HANDBOOK

ALTERNATIVE DELIVERY CHANNELS AND TECHNOLOGY

SoftwareGroup
doing it right

The MasterCard Foundation

IFC International Finance Corporation
WORLD BANK GROUP

ACKNOWLEDGEMENTS

The authors would like to thank the IFC team: Andrew Lake, Charles Niehaus, Joseck Luminzu Mudiri, Lowell Campbell, Greta Bull and Margarete Biallas for their contributions to the development of this handbook including in-depth reviews and invaluable insights. Also, many thanks go to Anna Koblanck and Bonny Jennings for making this handbook a user-friendly and easy-to-read resource.

This handbook was inspired by our clients and partners, many of whom have shared their experiences with us over the past few years and with whom we have partnered to scale up the provision of financial services through alternative delivery channels. In particular, we'd like to thank Denis Moniotte of Microcred, Nick Meakin of Urwego Opportunity Microfinance Bank and Kea Borann of AMK Cambodia for either providing specific feedback on the drafts or for allowing us to share their experiences in the handbook. The authors would also like to acknowledge the partnership with The MasterCard Foundation, particularly Ruth Dueck-Mbeba and the financial inclusion team, without whom this handbook would not have been realized.

Finally, the authors would like to note that any errors, either of omission or commission, in this document are entirely their own. The views presented herein represent those of the authors and the IFC team working on this paper, and are not an official position of the World Bank Group.

ISBN Number: 978-0-620-70761-9

HANDBOOK

ALTERNATIVE DELIVERY CHANNELS AND TECHNOLOGY

SoftwareGroup
doing it right

The MasterCard Foundation

IFC International Finance Corporation
WORLD BANK GROUP

SMS

CONTENTS

ACRONYMS

ADC	Alternative Delivery Channel
ADSL	Asymmetric Digital Subscriber Line
AML	Anti-Money Laundering
API	Application Programming Interfaces
ATM	Automated Teller Machine
BCP	Business Continuity Planning
BPR	Business Process Reengineering
CBS	Core Banking System
CFT	Combating the Financing of Terrorism
CIG	Core Implementation Group
CMS	Card Management System
CVV	Card Verification Value
DR	Disaster Recovery
DTMF	Dual Tone Multi Frequency
e-banking	Electronic Banking
e-money	Electronic Money
e-wallet	Electronic Wallet
EFT	Electronic Funds Transfer
EMV	Europay, MasterCard, and Visa
EOI	Expression of Interest
FAR	False Acceptance Rate, also known as False Matching Rate
FI	Financial Institution
FRR	False Rejection Rate

FSP	Financial Services Provider
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HCM	Human-Centered Design
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IMEI	International Mobile Equipment Identity
ICT	Information and Communication Technology
ICC	Integrated Circuit Card
iOS	Operating System developed by Apple
IP	Internet Protocol
IRR	Internal Rate of Return
ISO	International Organization for Standardization
IVR	Interactive Voice Response
J2ME app	Java 2 Platform, Micro Edition
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KYC	Know Your Customer
LAN / WAN	Local Area Network / Wide Area Network
m-banking	Mobile Banking
m-wallet	Mobile Wallet

Magstrip	Magnetic Strip Card
MDM	Mobile Device Management
MFI	Microfinance Institution
MFS	Mobile Financial Services
MIS	Management Information System
MM	Mobile Money
MNO/MVNO	Mobile Network Operator/ Mobile Virtual Network Operator
mPOS	Mobile Point of Sale
MTI	Message Type Indicator
NFC	Near Field Communication
OS	Operating System
OTA	Over the Air
OTC	Over the Counter
OTP	One Time Password
PDA	Personal Digital Assistant
POS	Point of Sale
PRSP	Premium Rate Service Provider
PSP	Payment Service Provider
RFI	Request for Information
RFP	Request for Proposal
ROI	Return on Investment
SaaS	Software as a Service

SIM	Subscriber Identification Module
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SSM	Software Security Module
STK	SIM Application Toolkit
SWOT	Strengths, Weaknesses, Opportunities, Threats
TAC	Type Approval Code
TAN	Transaction Authentication Numbers
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
UAT	User Acceptance Testing
URL	Internet Shortcut
USSD	Unstructured Supplementary Service Data
VAS	Value Added Services
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VSP	Virtual Service Provider
WAP	Wireless Access Protocol
Wi-Fi	Wireless Internet
XML	Extensible Markup Language
3G	3rd Generation Mobile Network
4G	4th Generation Mobile Network

Introduction

The ambition to reach full global financial inclusion requires that we address the challenge of delivering appropriate and affordable financial services to an estimated 2.5 billion unbanked individuals globally. One response to this challenge has involved the design of products such as microloans, low balance savings accounts, micro-insurance, and mobile money transfer that are specifically tailored to meet the needs of the often excluded low-income mass market. Delivering these products and services on a large scale, however, cannot be achieved without accessible channels that lower the cost of service and increase reach.

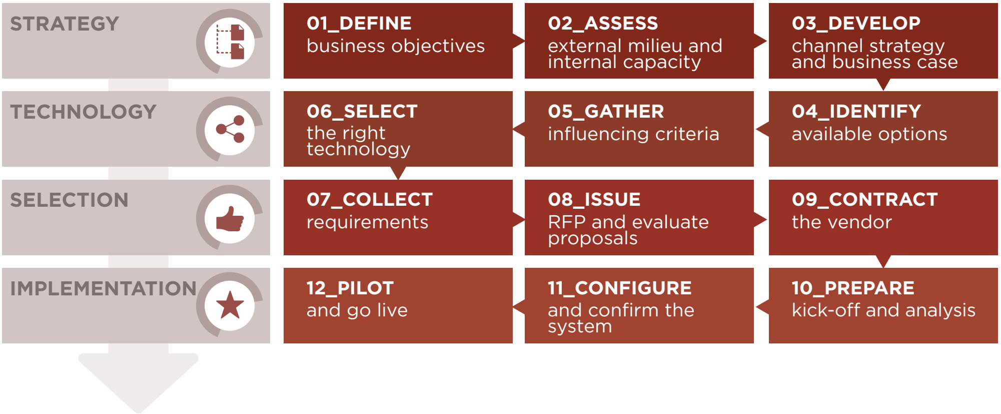
Alternative delivery channels, defined as those channels that expand the reach of services beyond the traditional bank branch channel, have emerged as a result of innovations in information and communication technology and a shift in consumer expectations. ADCs are transformative in nature, accommodating the demand for access to financial services "anytime, anywhere, anyhow". They rely heavily on information and communication systems and devices ranging from ATMs to mobile phones, all of which enable the instant transmission of financial and non-financial information between the customer and financial services providers. New technologies increase efficiency through automation, reduce operational costs, and improve service quality by cutting down on waiting times and offering more convenient access and reduced cost to the end-consumer.

For Financial Services Providers, particularly microfinance institutions, ADCs can help improve operational efficiency and cost-effectively expand outreach. Unfortunately, many FSPs lack the technical knowledge or skills needed to successfully implement ADCs. This includes not only the skills to manage the detailed implementation of ADC projects, but also the skills needed to navigate a competitive and crowded marketplace and build a relevant ADC strategy. Other factors beyond skills, such as a history of failed or painful IT implementations, limited budgets, and regulatory constraints can also result in poorly planned and implemented ADC projects. The net result is a patchy distribution of ADC success stories and many disappointing experiences, with poor uptake on channel platforms that are clunky, inflexible or costly.

The world of ADC technology, with the wide range of delivery channels, technology platforms, and communications and device options on offer, can be daunting, particularly for FSPs that have limited technical capacity. This handbook serves as a tool for FSPs to increase the technical understanding of ADC platforms and to provide practical guidance on how to approach an ADC technology project. While the focus is on the technical aspects of ADC projects, there are a host of other market and business factors to consider, which are introduced and discussed in brief where relevant. To help orient the reader, each chapter first covers the relevant business aspects before delving into the more technical considerations for readers seeking deeper insight.

The handbook has been organized according to a phased implementation framework illustrated in Figure 1. This framework is based on the understanding that all ADC projects must be based on a well-researched channel strategy that guides all future steps in the implementation process. Equipped with a strategy, the next step for the FSP is to consider and select the technology

Figure 1: ADC technology implementation process


STRATEGY
TECHNOLOGY
SELECTION
IMPLEMENTATION
01_DEFINE business objectives
02_ASSESS external milieu and internal capacity
03_DEVELOP channel strategy and business case
04_IDENTIFY available options
05_GATHER influencing criteria
06_SELECT the right technology
07_COLLECT requirements
08_ISSUE RFP and evaluate proposals
09_CONTRACT the vendor
10_PREPARE kick-off and analysis
11_CONFIGURE and confirm the system
12_PILOT and go live

> *This framework is based on the understanding that all ADC projects must be based on a well-researched channel strategy that guides all future steps in the implementation process.*

platform(s) best suited to the strategy. This step is a prerequisite to vendor selection, as it forms an important input to the requirements or specifications used to select the vendor(s). Once this information is available, and a vendor or partner selected, the FSP can finally implement the preferred channel solution. This framework will be referred to throughout the handbook. In addition, the handbook contains a glossary to fully explain the terms used in the document. It may be advisable to review this before launching into the handbook, to refresh the reader's understanding of the key terms and concepts as a background to the discussion. Lastly, to help FSPs apply the information in this guide to real-life scenarios, checklists are included at the end of the handbook. These checklists will help FSPs determine the key decisions or activities that should be completed at the strategy, selection and implementation stages.

It is difficult to estimate how long an ADC project will take or what financial resources it will require, as institutional capacity and context vary widely from situation to situation. This guide should give a variety of FSPs some fundamental direction for any ADC project and equip project teams with the basic tools to successfully navigate the process.

The handbook is structured as follows:

- **Chapter 1** provides an overview of ADCs and the technologies that underpin them.
- **Chapter 2** offers guidelines to develop a channel strategy, taking into account the internal and external factors that impact strategy decisions.
- **Chapter 3** outlines the different components of a technology platform, aiming to provide guidance on how the channel strategy can be mapped to a specific technology platform.
- **Chapter 4** highlights the importance of identifying requirements and outlines the steps involved in selecting the right provider and solution.
- **Chapter 5** introduces a best-practice implementation methodology and key considerations for a successful implementation. In addition, the chapter discusses how a channel should be monitored, maintained and scaled up after going live.

TECHNICAL DISCUSSION

Those interested in a more technical discussion can refer to the "From a Technological Perspective" sections included in most chapters.

See From a Technological Perspective

CHAPTER 1

Basic concepts and terminology

ADC implementations by FSPs employ many delivery approaches and use different terminologies, such as ‘e-banking’ and ‘branchless banking’. These variations in approaches and terminology are in part contributing to some of the confusion in the financial services sector about channels and technology. Hence, this chapter aims to ensure that all readers have a common understanding of the terms used in this handbook, and to introduce some of the basic concepts that will be referenced as we progress through the details of strategy, technology, selection, and implementation.

Alternative delivery channels

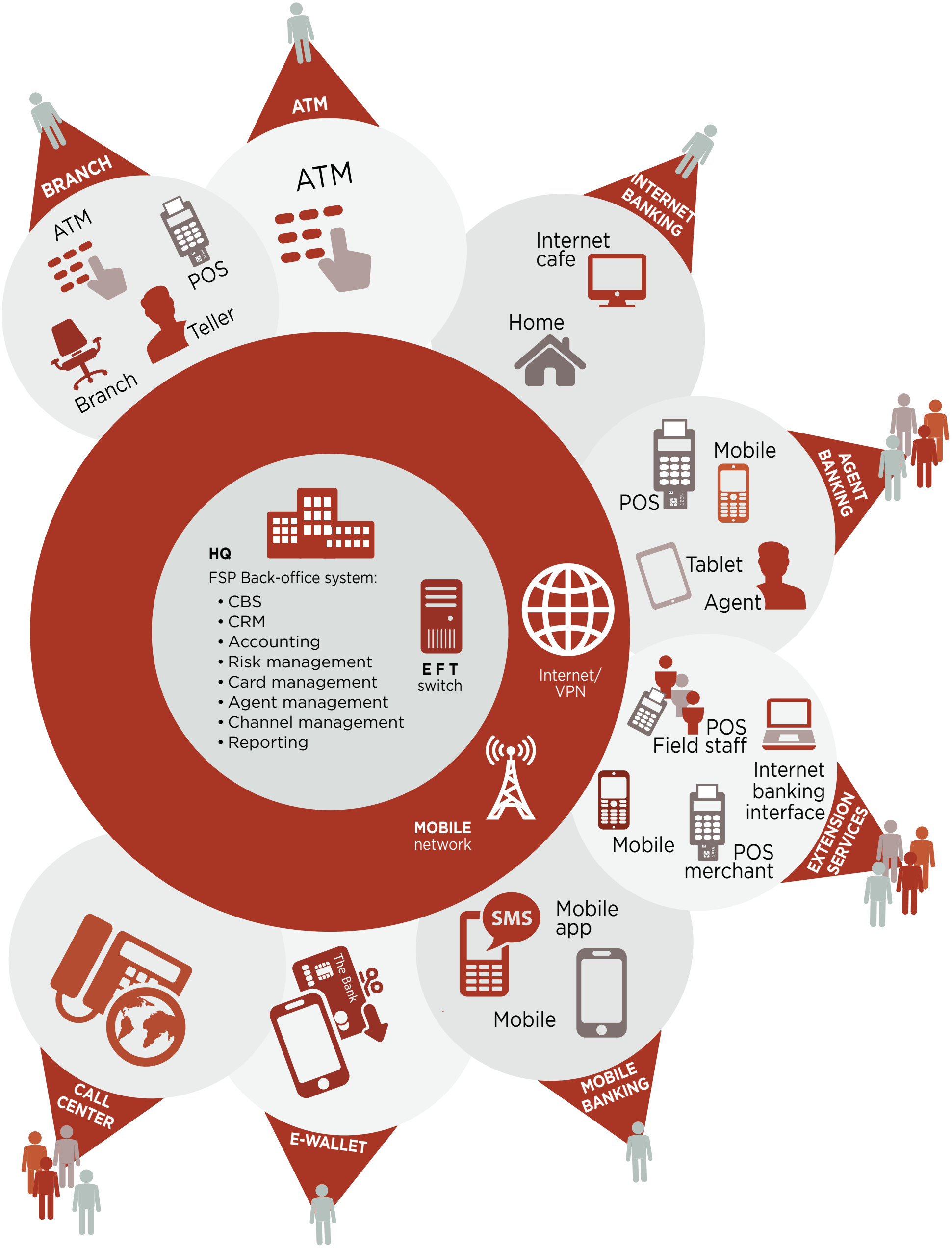
As a foundation to a discussion on ADC technology, it is important to clearly distinguish between the channel and the technology. For this handbook, we define the channel as the customer’s access point to a FSP – who or what the customer interacts with in order to access the financial service or bank account[1]. For instance, customers can access financial services at a bank branch, which is a traditional channel. With the advancement of technology, the term *Alternative* Delivery Channels denotes a broader range of options through which a customer can now access financial services without visiting a branch. These include ATMs, Internet Banking, Agency Banking, Extension/Field Services[2], Mobile Banking, and more recently Electronic or Mobile Wallets. These channels enable customers, FSP staff and agents to access banking services through technology solutions which are built either on Web, mobile or bespoke platforms. Figure 2 shows how these channels extend the services of a branch through systems which are connected to the Core Banking System (CBS) of the FSP.

