to the Grid, also known as a "processing hub", using a web browser to log in and use the core banking MIS (IBM is designing an offline processing capability for use in areas with limited connectivity). No large upfront investment for hardware servers or software licenses would be necessary. The processing hub would operate on the Software-as-a-Service (SaaS) model (the same as outsourcing for the purposes of this study): an MFI would pay on a per account or per client or per transaction basis, essentially renting access to the hub, as opposed to buying a software package or building from scratch. The MFI could outsource most of its IT and software development operation and pay to use the hub on an on-demand basis.

The microfinance processing hub concept has its roots in two IBM innovation events. In the summer of 2006, microfinance was one of the most active discussion topics in the IBM Innovation Jam, a global online brainstorming session involving 150,000 clients, partners, and employees across 104 countries. The Grid concept was also investigated 18 months ago when IBM held its annual Global Innovation Outlook event.

> **IBM**
>
> **Type:** Multinational IT company providing products, professional services, research and development
>
> **Client Range:** Provides outsourced IT operations and data centers for large banks and telecommunications companies
>
> **Key Points about the Processing Hubs:**
>
> - Will require only a PC and an Internet connection; no large upfront investment in hardware
>
> - Will operate on a "Software-as-a-Service" model: pay per account, per client, or per transaction
>
> - IBM is developing the Latin America hub
>
> - IBM and CARE are partnering on the Africa hub; currently conducting feasibility studies

As a result, the IBM microfinance team, based in New York but operating globally, has been working since September 2006 with the mandate to innovate entirely new business models that can dramatically increase the ability of poor communities around the world to access basic financial services. They have traveled to more than 20 countries around the world. Part of the team is working on the processing hub/outsourced solution. IBM also mined its own experience with implementing financial systems in developing countries. They closely examined two cases where IBM was involved either as the technology provider or systems integrator: (1) at FINO in India, incubated by ICICI Bank and (2) BANSEFI in Mexico where IBM was heavily involved (BANSEFI today has 3.5 million accounts), as well as other IBM projects involving mobile banking. They conducted extensive research into cost analysis and comparisons analyzing current IT cost per account at MFIs of varying sizes and service levels around the world.

---

[13] IBM. "IBM and CARE Partner to Advance Microfinance in Africa." Press release, December 4, 2007. http://www-03.ibm.com/press/us/en/pressrelease/22761.wss.

In Phase 2 of their research, they examined locations that would be most conducive to the implementation of a microfinance processing hub. They saw a great need for this service in Africa, but the business case was a challenge. Africa is very diverse, pricing pressures are high, and MFIs already operate at a low cost per transaction out of sheer necessity. Regulation and infrastructure also present challenges. Also, currently IBM does not have a large presence in the continent. IBM saw the risks as high and spread across many countries, with financial returns not happening for several years. However, during this time IBM was also in conversations with CARE International. CARE liked IBM's processing hub model and knew where and how to pursue funding for the project. IBM and CARE together developed the business and cost cases, meeting both the for-profit and development objectives.

TARGET MARKET

In IBM's analysis, MFIs today are very diverse in terms of coverage and operating maturity. Some MFIs are quite large (100,000+ customers) and operate much like established banks, while others are very small (100-1000 customers). According to IBM, large MFIs may already have made large IT investments, and their processes are well-established and they are therefore less interested in moving off their existing platforms. Small MFIs often operate in very unique ways, with business processes that are developed at a grassroots level, and it is difficult to make a case to add features that benefit just one MFI. IBM recognized this wide spectrum and took this into account in its marketing plans. For now it believes that the "middle" of the MFI market is the best target market for the processing hub.

IBM's intent is to create a neutral platform so that MFIs will feel comfortable migrating to the platform. IBM and CARE are not themselves financial institutions and thereby hope to minimize any concerns related to data ownership and conflict of interest that MFI clients may have.