[1] Given that FSPs are the target audience of this handbook, we will focus primarily on channels which are used to connect customers to bank accounts held at a FSP, as opposed to other financial products such as e-wallets and money transfer offered by non-bank financial services providers. An overlap clearly exists wherein FSPs may opt to use these non-bank services as one of their channels, such as when banks are linked to e-wallets services for cash in/out and payment purposes.

[2] For the purpose of this handbook we have differentiated Extension Services from Agency Banking, based on the user of the channel. While Agency Banking relies on use of third-party operators, Extension Services involves equipping FSP staff with technology solutions.

The term alternative delivery channel denotes a broader range of options through which a customer can now access financial services.

Figure 2: ADC Ecosystem



The most commonly used channels are introduced in Figure 3, along with additional information on how to and who can use this channel. As shown in Figure 3, channels can be self-service or Over the Counter, whereby the customer interacts with staff or third-party representatives such as an agent or merchant – dedicated or not. This distinction is important to bear in mind, as FSPs must always be aware of who or what owns the customer experience, and take measures to ensure that this interaction is equal, if not better than, what the customer would experience if using a traditional bank branch. The classification of a channel as either OTC or self-service becomes somewhat complicated for the case of e-wallets, since these channels typically require some level of OTC interaction to cash in/out and thereafter can be used in a self-service mode.

Figure 3: ADC (business)

	CHANNEL NAME	TYPE OF CHANNEL	WHO/WHAT CUSTOMER INTERACTS WITH TO TRANSACT	SAMPLE FUNCTIONALITY OFFERED BY THE CHANEL
	ATM	*Self-service*	*ATM*	*Cash out, balance enquiry, payments, cash deposit*
	Internet banking	*Self-service*	*Computer, phone, tablet, kiosk*	*Enquiries, transfers, payments*
	Agent banking	*OTC*	*3rd party agent, merchant, phone, POS, mobile*	*Cash in, cash out, payments*
	Extension services, (field staff, mini branch, branch on wheels)	*OTC*	*Bank staff: loan officer, susu collector, other FSP staff, POS, mobile*	*Account opening, cash in, cash out, loan applications, enquiries*
	Mobile banking	*Self-service*	*Phone*	*Enquiries, transfers, payments*
	E-wallet (m-wallets, prepaid cards, store cards)	*Self-service + OTC*	*Phone, computer, merchant, kiosk, ATM, agent, card*	*Cash in, cash out, payments, transfers*
	Call center	*OTC*	*Phone, customer service rep*	*Enquiries, transfers, payments*

If ADCs denote a point of access outside of the traditional bank channel, then ADC *technology* refers to hardware devices, software systems, and the technological processes that enable the provision of financial products and services over ADCs. For instance, a POS device can be the enabling technology for agency banking. Whether self-service or OTC, each channel requires the customer to interact either with a person (that is, an agent, field officer, call center representative or a merchant) or device (ATM, mobile phone or PC). In the case where the interaction is with a person, for example a third-party agent, it is typically the agent that initiates the transaction on a technology device rather than the customer, although at some point during the transaction the customer may also need to interact with the same device, for instance when entering a PIN on a POS. While in some cases it is easy to distinguish between the channel and its underlying technology, there are cases where the channel and the technology are the same, such as ATMs and Internet banking.

A range of products and services is accessible over the various channels. A list of the functionalities most commonly offered is shown in Figure 3, but this should be interpreted only as an example. Due to rapid innovation, the list of functionalities that is accessible to a customer over ADCs is changing almost on a daily basis. ATMs are now offering money transfer services, mobile banking allows for emergency loan applications, and extension services are quickly scaling up to offer almost all services commonly offered in the branches.

ADC risks

An additional topic to discuss as a foundation for the rest of the handbook deals with the risks associated with the use of ADCs. While all FSPs will have existing risk management practices to safeguard their business, the introduction of ADCs may require a reassessment of these policies and the introduction of new controls and risk monitoring systems. Certain characteristics of ADCs, such as a dependence on rapidly changing technology and their ubiquitous nature, mean that new risks may be introduced (for example, agent-level fraud). There is also the likelihood of an increase in existing risks or their severity (for example, in terms of dependency on the security of IT systems). A comprehensive risk review is required as part of any ADC project and the topic will be discussed at various stages in this handbook. Other resources, including the Risk Management Principles for Electronic Banking developed by the Basel Committee on Banking Supervision, the Global Technology Audit Guide series, and more channel-focused resources such as CGAP Focus Note No 75. “Bank Agent: Risk Management, Mitigation, and Supervision” provide deeper discussions on the topic (for full references see page 99).

Five risk areas have been identified as being particularly applicable to ADCs:

- **Legal** – the risk of lawsuits arising between any of the players involved in the channel (customer, agent, FSP, or supplier), either due to misuse of the channel, a lack of clarity of roles/responsibilities, or breach of contracts or laws such as data protection/AML.
- **Operational** – fraud/theft committed via the channel, failure to manage the liquidity of agents and ATMs, unauthorized fees charged for use of the channel, poor quality of service, and loss of private data.
- **Technological** – insecure data storage, weak back-office security, insufficient communication protection, poor authentication/authorization of users, inadequate integration between systems/third parties, or a lack of service associated with hardware/software failures.
- **Compliance** – the risk of fines or loss of license as a result of noncompliance with laws or regulations, including AML, CFT, Agency Banking, Mobile Money, Consumer Protection, Regulatory Reporting.
- **Reputational** – a loss of customer and market share as a result of the occurrence of any of the risks described above.

These risks should be taken into consideration throughout the decision-making process, as they will impact all aspects of an ADC technology project, from channel design to mode of authentication used by the end-user.

FROM A TECHNOLOGY PERSPECTIVE

For those readers interested in analyzing channels with a deeper technology lens, the following section includes a more detailed summary of the technology platforms that drive ADCs. For the purpose of this discussion, it is important to consider an ADC technology platform as the aggregation of four components:

1. A physical device
2. An application running on the device
3. A communication channel used to exchange data between the device and the FSP's host system
4. An authentication mode used to confirm the identity of the user of the channel.

Figure 4 on the following page shows the options available per channel in terms of device, type of application, communication, and the different types of authentication modes used per channel.

ADC devices

The device is the physical object with which a user interacts, such as a mobile phone to access an e-wallet. Since mobile phones are the newer entrants to the ADC space and many FSPs now rely extensively on them, it is useful to pay extra attention to these devices.

Mobile phones can be classified as being either basic, feature or smart. A basic phone has only voice, SMS, and sometimes USSD capabilities, but no data or GPRS capabilities. Feature phones have data connectivity in addition to the basic features, and can therefore be used to connect to the Internet or run mobile applications. Lastly, smartphones are the most advanced option, with processing capacity nearing that of a computer, and are suitable for complex applications or 'smart apps' in addition to the basic features and Internet access. Each of these classes of mobile phones use different operating systems, most commonly Android (Google), Windows (Microsoft) or iOS (Apple). These operating systems also apply to tablets.

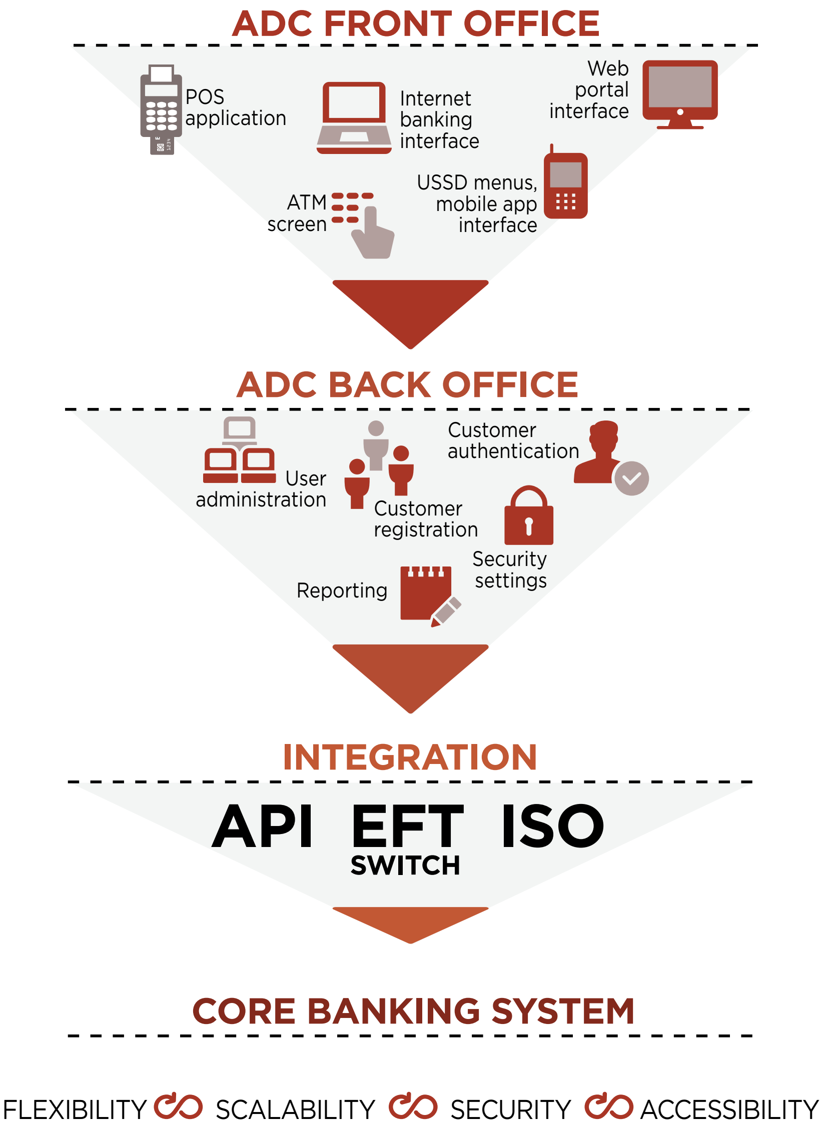
ADC applications

The application layer of ADC solutions consists of front-end applications, back-office administration modules, and the integrations between these systems and the Core Banking System. These are shown in Figure 5, with some examples of the system or functionality available at each layer.

Figure 4: ADC Technology Components

	CHANNEL NAME	DEVICE	APPLICATION	COMMUNICATION	AUTHENTICITY MODE
	ATM	*ATM, HSM*	*Bespoke tech*	*LAN (physical leased line, P2P satellite, VPN over internet, wireless), modem (GPRS, dial-up)*	*Card / PIN, bio, mobile*
	Internet banking	*Computer, phone, tablet, kiosk*	*Web*	*Internet (mobile, wireless, leased line)*	*Username, password, OTP*
	Agent / merchant	*Computer, phone, tablet, POS*	*Web, POS, mobile*	*Internet (mobile, wireless, leased line), mobile data (GPRS, 3G, 4G)*	*PIN, card, bio, physical ID*
	Extension services, (field staff, mini branch, branch on wheels)	*Computer, phone, tablet, POS*	*Web, POS, mobile*	*Internet (mobile, wireless, leased line), mobile data (GPRS, 3G, 4G)*	*PIN, card, bio, physical ID*
	Mobile banking	*Phone*	*Mobile*	*Mobile data (GPRS, 3G, 4G), SMPP, USSD*	*PIN, OTP*
	E-wallet (m-wallets, prepaid cards, store cards)	*Phone, computer, kiosk, ATM, POS*	*Web, POS, mobile, bespoke tech (ATM)*	*Internet (mobile, wireless, leased line), mobile data (GPRS, 3G, 4G)*	*PIN, card, physical ID*
	Call center	*Phone*	*IVR*	*Telecoms – Voice*	*Password*

Figure 5: ADC Solution Architecture: Front End, Back Office and Integration



Front office

The front-office component of the ADC technology platform is the software application that runs on the device, referred to as the front-end application for the purpose of this handbook. ADC applications can be based either on mobile, Web or bespoke platforms such as POS, ATM, and IVR. For instance, Internet banking runs on the back of a Web application. As with devices, mobile applications are the most complex, with four main types of applications. A more detailed comparison of these applications is provided in Chapter 3.

1. **SIM toolkit** – The first type of application commonly referred to as a SIM toolkit, or STK, is pre-loaded onto the mobile subscriber's SIM card, usually by a Mobile Network Operator. The application consists of a set of commands programmed on the SIM, and appears as a menu of Value Added Services. STK applications communicate using SMS messages sent by the application directly to the MNO's host system. In this same category, one can include emerging skin SIMs or thin-film SIMs, a technology that consists of a paper-thin plastic sheet with an embedded chip that can be adhered to the top of any SIM card. Touch points built into the skin SIM overlay filter information from and to the traditional SIM card. Skin SIM technology, which originated in China, is attracting a lot of attention from FSPs who are looking for mobile applications that can be launched independently of MNOs. Finally, both traditional SIM cards and skin SIMs can be used for Near Field Communication, a form of contactless communication between devices which is being introduced for a range of interactions, including payments and vouchers.
2. **USSD apps** – Unstructured Supplementary Service Data applications are supported by all handsets and involve an interactive session consisting of a two-way exchange of messages between the FSP's host system and the mobile phone user via an MNO network. USSD sessions can either be initiated by dialing an MNO-defined USSD short code (for example, *100#) or pushed by the provider to a customer's handset as part of an SMS. Sessions are typically limited both in terms of time and message size, with variations existing from one MNO to another. Offering applications over USSD requires either a direct relationship with the MNO or a contact with an intermediary provider, sometimes called an Aggregator or Premium Rate Service Provider that is licensed by the MNOs and usually the government to provide services over this channel.
3. **Native apps** – The third category of mobile application, commonly referred to as native apps, includes applications that are manually installed on the phone and run in almost the same way as a computer program installed on a PC. Native apps will depend on the operating system on which the mobile phone runs, for example, Android, iOS or Windows. Native applications can be developed to serve as a user interface for staff, agents or customers. Native applications are also increasingly being used as a replacement for the traditional POS devices, with the evolution of mPOS apps that typically interact with a card reader and/or printer to replicate the functionality of the traditional POS device. Lastly, native apps can run in online or offline mode to allow for data capture in areas of little or no connectivity, which is of particular interest to FSPs operating in rural areas beyond the reach of mobile coverage.
4. **Web apps** – The last type of application is a mobile website that runs on the browser of a mobile device accessed via a URL. Web apps function very much as a standard Internet website, but the size and features are designed to display and interact better on a mobile device than on a traditional website[3]. The main advantage of Web apps over native apps is that they work completely cross-platform on all devices with a browser, requiring no installation or intervention to update, as they rely on server-side processing instead of a local, phone-based application. However, Web apps operate in online mode only and hence are limited in terms of usability in areas of poor or no connectivity.

[3] There are two types of mobile websites: Wireless Application Protocol and HTML. The first is based on the WAP standard which is used to guide the design, creation, and display of a mobile website. Although it offers the benefit of running on millions of devices due to its historical use, WAP is being upstaged and therefore replaced by a newer standard, HTML5. HTML5 apps benefit from advancements in programming languages that mean they can provide a range of key capabilities such as offline support, graphics and video, geolocation, and field validation on the mobile browser. Currently, HTML5 can only run on mobile devices with the Webkit engine and are therefore limited in coverage.

Back office

While the front-office applications are perhaps the most visible to users of an ADC, they are reliant on back-office applications which form a critical component of the ADC platforms. These systems play many different roles but are typically used to drive the front-end applications and devices. They also allow FSPs to administer the channel users, define the products and services offered via the channel, control the security of the channel, and of course monitor and report on the channel activity and performance. These administrative systems can be sold separately from the front-end application, as is often the case with Card Management Systems used with ATMs or POS, or could be bundled together with the front-end application, as is commonly the case for mobile banking and agency banking solutions.

Integration

The final component of ADC application involves integration between the various systems involved in the ADC platform. Introducing ADC technologies in most cases requires some level of integration between the FSP's back-office systems (such as CBS, Accounting and ERP) and the technology driving the channel. In many cases, ADC solutions also require multiple integrations with third parties (m-wallet providers, bulk SMS providers and national switches), as well as several in-house systems (m-banking software, agency banking modules, accounting software, and CBS). As with the back-office components of an ADC solution, the integration software is often bundled with the solution, although increasingly, CBS providers are providing integration interfaces through which all external systems must communicate. The topic of integration is discussed in full in Chapter 3.

ADC communications

All ADCs ultimately require the exchange of financial or non-financial information between the FSP and the customer, which typically occurs over communication channels connecting the device and the back-office component of the ADC. There are currently six communication channels for ADCs:

1. **Local area network / wide area network** – ATMs and extension services like mini branches communicate over the FSP's LAN or WAN much like a computer on an internal network. Connectivity between these devices could be over physical leased lines, wireless connections, VSAT/satellite or a Virtual Private Network. LAN/WAN is mostly just used with ATMs.
2. **Internet portals** – Agents, extension services, and e-wallets may use secure Internet portals to exchange information. Where ADCs use Internet connectivity, a VPN is typically configured to provide an additional layer of security.
3. **Mobile data** – Mobile applications exchange information over mobile data services (GPRS, Edge, 3G or 4G[4]), Wi-Fi connections, or satellite-based communications. For the purpose of ADCs, mobile data services, which are provided by the MNO and accessible wherever there is data coverage, are the most commonly used, although Wi-Fi and satellite may still be relevant for some extension services.
4. **USSD** – The USSD communication channel is a standard, publically available GSM technology, controlled by MNOs. As discussed above, USSD applications exchange information over this channel. The use of USSD for ADCs has achieved significant uptake in markets where there is high mobile penetration as a result of the user-friendly, menu-based service. The USSD communication channel creates a real-time connection that is more responsive and secure, as it does not store the customer's data.
5. **SMS** – SMS is a 'store and forward' communication channel that involves the use of the telecom network and SMPP protocol to send a limited amount of text from one phone to another, or from one to many phones[5]. The use of SMS for ADCs is extensive and ranges from STK and native

[4] This refers to the generation of wireless communication technology which is differentiated by the speed of data services available. GPRS and Edge are 2G technologies providing a maximum download speed of 114kbps and 384kbps, respectively. 3G provides up to 3.2Mbps and 4G up to 299.6Mbps

[5] Note that SMTP is a different protocol traditionally used for sending email, but also commonly used for sending SMS messages via the Internet. Unlike true SMS on SMPP, SMTP does not use the telecom network, which can potentially be cheaper, but also presents issues in terms of reliability.

applications using SMS as the mode of communication, to basic applications being programmed entirely using the SMS channel, although these are typically quite limited in terms of functionality compared with other types of applications. SMS has proven to be an effective tool for notification services regarding One Time Passwords, transaction confirmations, or repayment reminders. A distinction is often made between 'pull' SMS messages, which are initiated by a customer to solicit a response from a provider, or a 'push' message, which is sent to the customer by the provider. To request a pull message, a customer must send a request to a short code (for example, send text 'BAL' to short code *12345#)[6].

6. **IVR** – Interactive Voice Response uses a computer application with voice recognition technologies and keypad tones during an interactive phone call between the customer and the FSP. These systems are designed to handle routine interactions such as enquiries or transactions which can be relied on to follow an expected workflow. Within the ADC world, IVR is of particular interest to FSPs serving illiterate or low-literate people, and to date has primarily been used in Latin America and Asia.
7. **NFC** – Near Field Communication is being used to make contactless transactions, including those for payment and access. NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. Consumers can make payments with a wave or tap of their NFC-enabled card.

Authentication

The last component of ADC technology is the mode of authentication, as illustrated in Table 1. This is of particular relevance, as one of the more apparent risks associated with ADCs is related to fraud arising from the authentication of a customer's or other user's identity, and failures which may occur during this process. Branch-based transactions can rely on well-trained tellers or staff whose judgement can be used to confirm customer identity using scanned photos, physical ID cards, signatures, and other tools. However, transactions initiated remotely through ADCs often require enhanced means of verification.

The three most commonly used factors are knowledge, possession, and inheritance as shown in Table 1.

Table 1: Different Types of Customer Authentication Factors Used in ADCs

FACTOR TYPE	DEFINITION	OPTION AVAILABLE
Knowledge	*Something that customer knows*	*Password, PIN, pattern, secret question, image*
Possession	*Something that customer owns or has*	*Bank card, mobile phone, OTP/TAN, physical ID card*
Inheritance	*Something that customer is*	*Biometric characteristic fingerprint, iris scan*

[6] Note that while USSD and pull SMS both use short codes, these are not necessarily the same code and may require that a customer enter a different code depending on which action they wish to take.

While exceptions exist for low-value transactions, best practice for authentication over ADCs dictates that two-factor authentication should be used, meaning that a customer must provide a combination of two different factors to access a system or transact on it. For example, an ATM transaction requires both a card (Possession) and a PIN (Knowledge). Two-factor authentication should not be confused with two-step authentication whereby a customer must go through a couple of steps to access a system, but where these steps do not necessarily involve a combination of different factors (for example, a PIN plus a secret question). The level of security delivered will be influenced not only by the number of factors used in authentication but also by the relative security of the factor itself. Therefore, poorly formatted passwords will not protect systems in the same way as those which adhere to best practice in terms of complexity and frequency of change. It is for this reason that authentication via biometric is typically used only as a single factor, since its level of complexity makes it very difficult for this factor to be compromised.

For ADCs, there are three commonly used options for authentication: payment cards, OTPs and biometrics (fingerprint, voice and iris). Each of these will be introduced here and discussed in further detail in Chapter 3 to present the various advantages and disadvantages of each.

Payment cards

Payment cards are perhaps one of the more traditional means of authenticating users over ADCs. Cards are typically dependent on a PIN for authentication, and users are required to remember this PIN and input it as a means of verification at the time of accessing the ADC. Two main types of cards are used; magnetic strip (magstripe) cards and smart cards. The former uses a machine-readable magnetic strip on the back of the card to store data about the customer, while the latter stores similar information on an embedded microchip, which includes its own operating system, memory, communications interface, security features, and the ability to encrypt and decrypt data. While smart cards have many uses outside of the financial sector, FSPs issue these primarily for use at ATMs or on POS devices. Smart cards are increasingly being produced, distributed, and used according to EMV® Specifications[7]. These EMV cards, referred to as 'Chip and Pin' cards, are steadily replacing the older magstripe cards.

These card types offer differing levels of security based on the PIN authentication method. For instance, to authenticate the PIN associated with a magstripe card, communication with a security module is required. The function of a security module is to issue, validate, and store certificates in a protected environment. A security module can be one of two types: a Software Security Module or a Hardware Security Module. The major difference is that an SSM is a program that runs on a general-purpose computer, while an HSM is a dedicated computer specifically designed to function in a security role. The HSM is a physical device connected to the network hosting the ATM, and has the primary functionality to generate the PIN numbers and store the encryption keys required to authenticate the PIN number provided[8]. In contrast, EMV cards have stored encryption details on the chip, which allows for a local authentication of the PIN, which is both faster and contributes to the high security standard associated with these cards.

[7] EMVCo was established to facilitate worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV® Specifications and related testing processes. Today there are EMV Specifications based on contact chip, contactless chip, common payment application, card personalization, and tokenization. This work is overseen by EMVCo's six member organizations – American Express, Discover, JCB, MasterCard, UnionPay, and Visa – and supported by banks, merchants, processors, vendors, and other industry stakeholders who participate as EMVCo Associates. Adopting EMV cards enables FSPs to not only ensure the highest standard of security for card transactions, but also opens up the option of connecting local or closed systems to external networks, either regional or international.

[8] Note that the HSM actually authenticates the PIN Block rather than just the PIN number itself. The PIN Block is made up of customer data read from the card combined with the encrypted PIN, generated using the ATM/POS pin pad.

There is a trend towards contactless payments via smart cards and NFC technology which uses short-range radio signals to exchange information between a card or mobile device and a terminal equipped to read this signal. When this technology is applied to cards, contactless payments[9] are made possible without a PIN and merely through the 'tapping' of the card on a terminal. MasterCard PayPass and Visa PayWave are just two examples of the applications of this technology, both of which are gathering increasing popularity for low-value transactions where payment speed is of particular importance, such as on transport or busy merchant locations. Mobile phone operators and handset manufacturers have also embraced this technology, with NFC-enabled phones and the ability of some phones to be certified by Visa/MasterCard to allow a user to link a SIM to a PayPass/PayWave account.

One-time passwords

For FSPs looking for higher levels of security without cards or biometrics, OTPs or Transaction Authentication Numbers are an option. These work on the basis of one authentication factor being generated only when needed, namely at log-in or transaction posting, and act as a single-use password or PIN. An OTP is generated using either a time or mathematical algorithm, whereas the TAN uses an algorithm that is dependent on details of the transaction itself. The most common use of OTPs/TANs is currently within the Internet banking channel, but is increasingly being used for mobile channels.

This password or number is typically generated on request, either via use of a physical dongle or a specific security software (for example, TruID[10]), which will require another security factor such as a PIN to grant access. Alternatively, the FSP's system can automatically trigger and embed a TAN or OTP within an SMS message, which eliminates the need to distribute either physical devices or install additional security software.

Fingerprint biometrics

With biometric systems, a fingerprint scanner is used to capture a person's unique fingerprint in order to verify identity at a later stage. Two major types of fingerprint scanners exist: optical scanners, which effectively read a picture of the fingerprint as a visual image, and capacitive scanners, which can sense differences in the ridges of a fingerprint using electrical currents. Capacitive scanners, although more expensive, are by far the most common in the financial sector, given the difficulty with which a scan can be falsified, thus preventing the use of a picture of a fingerprint.