PLANNED SERVICES AND FEATURES

The hub will eventually provide full support for integration with payment networks, four broad product services (credit, savings, payments, and insurance), comprehensive reporting capabilities, regulatory compliance with national government regulations, automated reporting for donors, and social performance reporting.

IBM will leverage its experience running outsourced IT operations and data centers for many of the largest banks and telecommunications companies around the world. According to IBM, these data centers have world-leading security measures such as biometrics and are "level 4" data centers, which is the classification describing the highest level of availability and fault tolerance that a data center can achieve[14]. IBM will leverage these assets and areas of expertise in building the microfinance processing hubs.

IBM will also bring the governance model it has developed through its experience running data centers for banks and telecommunications companies, describing rules of engagement, ownership issues, and roles and responsibilities, to name a few components. This is part of a toolkit of services or "assets" that IBM is offering which bundles critical services and support required to ensure an MFI's success with the microfinance processing hub: an "onboarding" process to assist the MFI with migrating its data and

---

[14] For an overview describing level 1 through 4 classification of data center availability, see http://www.adc.com/Library/Literature/102264AE.pdf or http://www.uptimeinstitute.org/cgi-bin/admin2/admin.pl?admin=view_whitepapers.

processes to the hub and includes training; security to protect the hub operations and MFI data from both internal and external vulnerabilities; and customer management which will include analytics, customer profiling, and segmentation analysis.[15]

STATE OF PLATFORM DEVELOPMENT

IBM says that they are actually well down the path to creating a processing hub to serve Central and South America. They mobilized a local team at the end of 2007, have the commitment of several institutions and MFIs, identified specific markets and are gathering requirements. The team is working on the solution design in Mexico, comprised of team members from India, Mexico, and the U.S., translating the requirements into the system design.

The Africa hub is not as far along as the Latin America hub, as the environment is more complex – more diverse processes, more stakeholders, more due diligence required around regulatory requirements, tax implications, and connectivity. The timeline for the Africa hub is also longer than that for the Latin America hub. The South Africa team is holding discussions with MFIs and carrying out a feasibility study to understand how MFIs are operating in the field today, and to verify the understanding of what their key needs are. A potential barrier that IBM is researching is regulations that may define whether transactions processing must execute and data must reside in the country where the MFI operates. Delivery channels are likely to be a main focus of the Africa hub.

In parallel, IBM has been working with Grameen Foundation in a partnership to help them accelerate the development of Mifos, an open source microfinance core banking platform. IBM is very interested in using Mifos in it's processing hubs, but must first ensure that Mifos will meet the requirements for security, scalability, and functionality of the hubs, which will also be somewhat unique for each region. Mifos is a relatively new solution in the market but has achieved an impressive first version which was released in 2007. Today, IBM has seven people in Dublin and four in Bangalore working with Grameen on Mifos 1.1.

REVENUE MODEL

The Latin America hub is owned by IBM so all revenue will accrue to IBM, whereas in Africa, CARE will finance the implementation of the Africa Grid, and IBM and CARE will have a profit-sharing arrangement that will take effect once the operation becomes cash flow positive. IBM and CARE recognize that many variables will affect the time period in which the hub will become cash flow positive. For this reason, this innovative public-private partnership was seen as an ideal way to tackle this important opportunity. IBM and CARE believe that the Africa Financial Grid will be able to deliver savings to MFIs while providing more flexible, secure, and scalable software, and ultimately enable MFIs to greatly expand their reach to poor communities across Africa.

FUTURE PLANS

IBM has longer range plans to establish processing hubs in China, Russia, and most recently Indonesia. In February 2008 IBM issued a press release announcing the collaboration between IBM, PT Permodalan

---

[15] For the full description of the toolkit, see IBM's presentation describing the processing hubs for microfinance, available at http://technology.cgap.org/technologyblog/wp-content/uploads/2008/02/processing-hub-public-121920071.pdf.