While biometrics is primarily used for authentication purposes, it can also assist FSPs in performing deduplication checks to ensure that the same person has not registered twice in the system. This can be particularly useful where there is a risk of multiple borrowing, since the same customer would be blocked from registering twice. Deduplication checks are not immediately possible on all biometric systems, since it will depend how the biometric data is stored and the ability to search this data, which can be both a factor of data type and processing power available for the task.

[9] Contactless payment systems are credit cards and debit cards, key fobs, smartcards or other devices that use radio-frequency identification for making secure payments. The embedded chip and antenna enable consumers to wave their card or fob over a reader at the point of sale. Some vendors claim that transactions can be almost twice as fast as a conventional cash, credit, or debit card purchase.

[10] TruID is a software token that creates OTPs which you use when logging on to the PortWise Application Portal. TruID can be installed on computers, cell phones, or PDAs.

CHAPTER 2

Building a channel strategy

Our journey to implementing an ADC solution starts with the formulation of a plan or channel strategy. This channel strategy is a critical component of the overall organizational strategy, and as such must be guided by the business' vision, mission, and strategy, as well as market conditions.

STRATEGY
TECHNOLOGY
SELECTION
IMPLEMENTATION

The channel strategy is informed by and is meant to contribute to the general business objectives of the FSP. For instance, if a FSP's vision, mission, and business plan are focused on serving SMEs, this same focus should be reflected in the channel strategy. A well-researched channel strategy should identify the channels to leverage and should be accompanied by a business case that considers the financial and operational implications of each channel. These tools will serve as a guide to all future steps in the implementation process.

The subject of a channel strategy is worthy of a paper of its own and the purpose of this handbook is primarily to show what information must be available as inputs to the technology decisions that will be discussed in later chapters. While our process shows a channel strategy as a prerequisite to the technology platform selection, in many cases there is a feedback loop between these steps, so that the strategy is only finalized as/when a decision is taken regarding the technology or platform. It should also be noted that a channel strategy does not imply choice of a single channel, but could result in an integrated, multi-channel strategy that combines several channels and technologies to achieve the overall business objectives. This is a common trend, with FSPs starting with one channel (for example m-wallet) and then linking this with other channels (for example m-banking or ATM). Finally, a channel strategy can be vastly transformative to a FSP's core business, and therefore requires strong buy-in and support at the board and executive levels.

This chapter focuses on how to assess market conditions and the internal operations of a FSP, and to develop a channel strategy that is in line with the business' objectives and customers' needs. The following steps, sometimes iterative, should guide the reader through the decision-making process:

1. Define the ADC objectives
2. Assess the environment
3. Develop the channel strategy and business case.

STEP 1:
Define ADC objectives

Typically, a business problem or challenge has triggered the need for an ADC solution. These triggers could include operational bottlenecks, a need for scale, customer demands and preferences, new segments, or greater outreach. Alternatively, a market opportunity could act as a trigger, presenting an attractive business proposition based on a clear gap between supply for and demand of a product/service. Identifying these triggers, even at a high level, offers direction and focus in the early stages of developing a channel strategy and will help the FSP define the objectives of the ADC strategy in alignment with the mission and vision of the organization.

This step should also result in the allocation of human resources – IT, audit, risk, and operations – in the form of a channel strategy team. Deciding whether these resources are available in-house requires assessment of availability and experience in the subject area. Resources who have worked on similar exercises in the past will be better equipped to conduct the exercise building on experience, while the use of external consultants for this task can bring the benefit of wider market experience. The team allocated to the development of the strategy is in most cases different to the one tasked with implementation of the channel, as the skills required differ considerably.

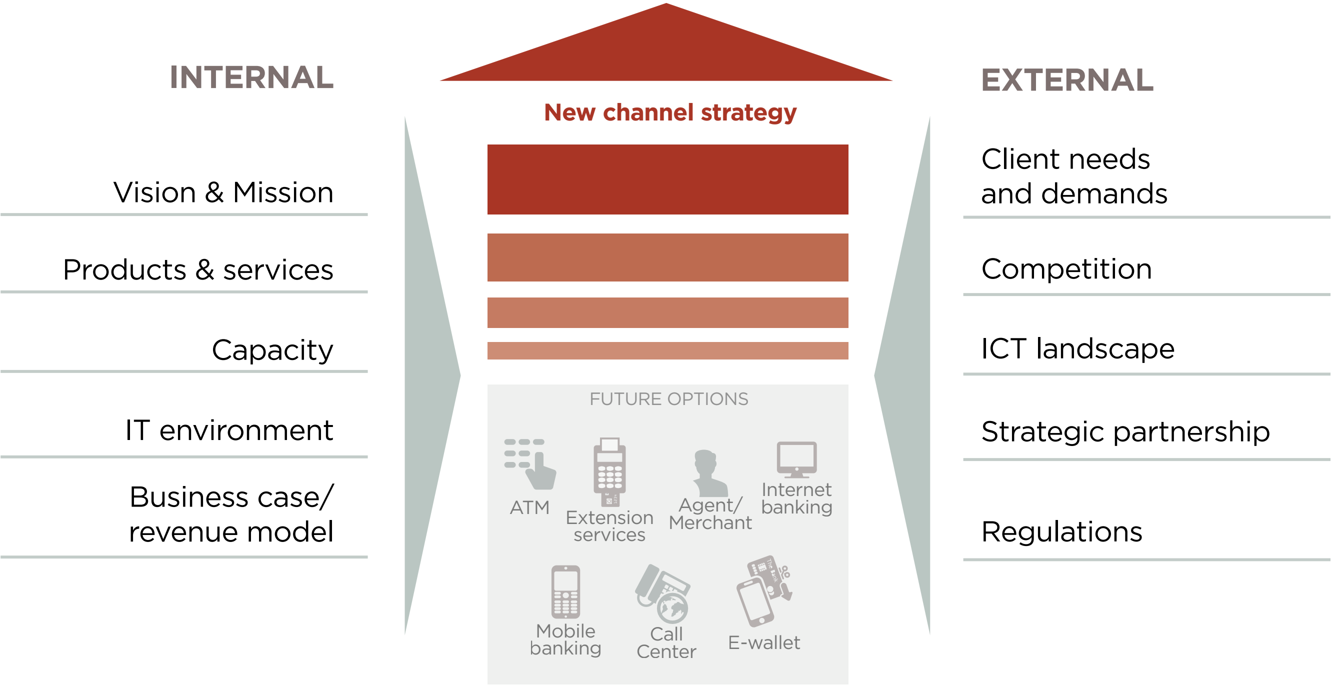
This step should also result in the allocation of human resources in the form of a channel strategy team.

STEP 2:

Assess the environment

The decision to pursue a specific channel or channels must take into consideration many internal and external factors. These factors are summarized in Figure 6, which shows how the channel strategy is influenced by both the internal and external environments within which a FSP operates. The channel strategy therefore involves an assessment of each of these factors separately and collectively, as outlined in this graphic.

Figure 6: ADC Channel Strategy



External assessment

The market is constantly changing, influenced by innovations in ICT, competition, regulation, and customer behavior – all of which are outside the control of a FSP. An assessment of these external factors can help one understand customers' needs and market demand, as well as identify opportunities and threats which should be factored into the channel strategy.

Customers' needs and demands

Developing a channel strategy should be a customer-centric exercise. It is the end-user who will ultimately determine the success of the channel strategy based on their adoption and usage of the channels provided. Taking the time to really understand the customer ensures that their needs and capabilities are not assumed, but rather are confirmed through direct interaction and feedback. This assessment could be done through focus groups, surveys, or by mining available customer data. Irrespective of the tools used, this stage serves to reach an understanding of which products, features, and services are most valued by customers, the difficulties that customers may have with existing channels or competitor channels, the customers' capacity to interact with these, and the willingness and capacity to pay for ADCs. Finally, by combining direct customer input with target market analysis, a FSP should be able to decide if customers are adequately equipped in terms of financial literacy and technology to interact on a self-service basis or if OTC channels are required.

Competition

Assessing the competition in the market is an essential component of any business strategy, providing both an offensive and defensive strategic context for the FSP's channel strategy. The first step in this analysis is to identify other companies providing similar or complementary channels, and to conduct a thorough analysis on what is currently being offered, how it is being offered, and at what price. The easiest way to do this is to stage a mystery shopping exercise to experience the competitors' offerings from a customer perspective. Further analysis can be conducted with media scans and targeted research to determine how competition might react under certain circumstances. Lastly, primary market research with existing customers is also a good way to get information on their experiences with competitor products and pricing. Once the FSP has a clear picture of the competitive market, this information can be used to identify gaps in the marketplace that could be exploited by a channel strategy.

Regulation

Regulatory policy influences the market by mandating who can do what, where, and which rules apply when it comes to financial services. ADCs are a complex topic for regulators, as the space is constantly changing. It is the FSP's responsibility to assess and understand the obligations *vis-à-vis* the regulator and other relevant authorities. Clearly, regulations governing the use and issuance of e-money/mobile money, mobile banking, agency banking, Internet channels, and remote branches are the most obvious ones to consider. But others, such as regulations governing access to communications, interoperability, electronic documents or signatures, KYC, biometrics, national ID, and AML/CFT must also be considered, as they may impact some component of the channel.

In markets where no regulations exist for these activities and/or where regulators are unfamiliar with mobile money or agency banking, a FSP may need to organize a workshop or presentation with the regulator to explain the concept and its plans. In such cases, an internal 'champion' should be allocated the task of building a relationship with the regulator to ensure that it remains supportive of the project as the project moves through the phases of implementation. In cases where there is no specific regulation, a FSP may need to consider applying for a 'Letter of No Objection' as a quick and easy way to comply with regulatory measures.

The regulatory assessment should not only focus on the bigger picture of what is, or is not, allowed, but also on how some of the details of regulations may influence the implementation of the channel. For example, the agency banking regulations in Kenya require the production of a physical receipt for all transactions performed by third parties[11], meaning that a printer or receipt book is required[12].

ICT landscape

By definition, ADCs require users to be able to access systems that are remote to their location at the time of transaction. Such access is dependent on the availability of a supportive ICT infrastructure for the end-users of the ADC. As discussed in Chapter 1, this requires access to a physical device, an application running on the device, and a communication channel to transfer data between the customer and FSP. As part of the external assessment, the FSP will need to analyze what is available to target customers or users at each of these levels.

At the device level, it is important first to know what types of devices – such as ATMs, POS, kiosks, computers and mobile phones – are accessible to the target market. For some of these devices, information about distribution and availability may be publically accessible, as with POS or ATM networks, which are typically monitored by the regulator. By contrast, the statistics regarding the availability of personal computers or phones may be harder to access, with only high-level statistics available. Market surveys, either conducted by the FSP's strategy team or by external parties, can provide some insights and ideally would contain some additional information, including which models of each device are the most popular. This is particularly important for mobile phones where the FSP will need to decide which type of phone to cater for: basic phones, feature phones or smartphones. Included in this assessment should be the projected future uptake of particular devices to understand likely market trends. Additionally, the cost per device – information infinitely easier to access than market distribution – can provide a good proxy for penetration data, and will also be an important input to the business case.

Secondly, the FSP will need to assess the availability of options for the application layer. Although important, this information is less critical than the device or communication layer. Ideally, ADC solutions should work on all operating systems, but the reality is that many solutions are not immediately cross-compatible and often require additional resources that may not be worth the investment. For example, knowing what proportion of the target market is using Windows phones may help with the decision whether smart apps should be built to work on this platform.

Next is to review the availability, quality, and affordability of the communication options available to the target market. The FSP will need to identify which communication channels are accessible to the target market, considering the full range of options, including SMS, USSD, mobile data services, Internet, LAN/ WAN, IVR, or NFC. Market research on these options should be conducted to identify which of these options are reliable, affordable and have available bandwidth to support the traffic of the channel over time. In most cases – and unless using IVR or NFC – the FSP will be dependent on an MNO or other connectivity provider for this component. Such partnerships can be problematic for some FSPs, particularly where there is competition, real or perceived, between the two parties. This is most noticeable with the USSD option, which is well suited to host an ADC due to its compatibility with all types of mobile phones, but in many markets is either restricted in terms of availability, is subject to poor quality service, and/or is expensive to access. This reality has forced some FSPs to consider alternative communication options such as data services, STK, thin SIM, or IVR, so that they have more control over this critical component. At this stage of the analysis, the channel strategy team needs to invest time in researching all of these options and

[11] The Central Bank of Kenya website (https://www.centralbank.go.ke/index.php/banksupervision#agent-banking) states: "Bank agents are required to issue receipts for all cash deposit and withdrawal transactions. Additionally, the principal institutions are required to have in place adequate agent identification arrangements and customer feedback mechanisms to aid in the verification process. Further, bank customers are at liberty to verify the status of particular agents from local branches of principal institutions before using the services of any agent."

[12] http://www.bu.edu/bucflp/files/2012/01/Guideline-on-Agent-Banking-CBKPG15.pdf

ideally analyzing the various options as they operate in the market to develop a well-informed opinion regarding quality. During this analysis, the channel strategy team should bear in mind the potential for ADCs to operate in a limited offline mode. Typically, this is only applicable to OTC channels, particularly extension services and possibly agency banking, and for a limited range of transaction types (non-financial transactions).

The last component of the ICT landscape that should be considered during the assessment is the availability of grid-based electricity or other power alternatives to ensure that devices and connectivity options can access power. Designing a strategy in areas beyond the grid, or where the electrical supply is poor, one may need to consider backup alternatives to ensure continuity of service. The cost of these backup options should be incorporated in the business case.

Strategic partnerships

Many ADCs will require partnerships to be formed between the FSP and a third party. These third parties could be vendors, m-wallet providers, PRSPs, MNOs, and national or international switches. Irrespective of the purpose of the partnership, it is important to find partners that are operationally, technically and commercially aligned, and that revenue is generated and distributed throughout the supply chain[13].

Operationally aligned

- The FSP must ensure that a potential partner is not targeting the same customers with the same or alternative products/services. In that case they are competitors, not partners. Services should be complementary or value-add for your customers.
- The FSP must be sure that it has done sufficient research (has 'shopped around' sufficiently) to identify the best partner in the market (to be discussed more in Chapter 4).
- Partners must be willing to agree to targets for the partnership and have the means to measure performance against these targets.
- The FSP should assess the partner's current infrastructure on the ground, and the reach and utilization/ performance of this infrastructure to determine whether there is significant overlap in the infrastructure of the partner organizations or if it is complementary.

Technically aligned

- The proposed partner's competency needs to be confirmed based on historical track record of delivery.
- The technology platforms of the partners should be considered to ensure that they could be integrated with the FSP's systems (where applicable).
- Both partners must have sufficient compliance and controls in place to mitigate issues which may put the partner or partnership at risk.

It is important to find partners that are operationally, technically and commercially aligned.

[13] Flaming, M, Mitha, A, Hanouch, M, Zetterli, P, and Bull, G (2014). Partnerships in Mobile Financial Services: Factors for Success. IFC: Washington, D.C.

Commercially aligned

- The costs being charged must be confirmed as affordable and competitive in the market, ideally with a business case to support the fact.
- The partner's business viability needs to be confirmed so that the FSP is sure that it will play its role even in the initial periods when the channel may not be extremely profitable.
- There should be benefit for all parties that is proportionate to the respective contributions to the partnership, whether this is through a revenue-sharing model and commission arrangement or other means of shared value, to properly motivate partners to participate over the duration of the relationship.
- Lastly, it is good for FSPs to get a measure of how important it will be to the partner and to look at the relative size of the two parties. Will it be a priority customer, a 'big fish' whom the partner will work hard to keep happy, or does its relative size mean it is a 'small fish' that may struggle to get the partner's attention?

Internal assessment

While the external assessment can help identify consumer demand, market opportunities, and threats, an internal assessment allows an organization to evaluate its position with regards to operational constraints and strengths. This assessment should ideally include five areas:

Product and service offering

ADCs by definition are a means for the FSP to distribute its products and services. As such, any channel strategy needs to be designed with the specifics of the FSP's products and services in mind. Not every product and service is appropriate for every channel; the FSP should review current and planned products/services to determine which channel options would be most convenient for the customer to access these products/services. For instance, a customer with a savings account needs access to deposit and withdrawal services from this account outside of branch hours; a self-service mobile banking application would not meet this need because one cannot withdraw money from a phone. In this case, the channel strategy team should consider channels that facilitate cash withdrawals such as ATMs, POS, or agency banking.

Current channel strategy

Should the FSP have existing channels in operation, it is critical that it takes this opportunity to assess the success of these channels. This could include an analysis of performance (usage rates, registration rates, and valued services) and operational efficiency. Additionally, customer feedback should be obtained to determine what improvements or changes would be of benefit. Existing channels should also be reviewed to understand how they could complement new channels, such as linking ATMs with an existing mobile banking platform. Developing an integrated multi-channel strategy will increase the number of touch-points for the customer and streamline the customer experience. For example, an existing mobile banking platform could potentially be used to direct clients to the nearest ATM location or to enable NFC technology on the mobile for cardless transactions at the ATM. Lastly, the sustainability and cost of implementation of the existing channels should be reviewed not only to ensure sustainability but also as inputs to the budgets required for future ADC projects (for example, cost of integration and resources required to manage the project).

IT environment and strategy

The assessment of the internal IT environment needs to consider several different areas, including the state of the CBS, the IT strategy, and any existing or planned IT projects that could overlap with the ADC project. In terms of the CBS, the channel strategy team should consider the current state of the CBS, including its stability, pending upgrades, its capacity to support a full integration, and whether it is decentralized or centralized. A weak or unstable CBS will quickly sabotage any ADC project, and difficult as the decision may be, FSPs may need to postpone ADC projects until their CBS is stable to the extent that it can support the integration of a channel, both functionally and from a scalability point of view.

CASE STUDY

MicroCred

MicroCred Group is an investment company, established in 2005, that builds and manages an international network of financial institutions in emerging markets. These FIs share the common mission to provide quality financial services that are accessible and adapted to the needs of unbanked and/or under-served people, particularly micro, small, and medium entrepreneurs in the five African countries of Côte d'Ivoire, Mali, Madagascar, Nigeria, and Senegal, as well as through two affiliates in China's Sichuan and Nanchong provinces.

MC's objective is to expand its distribution network and capacity to reach new customers, especially in rural areas. All MC operations have been successful and have managed to achieve profitability using traditional branches. However, the economics of branch channels have limited MC to a primarily urban clientele. In 2013, MC launched a major transformation program supported by a multi-channel distribution network to reach mass-market customers beyond the limits of branches and into rural areas. The multiplicity of distribution channels, accompanied by product development, market intelligence, process automation, and marketing efforts, is critical in supporting the delivery of innovative products.

MC identified the following quality targets: simplicity/intuitiveness, availability, robustness, and coherence among channels to be applied as core themes throughout the channel strategy. To address these challenges, MC used a human-centered design approach to systems design and development that aims to make interactive systems more usable by focusing on the customer's use of the system and applying knowledge and techniques based on human factors, ergonomics, and usability. MC empowered a cross-functional team to design the service based on extensive field research and observation. MC monitors the quality of service provided to customers, frequently releasing small adaptations based on constant feedback loops.

Reflecting on its ADC strategy, Microcred's Head of Alternative Delivery Channels Denis Moniotte noted: "The modern delivery channels in financial services require a major shift in the way we organize ourselves within the bank. It pushes some functions that have traditionally been managed by our back-office staff into the front line, which brings new challenges. For example, when we implement agent banking, mobile/Internet banking or an ATM network, customers become users of our banking IT platform. It is about opening new doors, and making sure that the core processes will support the new doors."

The internal assessment must also consider the FSP's IT strategy and how ICT will be used to deliver the organizational strategy. Most FSPs who are designing or updating an IT strategy will feature ADC technologies as one of the business' critical systems. While a linkage between the IT strategy and the channel strategy must exist, these are very different plans, with the former primarily being determined by the IT department, while the channel strategy is a result of inputs across the business as a whole, with key components which require input and support from the IT department. The direction outlined in the IT strategy must be considered in the formulation of the channel strategy to ensure that they are well aligned. Topics of particular importance will be the strategy for the procurement of IT systems, preference for different hosting scenarios, disaster recovery/ backup policies, business continuity[14], security standards, and if available, any protocols for the integration of systems. At this point of strategy formulation, it is important to review and incorporate any existing IT policies that are relevant to the channel strategy, or potentially create new policies to complement the new channels.

Either as part of the IT strategy review, or perhaps as a direct assessment of the existing internal security policy, the FSP needs to consider the mode of authentication used to verify a customer's identity, as introduced in Chapter 1. This typically involves a review of existing modes of authentication, be they cards, biometric or PIN/ password systems to determine the appropriateness of these authentication methods to any channel. For example, the cost and logistics of distributing cards for FSPs looking to launch a mass-market savings product may result in the conclusion that biometrics, as a mode of authentication, is more reliable and easier to administer than PIN/password-based systems. Additionally, FSPs may wish to make decisions regarding the interoperability of the authentication mode, perhaps standardizing the use of EMV cards across all channels. This topic will be revisited in detail during the requirements analysis phase. At this point the goal is simply to audit the existing authentication methods, and if relevant, decide which method is most suitable.

The final area for consideration is the existence of IT projects which may overlap with the timing of the ADC project, or perhaps limit the resources available to allocate to it. From a technical perspective, the impact and potentially the integration of a new ADC will need to be considered. For example, if there is a plan to implement a new data warehouse, the ADC project should bear this in mind and ensure that data derived by the channel is also fed into this new data warehouse.

The internal analysis must also consider the financial, operational and human resources available to launch and manage a channel strategy. The financial resources required to introduce a new channel can vary depending on the scope of the project, and while the IT systems component may be one of the larger elements of the budget, provisions need to be made for channel development, marketing, operational pilots, and channel support services. The channel strategy team should consider the significant cost implications of the initial technology procurement, but also the running costs associated with the channel. An estimated budget should be assigned from the beginning and stakeholder commitment obtained to ensure that the funds required will be allocated to this project. The subsequent vendor selection process can help to finalize the exact budgets required to finance an ADC project, but high-level estimates should be considered at this point based on information obtained from the assessment exercise.

The resource assessment should also consider the skills and availability of staff to manage both the channel implementation and ongoing operations. Required skills include project management, channel management,

[14] A Business Continuity Plan (BCP) is of particular importance for FSPs to enable critical services or products to be continually delivered to clients despite system interruptions or disaster. The business continuity planning process involves the recovery, resumption, and maintenance of the entire business, not just the technology component. While the restoration of IT systems and electronic data is important, recovery of these systems and data will not always be enough to restore business operations. The Federal Financial Institutions Examination Council offers the IT Examination Handbook, which includes a booklet on BCP, at http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx.

IT, audit, risk, operational, finance and accounting, and agent management (if applicable). An inventory that takes into account these requirements can inform a FSP's need to recruit additional staff. This could be a temporary requirement for a project manager to drive the implementation team, or a permanent restructuring to manage ongoing support once the channel is in operation. A FSP should expect to employ an operational team that will work closely with vendors, IT, audit, risk, and customer support, all of whom will require training on roles and responsibilities with respect to ADC operations.

Internal risk and compliance

As business processes change with the evolution of technology and changing customer expectations, threats emerge as new vulnerabilities are discovered. Introducing ADCs increases an institution's overall risk profile and the level of risks associated with offering financial services, particularly legal, operational, technical, compliance, and reputational risks, as discussed in Chapter 1. Risk management involves a set of processes through which an organization identifies, analyzes and responds appropriately to risks that might adversely affect the realization of the organization's business objectives. Risk management tools include IT controls, which are selected and implemented on the basis of the risks they are designed to manage. As risks are identified, suitable risk responses are determined, ranging from doing nothing and accepting the risk as a cost of doing business to applying a wide range of specific controls.

New channels should be thoroughly evaluated for any perceived risks and measures designed to control, avoid, accept, or transfer these risks to the customer or a third party. Liquidity risk in cash management is particularly relevant for ADCs. For example, some FSPs mitigate liquidity risk for ATMs by outsourcing cash management to companies that specialize in this service, with armoured vehicles and armed personnel. Developing policies and measures to mitigate these risks is a continual process, initiated in the formulation of the channel strategy and finalized throughout the subsequent steps in the process to ensure that on implementation, the FSP's risk management framework is fully updated based on the risks associated with the ADC. With a sound risk assessment and robust risk mitigation strategies, MFIs can successfully implement ADCs that will ensure the protection of assets, security of transactions, prevention of fraud, protection of client privacy, data security, and compliance with laws and regulations that are applicable to digital financial services, regardless of which option is selected. For microfinance practitioners, we would recommend the "Digital Financial Services Risk Assessment for Microfinance Institutions Pocket Guide" developed by the Digital Financial Services Working Group[15].

Ensuring that ADC operations and technology platforms are compliant requires FSPs to be aware of and conform to the requirements and regulations in their respective markets. Compliance is typically enforced through a management process that identifies the applicable requirements (defined, for example, in laws, regulations, contracts, strategies, and policies). FSPs will generally have a compliance officer who is responsible for assessing the state of compliance and the risks and potential costs of noncompliance, and for initiating any corrective actions required. While governance and management controls are established to ensure that effective information management and security principles, policies, and processes are in place, technical controls can be used to ensure the reliability of almost every other control in the organization. The ability to automate technical controls that demonstrate compliance with management's intended information-based policies is a powerful resource for an organization. Similar to the risk management assessment, at this point in the ADC implementation it is important for the FSP to identify any potential compliance issues and adapt the framework to address these. Other measures such as internal auditing should be considered part of the long-term risk management strategy to continuously evaluate potential threats and vulnerabilities and the manner in which the organization manages risk.

[15] Digital Financial Services Risk Assessment for Microfinance Institutions Pocket Guide (September 2014). The Digital Financial Services Working Group, Washington, D.C.

STEP 3: *Develop the channel strategy and business case*

The channel strategy

Having defined the objectives and conducted an internal and external assessment, the FSP's channel strategy team can now define a channel strategy.

This is a project-planning document that outlines how the FSP will meet customers' needs and at the same time address the challenges identified in Step 1.

The channel strategy document should specify:

1. The business goals and objectives that the proposed channels are meant to address, as established in the FSP's business plan or strategy.
2. A market analysis, including market research and competitor and regulatory reviews.
3. An analysis of the proposed channels and technology (device, application, and communication) and how they will meet business goals and customer needs.
4. A SWOT analysis of the proposed channels and technology.
5. A recommendation, based on the analyses above, of which ADC solution to pursue.
6. An operational, financial, and IT requirements analysis and a recommendation of whether to 'buy', 'rent' or 'build'.
7. A high-level timeline and project plan, including roles and responsibilities of key stakeholders or internal teams.
8. A high-level budget, including the source and uses of funds.
9. A risk analysis, including potential impact and mitigation.

At this stage, the focus should be on reaching consensus and eventually a decision internally about which ADC solutions to pursue. Specifics, such as business projections, targets, and timelines can be tackled in the business case to analyze the commercial viability of the chosen solution.

CASE STUDY

Buy, build or rent?