Nasional Madani (PNM), a unit of the Ministry of Finance, and PERBARINDO, an Indonesian rural banks association, to establish a shared financial services platform for rural credit banks[16].

---

[16] IBM, "IBM, PT Permodalan Nasional Madani and PERBARINDO Collaborate to Enhance Microfinance Capabilities of Rural Credit Banks in Indonesia," Press release, February 14, 2008, http://www-03.ibm.com/press/us/en/pressrelease/23517.wss.

SELECTED BIBLIOGRAPHY

Below is a list of sources, both cited and not previously cited, used in the preparation of this Decision Guide. It is not meant to be a complete record of all sources used, but is provided for the convenience of the reader who wish to learn more about any of the topics listed.

OUTSOURCING FOR MICROFINANCE

CARE. "Africa Financial Grid – A CARE-IBM Partnership to Revolutionize IT for Microfinance." CARE, February 2008. http://edu.care.org/Documents/Africa Financial Grid - MFI Intro - Feb 08.pdf.

CARE. "IBM and CARE Partner to Advance Microfinance in Africa." Press release, December 2007. http://www.care.org/newsroom/articles/2007/12/20071205_ibmpartnership.asp.

IBM. "IBM and CARE Partner to Advance Microfinance in Africa." Press release, December 4, 2007. http://www-03.ibm.com/press/us/en/pressrelease/22761.wss.

IBM. "IBM, PT Permodalan Nasional Madani and PERBARINDO Collaborate to Enhance Microfinance Capabilities of Rural Credit Banks in Indonesia." Press release, February 14, 2008. http://www-03.ibm.com/press/us/en/pressrelease/23517.wss.

IBM. "IBM Processing Hub for Microfinance – A Discussion Document." IBM, December 2007. http://technology.cgap.org/technologyblog/wp-content/uploads/2008/02/processing-hub-public-121920071.pdf

IBM. "Banking the Unbanked – Expanding Financial Services Access." Presentation, Apconex 2008, Jakarta, Indonesia, May 8, 2008. http://www.apconex.net/2008/download/presentation/day2/bpr/IBM - Microfinance in Indonesia.zip.

MIS FOR MICROFINANCE

CGAP. "Information Systems: Frequently Asked Questions." http://www.cgap.org/gm/document-1.9.2017/IS_Technology_FAQs.pdf.

Waterfield, Charles. "MIS for Microenterprise: A Practical Approach to Managing Information Successfully." The Aspen Institute, 2002. http://fieldus.org/Publications/index.html#mis.

Waterfield, C., N. Ramsing. "Management Information Systems for Microfinance - A Handbook." CGAP Technical Tool Series February 1998. http://www.microfinancegateway.org/content/article/detail/1631/.

OTHER OUTSOURCING REFERENCES

Barry, Christine. "Evaluating the Vendors of Small Banks' Core Banking Systems: Effective Cross-Selling is the Key to Success." The Aite Group, January 2007. http://www.aitegroup.com/reports/200701291.php.

CGI. "Principle-centered Sourcing: Guiding Principles that Shape Successful Outsourcing Partnerships." CGI, October 2006. http://www.banktech.com/whitepaper/Architecture/Infrastructure/principle-centered-sourcing:-guiding-principles-thwp1212966444702?articleID=19600036.

Gillis, Art. "Outsourcing is Now More Popular With Banks than In-House, and Bill Gates Knows Why." *Bank Systems and Technology: The Blog*, May 12, 2008. http://banktech.com/blog/archives/2008/05/outsourcing_is.html.

Healey, Michael and Heather Vallis. "SaaS: Red Light, Green Light." *Information Week*, April 21, 2008. http://i.cmpnet.com/informationweekreports/doc/2008/207400212.pdf.

Magda, Beverly. "SaaS To The Rescue." *Information Week*, May 19, 2008. http://i.cmpnet.com/informationweekreports/doc/2008/207800343.pdf. Includes a CIO SaaS checklist and tips for success with SaaS.

Varanasi, Ramprasad and Pradeep K. Mukherji. "Relationships at the Core of Successful Outsourcing Contracts." Edited by Avinash Vashistha. Tholons, August, 2007. http://www.tholons.com/nl_pdf/070731_Core_Successful_Outsourcing_Contracts.pdf.

TOTAL COST OF OWNERSHIP

Aggarwal, Sanjeef. "TCO of On-Demand Applications Is Significantly Better for SMBs and Mid-Market Enterprises." The Yankee Group, June 1, 2005. http://www.netsuite.com/tco.

Conry-Murray, Andrew. "TCO Analysis: Software as a Service – Same Dog, Different Fleas." *Network Computing*, March 5, 2007. http://www.networkcomputing.com/showArticle.jhtml?articleID=197700166.

Kingstone, Sheryl. "Understanding Total Cost of Ownership of a Hosted vs. Premises-Based CRM Solution." The Yankee Group, June 2004. http://www.bakerhill.com/emcfiles/folderdocid7788/yankee_white_paper_TCO_vs__premise.pdf.

DATA SECURITY AND DATA BREACHES

American Institute of Certified Public Accountants (AICPA). "Statement on Auditing Standards (SAS) No. 70, Service Organizations." SAS 70. http://www.sas70.com/about.htm.

Attrition.org. "Data Loss Archive and Database Open Source (DLDOS)." http://attrition.org/dataloss.

Baker, W.H., C.D. Hylender, J.A. Valentine. "2008 Data Breach Investigations Report." Verizon Business Risk Team. http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

Brown, Colin and Ben Russell. "Lost in the post: the personal details of 25 million people." *The Independent,* November 21, 2007. http://www.independent.co.uk/news/uk/politics/lost-in-the-post-the-personal-details-of-25-million-people-758867.html.

Open Security Foundation. "OSF Dataloss Database beta." http://datalossdb.org/. (note: attrition.org is migrating DLDOS to this database).

Politics.co.uk, "HMRC Security Breach." November 21, 2007. http://www.politics.co.uk/issueoftheday/opinion-former-index/economy-and-finance/hmrc-security-breach-$481844$481844.htm.

Smith, Robert Ellis. "Laptop hall of shame." *Forbes,* September 7, 2006.
http://www.forbes.com/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html.

REGULATIONS
FFIEC IT Examination E-Banking Handbook, pages 26-30, Information Security Program.
http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf.

U.S. Government Export Portal. "Safe Harbor Overview."
http://www.export.gov/safeharbor/SH_Overview.asp.

DATA CENTER MANAGEMENT
Renaud, V., J.H. Seader, W. P. Turner IV. *"*Operational Sustainability and Its Impact On Data Center
Uptime Performance, Investment Value, Energy Efficiency, and Resiliency." The Uptime Institute, May
15, 2008. http://uptimeinstitute.org/cgi-bin/admin2/admin.pl?admin=wp_form&id_field=30.

Turner IV, W. Pitt, J.H. Seader, V. Renaud, K.G. Brill. "Tier Classifications Define Site Infrastructure
Performance." The Uptime Institute, May 15, 2008. http://uptimeinstitute.org/cgi-
bin/admin2/admin.pl?admin=wp_form&id_field=9.

U.S. ORGANIZATIONS WITH A FOCUS ON FINANCE FOR LOW AND MODERATE INCOME POPULATION
Community Development Financial Institutions Fund, http://www.cdfifund.gov/.

Credit Builders Alliance, http://www.creditbuildersalliance.org/.

SOFTWARE PROJECT MANAGEMENT AND DEVELOPMENT
Brooks, Frederick P., Jr. *The Mythical Man-Month: Essays on Software Engineering*. Boston: Addison-
Wesley, 1975. Anniversary edition with four new chapters, 1995.