In the current market, the most commonly observed strategies for IT systems procurement are either to 'buy', 'build', or 'rent' systems which are defined as follows: an organization can purchase either a license or bespoke solution from an existing vendor (buy), choose to build a customized solution from scratch (build) or leverage Software as a Service (SaaS) to 'rent' software from a vendor. This approach to procurement is separate from the decision of how and where to install and host the systems used by the FSP, which could be either on in-house servers, at an external data center, or in the cloud. While there is an increasing amount of overlap between these two strategies, that is, SaaS products being hosted in the cloud, this need not always be the case, with in-house or licensed products also being stored in the cloud for security and ease of management. The decision regarding procurement of systems is influenced by a range of factors, including uniqueness of requirements, security, legal and compliance issues, the organization's skill and available labor, hosting requirements, cost, time, and vendor availability. FSPs will need to consider each of these factors carefully, alongside the advantages and disadvantages of each option, which are summarized below. Some channels, such as mobile banking and ATMs which are used on third-party networks, lend themselves particularly well to such models. The SaaS option is especially attractive to FSPs that are testing out new channels for the first time and are therefore unsure of the results.

	BUILD	**BUY**	**RENT**
	Custom Development	*Commercial System*	*Software as a Service*
Advantages	• *Can provide solution exactly matched to FSP requirements.* • *Full ownership rights to all IP and source code, compared with commercial software.* • *FSP will own the system.* • *Offers full control over data.* • *Cost of in-house support potentially lowers ongoing maintenance costs.* • *Ownership of tangible software/hardware assets.*	• *Can provide complete solution to FSP.* • *Proven solution.* • *Availability of support for a full team* • *Option to customize with support of vendor expertise.* • *Flexible solution and could potentially lower costs, with more efficient workflows and added functionality.* • *Offers full control over data* • *Ownership of tangible software/hardware assets.*	• *Shorter implementation time.* • *Ready solution.* • *Lowest initial cost to FSP.* • *No hardware investment required (if cloud based).* • *Minimal IT dependency for application and hardware maintenance.* • *Solutions can be easily scaled up or down with little time and effort.* • *SaaS upgrades are iterative, with limited involvement required.*
Disadvantages	• *Higher upfront investment, including additional hardware purchases if needed.* • *May take much longer to implement.* • *Fully dependent on expertise and reliability of programming skills in-house (FSP becomes a software house).* • *Presumes that the FSP has sufficient knowledge of the systems to fully extract requirements and design the system well.* • *Generally seen as more risky, as typically relies on key individuals.* • *A less agile option and CBS will always take preference, which may put severe constraints on your ADC plans unless carefully managed.*	• *Higher upfront investment, including additional hardware/software purchases if needed.* • *May require FSP to compromise to suit available functionality.* • *Customization for specific requirements can be costly and/or time consuming.* • *Dependency on IT vendor for support can be a challenge, depending on upfront negotiations.* • *Upgrades can be expensive and time consuming and often mandated by vendor.*	• *Usually not customizable and limited in functionality.* • *May not support all required functionality.* • *Long-term cost can turn out to be higher for bigger FSPs.* • *Control is relinquished to vendor.* • *Potential regulatory issues about storage of data/business critical systems (if cloud).* • *Dependency on IT vendor for support can be a challenge, depending on upfront negotiations.* • *Integrations with other corporate systems can get complicated; well-defined Web services should be available from vendor.*

The business case

A well-researched channel strategy should be accompanied by a business case that considers the financial and operational characteristics of each channel. The business case can be a basic five-year financial model that captures the investment required, ongoing costs, new revenue streams, and cost savings that are attributed to this new channel. While a positive financial return from transaction revenues would be the ideal output of the business case, some FSPs may pursue a channel strategy despite a poor return on the channel alone, as there may be indirect benefits to the rest of the business, such as opportunities to cross-sell, deposit mobilization, and lower costs. Regardless of the profit motive, FSPs deploying new channels should monitor the trend in transaction volumes, as this ultimately impacts on both costs and revenues. For instance, a high volume of transactions has cost implications in terms of license fees to be paid to vendors, commissions to be paid to agents, or USSD charges levied by MNO partners. Similarly, knowing how many transactions per customer are required to break even can inform marketing strategies to increase customer adoption and usage of the channel. Ideally, the channel business case should include the following inputs:

1. Assumptions based on the internal and external analyses, such as the size of the addressable market, growth projections, transaction volumes and values, or other cost and revenue drivers.
2. Distribution of ADCs – the number of touch points and projected growth over time.
3. Cost structure, including capital expenditures, staff costs, and marketing and IT costs.
4. Pricing structure and other fees per transaction type or per product for each channel.
5. Number and types of partners and the fees and costs accruing to each.
6. Projected cost savings and operational efficiencies accruing to the FSP as a result of the new ADC, such as a reduction in the cost of funds and increased staff productivity.

The financial model can help the FSP build KPIs and targets that can be used during and after implementation to assess the success of the ADC solution. KPIs can be centered on outreach (for example, ‘ADC will help reach 2 million clients’), impact (for example, ‘15 percent of new customers will come from rural areas’), market share (for example, ‘become the leader in money transfer’), efficiency (for example, ‘reduce account opening time to two hours’), or sustainability (for example, ‘achieve operational profitability in two years’). The **Chapter 2 checklist** at the end of this handbook provides an example of a summary business case document for an ADC, with some proposed critical indicators to monitor.

As a last step, the channel strategy team should test the business case against global/regional benchmarks or case studies. For instance, if in a similar regional market, an ADC project typically breaks even by Year 5, then a business case that promises break-even in Year 1 would not be realistic. Global and regional benchmarks can be obtained through secondary research (such as annual reports or industry reports), as well as from experts, practitioners, and vendors. Some FSPs may also wish to build a separate business case for other stakeholders, such as agents or MNOs, to confirm that incentives are structured in a way that ensures the viability of the channel and also to quantify the investments (for example, in an agent channel) or costs (for example, USSD costs) over time.

CHAPTER 3

Mapping strategy to a technology platform

It is important that FSPs carefully consider the implications of using one technology over another to ensure that the technology platform selected is aligned with the channel strategy and therefore enables the FSP to meet its business objectives.

STRATEGY
TECHNOLOGY
SELECTION
IMPLEMENTATION

Equipped with an ADC strategy, FSPs are frequently tempted to select a vendor in a rush or to commence in-house development with little or no consideration for which enabling technology best suits its strategy. For some channels such as ATM or Internet banking, this approach, while not recommended, can still yield success, as the solutions available to run these channels are quite well defined and the technology is more or less inherited by the choice of channel. In contrast, agency banking, extension services, mobile banking, and e-wallets present a broader suite of choices involving a host of different technology platforms, which offer very different user experiences. It is important that FSPs carefully consider the implications of using one technology over another to ensure that the technology platform selected is aligned with the channel strategy and therefore enables the FSP to meet its business objectives. Determining the technology platform, which requires decisions at both the application and device layer, needs to happen before a FSP can proceed to vendor selection and implementation activities. This chapter aims to guide the reader on how to identify the right technology platform and involves the following steps:

1. Identify the technology options available
2. Confirm the criteria that will influence the decision
3. Select the preferred platform.

For the more technical reader we will discuss in detail the benefits and disadvantages of different applications and devices used for mobile-based channels, as these are by far the most complex channels in the market at present.

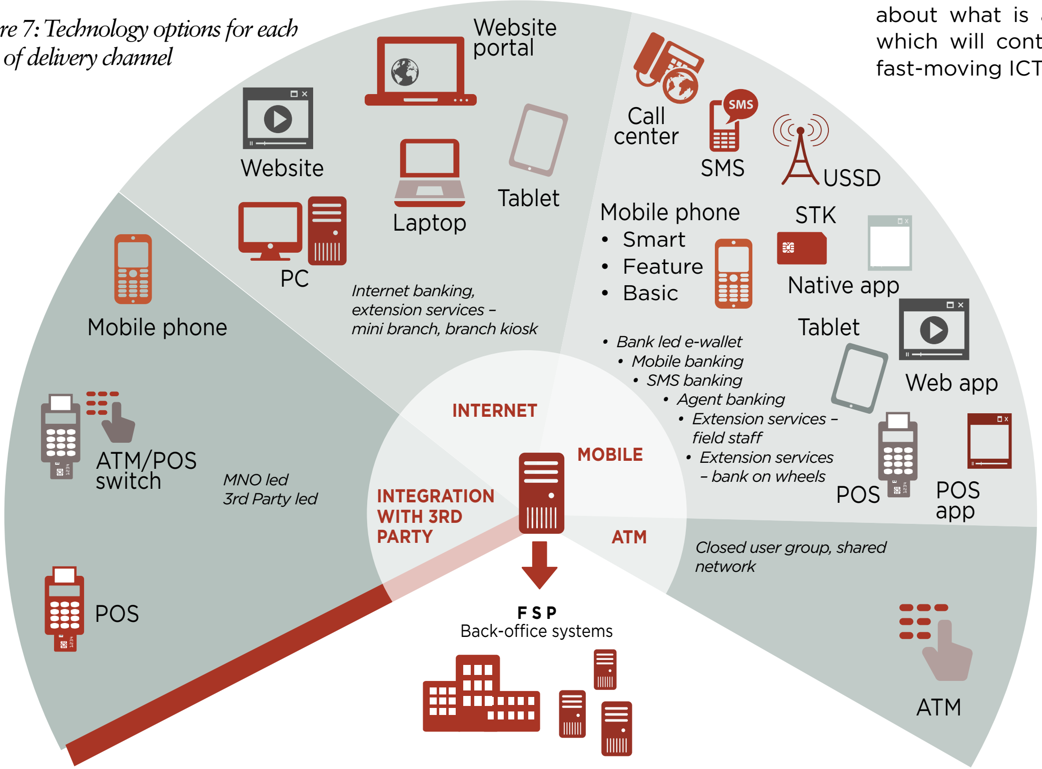
STEP 4: *Identify available options*

ADC technology, like most technologies, is changing at a speed that is difficult for even the most avid technology expert to keep pace with. It therefore comes as no surprise that FSPs are often confused about what options are available to them and for that reason tend to pursue the cheapest platforms or those touted by an aggressive vendor. To avoid these mistakes, FSPs need to spend some time prior to vendor selection researching the available options and understanding the benefits and disadvantages of the technology platform that they decide to pursue.

Figure 7 illustrates the range of technology options for each of the ADCs discussed in this handbook, depending on whether the channel will require a third-party integration or can run on the Internet, on a mobile platform, or through a bespoke application such as ATM. As the diagram shows, some channels like the ATM provide very few choices, while others such as mobile channels offer many options at the device, application, and communication levels (for more on the components of a technology, please refer to Chapter 1).

The technology selection needs to be somewhat iterative, reverting back to the strategy with informed decisions about what is available in the market, which will continuously change in this fast-moving ICT world.

Figure 7: Technology options for each type of delivery channel



5

STEP 5:

Gather influencing criteria

Once technology options have been identified, the FSP may consider the following criteria about which technology to use:

- **Types of transactions** – The financial and non-financial transactions (account opening, loan applications, and cash withdrawal/deposit) which should be supported by the channel. The type of transaction is closely related to the size of data that needs to be transmitted via the channel. For example, account opening frequently requires capturing of a photo or other image, which places a higher load on the platform in terms of data transfer.
- **Security levels** – Depending on the type, value, and relative risk associated with the transactions being processed, the FSP needs to decide what level of security is required from the channel. Other factors influencing this decision include the security standards dictated by third-party networks (EMV provides full specifications of the levels which must be available to participate) and the reputational risk to the FSP should a breach of security occur. While most FSPs would always prefer the highest levels of security available, this decision may ultimately become a cost-benefit analysis, as the highest levels of security will always require the largest investment.
- **Mode of authentication** – Closely related to the security levels, the FSP should ideally decide how customers will be authenticated over the channel, a topic introduced in Chapter 1 and referred to again during the formulation of the strategy. At this point, a final decision is required to know if the channel must be compatible with cards, biometrics, or OTPs. This decision will depend on a series of other criteria, such as KYC regulation, availability of a national ID, customer literacy levels, and use of cards and availability of handsets within the target population. Table 2 compares the advantages and disadvantages of each authentication mode.
- **Quality/availability of communication channels** – It is critical that the FSP is aware of the availability, reliability, accessibility, cost, and quality of the various communication options in its target market and areas of operation. This specifically means knowing whether USSD is available, the quality of mobile data services, and the extent of coverage in the target market. Additionally, the cost and reliability of these services need to be ascertained to prevent selection of a technology platform that is reliant on an inherently unstable network.

The technology selection process needs to be iterative, reverting back to the strategy

Table 2: Modes of authentication

MODE	ADVANTAGES	DISADVANTAGES
Card+PIN	• *Well-established process which is used globally as the most common way to secure financial transactions.* • *Possession of cards can be seen as a status symbol.* • *Convenient for customer to store value without carrying cash.* • *Introduces options for a range of card-based products.*	• *Expensive to produce, distribute and maintain cards (and PINS).* • *Not accepted widely in all markets (especially outside urban centers).* • *Customers have issues remembering the PIN or write it directly on card.* • *Cards can be misplaced or stolen.*
Biometric	• *After upfront investment, cheaper to maintain after one-off registration (bio cannot be lost or forgotten).* • *Well suited to non-literate populations and where no national ID card exists.* • *Provides additional functionality such as deduplication.* • *High-quality authentication factor, that is, hard to falsify so can be used as part of a single factor authentication.*	• *Not yet as widely used across all channels so may need to be used in conjunction with card/PIN (few biometric ATMs).* • *Upfront investment requires distribution of biometric readers which can be expensive.* • *Device failure/unreadable bio records can occur and needs to be catered for with a backup process.* • *Quality of finger prints depend on profile of customer – for example, people who perform manual labour such as in agriculture may have damaged finger prints.*
OTP	• *Cheapest option from the FSP perspective as no devices, cards to distribute.* • *User-friendly workflow.*	• *Transaction times will be influenced by delivery time of the OTP which can be unpredicatable in many countries.* • *Requires all customers to have a phone which is pre-registered with the FSP.* • *Lower grade of authentication factor so must be part of a two-factor process.*

STEP 6:
Select the Platform

- **Handset availability in the market/ target market** – Knowledge of the types of devices available in the market and used by the target users of the ADC platform is a critical input to the decision, particularly for mobile ADCs. In reality, this information may be hard to obtain and may require the FSP to conduct a survey to determine, for instance, what phones their customers are using. There will be a huge difference from one country to another on handset availability and it is imperative that these local trends are taken into consideration. Analysis of local differences also needs to take into account the requirement to support multiple languages and character sets and how this requirement can be met by various devices. Where the ADC platform will be operated by an intermediary, such as a field staff member or third-party agent, the FSP will have more control over the devices used and hence the analysis will be based more on cost, security, and durability.

Equipped with a list of options and the information to make an informed decision, the FSP can now draw some conclusions on three levels: the application level, the device level, and the communications level (refer to Chapter 1 for more information).

To illustrate the decision-making process, we have worked through some examples for mobile and agency banking in Figures 8 and 9. There is no ‘one size fits all’ approach and readers will need to weigh and adjust their decisions according to their best judgement of what is most suitable for their target users.

> *There will be a huge difference from one country to another on handset availability and it is imperative that these local trends are taken into consideration.*

Decision tree: mobile banking

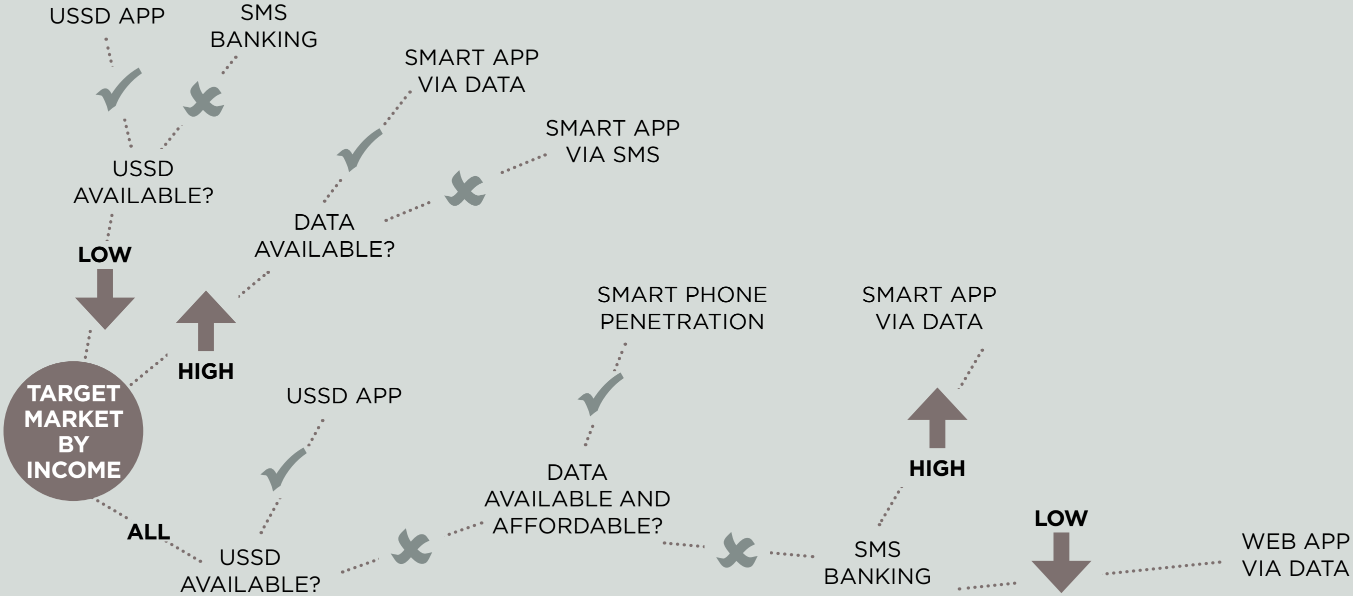
For mobile banking, the communication and devices that are available to the target market dictate the technology choices. In this decision tree, we have opted to consider the income level of the FSP's target market as the initial input to the decision. The order in which these input factors are applied could be switched, or indeed, considered through a different proxy, such as type of handset available to customers – smart, feature, or basic. The decision about which to use may depend on the data available from the assessment phase (for example, the question would be: "do we have a comprehensive survey of customer handsets?"). For those FSPs targeting only higher-income customers, we presume a smartphone would be available and that these users would be more tech-savvy and hence capable of installing a native app. To finalize the decision for these users, we would need to know the quality and availability of data services on the customers' phones, which, if available, would imply using a smart app over a mobile data connection. If data is not available, a smart app could still be used, but with SMS as the means of data connectivity, although this will introduce some limitations on the types of services that will be available due to the size of the message that can be communicated.

The second option identified is where the FSP's market is purely in the lower-income segment, in which case the key decision would be availability of the USSD channel, which would be the recommended option, as it runs on all handsets and is an easy-to-use, menu-based application. In case this channel is not available, and only very basic handsets are used, then the only choice is SMS, which has limitations in terms of security and complexity of transactions supported.

Our last option on the decision tree is where a FSP wants to introduce a service that caters to all market segments, which again needs to consider USSD availability, which, if available, should be used. If only data services are available from a mobile phone and smartphone penetration is high, then a smart app would be the logical choice. For areas where data connectivity is unavailable, or too expensive, the only option is to use SMS. If we have data but no smartphones, then a Web app running on a feature phone would be the ideal option, as it requires no installation by the customer.

The only option that has not been discussed in this graphic is a J2ME app, which could be another consideration where the Web app has been recommended, as both run on feature phones. The major difference between these two is the requirement for J2ME to be manually installed and updated, which for customer-level solutions is not ideal.

Figure 8: Technology Choices for Customer-level Mobile Banking



Decision tree: agency banking

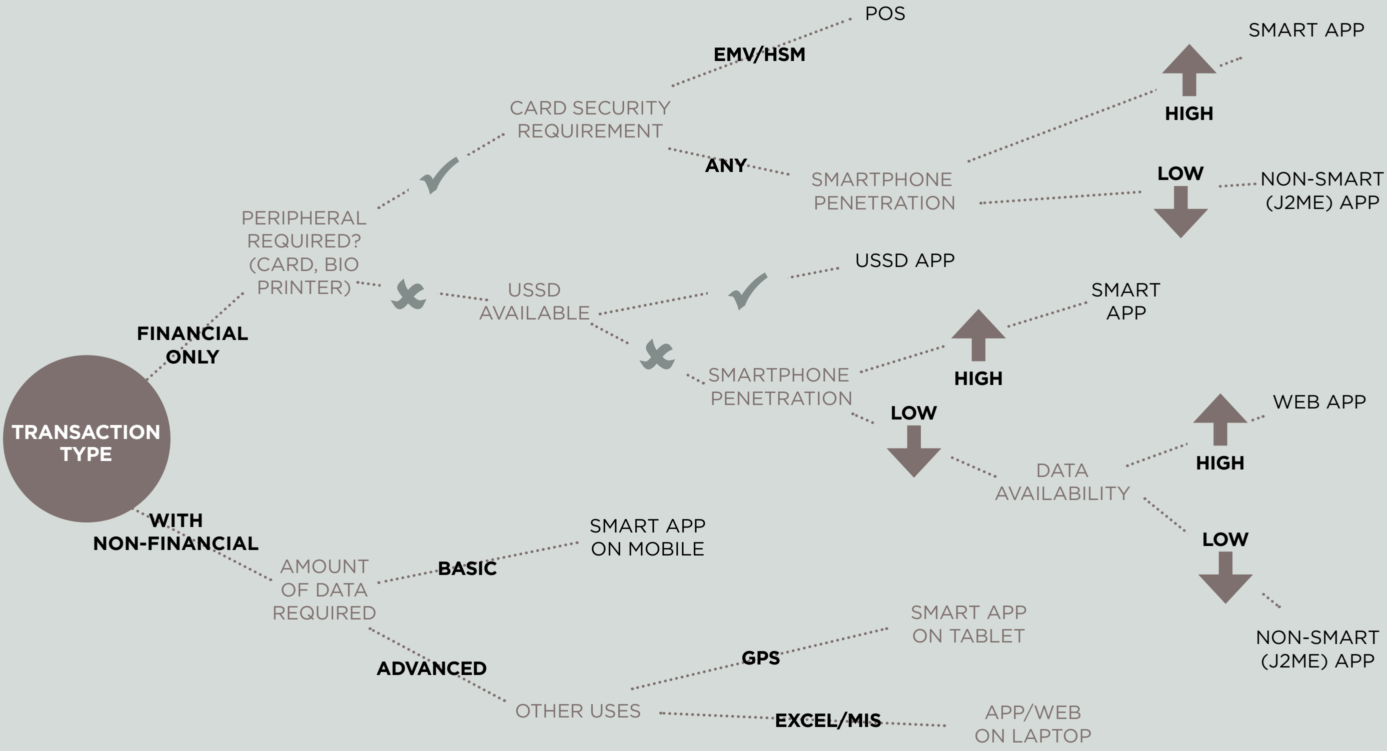
First, the use of peripherals may be considered and this will be influenced not only by the level of authentication required – which will dictate the need for either a card reader or a bio reader – but also by the regulatory requirements for physical receipts to be produced, which could introduce the need for a printer. For FSPs using cards, an important factor to be considered is the level of security or card standard (EMV) that it wishes to apply, as this will impact both on the device (the need for encrypted pin pads) and on the application standards and certification. Other important factors include the amount of data captured and the functionalities for non-financial transactions, such as loan applications and social performance data. A decision is required if all data should be input ("does the FSP want to go digital in terms of data capture?") and if any other data types (such as GPS coordinates of client location, taking of a client photo, signature, or biometric data) need to be considered.

Using this decision matrix, it can be concluded that a POS device is best suited when only financial transactions are required, using high-security cards or biometrics. Alternatively, smart apps are more appropriate when no USSD is available. They can also be used for card transactions, although the security may be less than with a POS device, unless an external pin pad or card encryption is used. Smart apps will also play a role when a FSP wants to do non-financial transactions, with options to use either a phone for small amounts of data entry, or a tablet for larger amounts of data.

USSD also plays a role in agency banking, although it is limited to financial transactions and typically requires both the customer and the agent, on different USSD sessions, to securely complete both cash in and out (cash out would be initiated by the customer on one USSD and cash in would be initiated by the agent on another session). The major limitation with USSD for agency banking is that printed receipts, biometrics, and cards cannot be used with this technology.

Other types of mobile applications, including J2ME and Web apps, also have a potential role in agency banking technology, although each cater for quite a specific set of circumstances and one could easily argue against using them, as the primary use is when there is a preference for a solution to run on feature phones. Given that agency banking works with a controlled group of users (agents and staff), FSPs may decide to invest in smart handsets, given that the price differential between smartphones and feature phones is quickly disappearing, primarily due to the decreasing cost of smartphones.

Figure 9: Technology Choices for Agency Banking



FROM A TECHNOLOGY PERSPECTIVE

For those readers interested in the more technical details, this section discusses the applications and different devices which could be components of an ADC platform.

Applications

Apart from ATM and Internet banking channels, which have standard software, all other ADCs operate on a variety of customisable software applications. Each of these applications has certain advantages and disadvantages, as outlined in Table 3. Smart and non-smart native apps have been combined as the major difference between the two is in the choice of device and not the application functionality. While SMS has mostly been talked about as a communication option, we include it in the analysis of potential applications to show how it can still provide some limited functionality as an application.

Table 3: Application Advantages and Disadvantages

APPLICATION OPTION	ADVANTAGES	DISADVANTAGES
SMS	• *Available in all countries and relatively easy to set up.* • *Accessible on all handsets.* • *Lower dependency on relationship between the MNO and the FSP (can send to all networks unlike USSD, which is per network).* • *Easy to use and most customers familiar with the technology.*	• *Very limited functionality due to limit of message size and non-real-time connection.* • *Limited security, as data entered in SMS is available as clear text in sent messages.* • *Delay in delivery of messages can occur and is beyond control of the FSP.*
STK	• *No software installation required.* • *Device independent, so will work on all handsets.* • *User-friendly menu interface.* • *Encryption keys are stored on the SIM, so applications have control over the security levels.* • *If FSP has access to STK, they can have full control over the channel – (less dependent on third party).*	• *Requires MNO or MVNO license.* • *Involves issuing of SIM cards.* • *Updates to the application are difficult to coordinate, requiring either reissue of SIMs or Over the Air push updates.* • *Customers may need to manage a 2nd SIM card (though not necessarily replace their network SIM) or apply a skin SIM.*

USSD	• *No software installation required.* • *Device independent, so will work on all handsets.* • *User-friendly menu interface.* • *Encryption is in-built in channel, providing good security.* • *No information is recorded on the device.* • *Usage is tied to a registered phone number, which aids in the authentication process of the user.*	• *Not available in all countries.* • *Requires an agreement with an MNO, which is not always forthcoming.* • *No support for peripherals, such as card readers, biometrics, or receipt printers.* • *Primarily supports financial transactions.* • *Limited session length.* • *No offline support.* • *Can be more costly than others depending on MNO communication fees (which are often beyond the control of the FSP to influence).* • *Security (encryption) is fully dependent on the provider of the channel.* • *In many countries, the frequency of dropped sessions is high and still charged to the customer, regardless of whether a transaction was completed successfully.*
NATIVE MOBILE APPS	• *User-friendly and rich user interface.* • *More functionality available – camera, signature, and GPS.* • *Supports connections to peripherals: bio devices, card readers, and Bluetooth printers.* • *Can work offline/online and even in online mode can be more forgiving of poor quality connections.* • *Suited to both financial and non-financial transactions.*	• *Manual intervention required to install and updates often required.* • *Requires support for specific or multiple devices/operating systems, so different versions are required (Java, Android, or iOS).* • *Security must be built in and is not automatically present.* • *Multiple functionalities typically require use of external devices.* • *Compatible handsets tend to be more expensive (feature phone or smartphone), hence less accessible to the full market.*
WEB APPS	• *No software installation required.* • *User-friendly and rich user interface.* • *Full functionality available, but limited access to peripherals.* • *Can be used on different devices (mobile/tablet/netbooks/notebooks).* • *Suited to both financial and non-financial transactions.*	• *Requires good continuous data connectivity.* • *No offline support.* • *Security must be built in and is not automatically present.* • *Requires support of multiple browsers.* • *Limited access to peripherals.* • *Compatible handsets tend to be more expensive (feature phone or smartphone), hence less accessible to the full market.*
WEB PORTAL	• *Can use CBS directly if a Web-based system is available.* • *No software installation required.* • *User-friendly and rich user interface.* • *Full functionality available, but limited access to peripherals.* • *Can be used on different devices (mobile/tablet/netbooks/notebooks), with some limitations.*	• *Requires a reliable and continuous data connection to use (no offline support).* • *Limited access to peripherals (Bluetooth printers and card readers).* • *When used on a tablet/smartphone, usability may not be as good as a mobile application.*
IVR	• *Ability to serve large numbers of customers simultaneously.* • *Pre-recorded messages for consistent accurate communication of information.* • *Limited human intervention to maintain – enables customers to do their own transactions without having to talk with someone.* • *Hosted solutions for small institutions with limited technology experience.*	• *Speech recognition makes it more difficult to navigate an IVR and customers will be inclined to speak with a live person.* • *Complicated menu levels and choices; it can be easy to get lost in IVR.* • *Cost of hosting can be high, depending on the usage.*

Devices

Devices, whether used by the end-customer or an agent/staff member, carry with them many advantages and disadvantages that need to be considered during the selection phase. Some of these are outlined below, with the exception of the POS device, as the application and device need to be considered as one for this channel technology.

Table 4: Device Advantages and Disadvantages

DEVICE OPTION	ADVANTAGES	DISADVANTAGES
BASIC PHONE	• *Cheapest handset/device available.*	• *Only compatible with USSD and STK applications.*
FEATURE PHONE	• *Still relatively low cost compared with other options.* • *Good battery life (compared to smartphones).* • *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Good usability if used for small amounts of data.* • *Excellent portability.* • *Embedded data transfer/GPS capabilities.*	• *More expensive than basic phones.* • *Phone features may limit its function and usability (GPS, Bluetooth, touch screen – model dependent).* • *Peripheral functionality is managed on separate devices (bio reader and printers) and not in-built as with a POS.* • *Less popular platform for app development so may have less access to other apps (if required).* • *Peripherals are limited and need to be managed separately.* • *Not suited to entry of large amounts of data.* • *No in-built security.*
SMARTPHONE	• *Moderate hardware cost relative to processing capacity.* • *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Good usability if used for small to moderate amounts of data.* • *Excellent portability.* • *Embedded data transfer/GPS capabilities.* • *Access to a wide variety of apps/popular development platform.*	• *Peripheral functionality is managed on separate devices (i.e. bio reader, printers) and not in-built as with a POS* • *Battery life may limit some uses (Bluetooth and GPS).* • *Not suited to entry of large amounts of data.* • *No in-built security, but can be added as peripherals or embedded in app.* • *More expensive option compared with feature/basic phones.*

TABLET	• *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Good usability – including more comprehensive screens – reports, and data entry.* • *Good portability.* • *Good battery life for specific models.* • *Embedded data transfer/GPS capabilities.* • *Access to wide variety of apps/popular development platform.*	• *Peripherals need to be managed separately, although some accessories such as tablet covers are available with biometric reader and card scanner built in.* • *Battery life may limit some uses (Bluetooth and GPS).* • *No in-built security, but can be added as peripherals or imbedded in app.* • *Relatively expensive option, although some low-cost options exist.*
LAPTOP/ NETBOOK	• *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Excellent usability.* • *Longest battery life for specific models.* • *Can potentially extend the use: access Web-based CBS and other systems directly.* • *Significant computational power compared with mobile devices.*	• *Requires more training/support and computer literacy.* • *Less portable.* • *Potentially less battery life.* • *No in-built security, but can be added as peripherals.* • *Most expensive device option.*
POS (DEVICE + APP)	• *Strong in-built security.* • *Device is portable and durable.* • *Single device for multiple functions (bio, print, card reader, SIM card) which is a must for many agent banking platforms that require receipts.* • *Fast operation.* • *Limited misuse.*	• *Restricted functionality due to numeric keypad (mostly suitable for financial transactions).* • *Specialized training required for users to operate and troubleshoot the devices/application.* • *Installation and updates support is required often, with some level of manual intervention.* • *Communication capabilities are optional and influence the price (SIM card versus cable or Wi-Fi).* • *Limited offline capabilities.* • *Limited vendors/developers and often have restricted access to device.* • *Cost of device.*

CHAPTER 4

Vendor selection

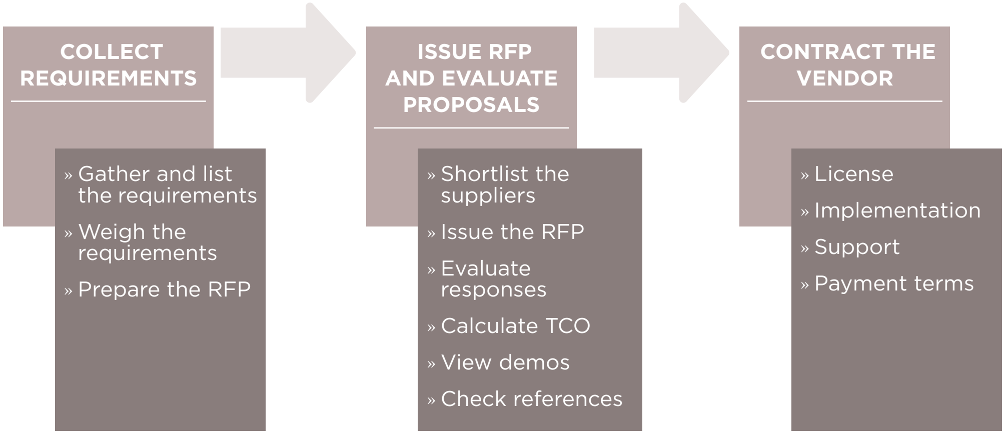
Following the selection of channels and technology platforms, the FSP is now ready to identify the right vendor or partner to help launch the chosen ADCs.

Depending on the size and scale of the ADC project, the FSP may choose to follow a formal Request for Proposal process. This decision will likely be influenced by the FSP's procurement process, the available budget and previous experience. Some FSPs have found that an in-depth gap analysis or requirements workshop with a small number of prequalified vendors can still yield a successful selection. While this approach typically requires some consulting fees up front, it can contribute to considerable cost savings in the long term because the FSP will be equipped with a deeper understanding of the vendor's solution and skills before commencing the full implementation. This chapter will still focus on the more formal, comparative RFP process, although the same points covered could be applied to a non-comparative or competitive selection. Regardless of which approach is used, this stage of the project must help the FSP define its needs, build consensus and obtain stakeholder buy-in for the project, and ideally foster a rational and transparent selection process.

Selection overview

The selection process can be divided into three main stages, as shown below:

Figure 10: Selection process



COLLECT REQUIREMENTS

- » Gather and list the requirements
- » Weigh the requirements
- » Prepare the RFP

ISSUE RFP AND EVALUATE PROPOSALS

- » Shortlist the suppliers
- » Issue the RFP
- » Evaluate responses
- » Calculate TCO
- » View demos
- » Check references

CONTRACT THE VENDOR

- » License
- » Implementation
- » Support
- » Payment terms

> *Ensuring full participation across the business at the outset can help build critical support for the project and protect against selection of a system that does not adequately represent the full needs of the business.*

Initiation

Provided that a FSP has invested the time in the previous stages, the initiation stage of the selection process should be quite straightforward, as the business case and objectives would already be known. However, identifying stakeholders and a specific project team to lead the selection process should ensure representation from across the relevant business units (IT, audit, operations, and finance) so all will have an opportunity to have their priorities considered. This project team will be responsible for defining the selection process, the scope of work and selection timelines in accordance with specific procurement policies and requirements. Ensuring full participation across the business at the outset can help build critical support for the project and protect against selection of a system that does not adequately represent the full needs of the business. This selection team typically becomes the implementation team such that continuity exists between these two critical stages.

STEP 7:

Collect the requirements

Collect the requirements

FSPs should go into the selection process equipped with high-level requirements for the various components of the ADC. While some of these requirements may be easily identified directly from the channel strategy and/or selection of technology platform, some additional requirements, such as transactional workflows, are not obvious, particularly those related to the back-office components of the ADC solution. Taking the time to identify these additional requirements will not only increase the chances of identifying the right solution, but will directly influence the success of the implementation. For all systems, a fully functional specification should be documented at the beginning of the implementation stage of the project, and it is at this point that detailed configurations and decisions are made. This requirements analysis stage is merely to ensure that core requirements are identified as inputs to the selection process. In fact, it is important that these requirements should remain quite high-level, as it is very likely that detailed requirements will change over time as the selection team is made aware of available features and functionality of the proposed solutions.

The selection team should agree on a final list of requirements which can be circulated to potential vendors. Where the selection team has limited experience with ADCs, external consultants can help identify the requirements, as can research. Lastly, learning from FSPs in other countries that have implemented similar channels can be a valuable input to the requirements analysis stage. To assist in this important step in the process, we discuss the most common requirements including security, integration, and back-office systems in the technical section of this chapter. For those looking for more detail on specific channel requirements, the checklist will also provide some additional information.

Weigh the requirements

After the selection team has clearly identified what it is they want the ADC system to do, it is important to make a decision about the relative priority of these requirements as it is unlikely that all hold equal importance. This can be done either through a rating scale to indicate those which are 'must-have' functions versus those that would be 'nice to have'. This will provide valuable input to the vendors so they know which items are of most importance and will assist in the scoring of proposals.

Prepare the Request for Proposals

Once requirements have been identified and weighted, the FSP typically needs to compile these into a RFP document that should provide all the necessary information to help vendors prepare a suitable offer. With this in mind, the RFP should include the following:

1. Brief background about the FSP.
2. Business and channel strategy (may include a phased approach).
3. Business goals that the solution should address.
4. Selection process and deadlines.
5. Criteria for decision-making, including preferences on different licensing structures (license versus SaaS versus revenue share).
6. Expected content and format for the response.
7. Functional, technical, and implementation requirements with weighting to reflect priority.

Given the large number of systems that are priced based on a user/account/transaction basis, it is useful if the strategy section includes projections so that a vendor has all of the required information to cost the solution, and so that the FSP can analyze the full cost over a five-year period. Disclosing the criteria for decision-making will allow the vendor to understand the organization's priorities at a higher level while the functional, technical and implementation requirements should provide a more granular representation of what is important to the FSP. These functional requirements should be a direct output of Step 2 and ideally are formatted in a table or worksheet to ease the burden of analysis. Where relevant, it is useful to indicate if certain functionality will be required only in a second or subsequent phase of the project, as this way, cost proposals can be aligned to the actual timing of when the functionality will be used.

Clear directions and expectations need to be provided as part of the RFP document so that vendors know what should be included in proposals. Ideally each vendor's proposal should include the following:

- Executive summary.
- Company information.
- Scope of the solution.
- Requirements fulfilment (showing how vendor systems meet the stated functional, technical and implementation requirements) and compatibility with back- and front-end interface.
- Proposed architecture.
- Project implementation approach – including design, piloting, risk assessment, audit considerations.
- Training and documentation.
- Description of support services and location.
- Cost for the solution, including license, implementation, upgrades, and support.
- Payment terms.
- References.
- CVs of key team members.
- A copy of the License Agreement and Service Level Agreement for support.

8 STEP 8: *Issue the RFP and evaluate proposals*

Depending on the FSP's procurement policy, the timeline for the selection process and the organization's knowledge of the market, the FSP may choose to publish an open RFP or to invite only selected vendors. The latter is more efficient and can be achieved with a formal prequalification round, referred to as a Request for Information or Expression of Interest, or informally through some research into the potential vendors. While the formal prequalification round can help narrow down a short list, it requires additional time for review and assessments of submissions.

Who should be invited to the RFP?

An Internet search is the easiest way to narrow the list of firms invited to respond to the RFP. Technology conferences are also useful, as are conversations with consultants and peers. The selection team can then contact the vendors to:

1. Check if the vendor qualifies based on high-level requirements (online versus offline, and what applications/modules are available).
2. Confirm that the vendor is interested in participating in the RFP.
3. Ask for the estimated price range to make sure that the solution is within the budget. While not all vendors will be willing to share this information, it is usually possible to at least get a ballpark estimate of costs.

How to evaluate the responses?

Evaluation needs to include several steps to analyze the proposals received, calculate and compare the financials and then to qualify this information by viewing a product demonstration and speaking with existing customers in the market. In cases where there are more than three qualified participants, the organization can choose to rank the participants and only evaluate the top three participants further.

Plot, analyze, and compare responses

Scoring RFP responses is the most straightforward part of the evaluation. Compute the percentage of the requirements that is met with consideration to the weighting of these requirements. Usually, a 75 percent fit is good enough, as it is unlikely that a single solution will meet all of the requirements. This step must be done with a certain amount of scepticism, as it is quite easy for vendors to indicate on paper that they can meet certain requirements, and later have difficulty demonstrating these capabilities or providing references in a live environment.

Flesh out the financial proposition

The cost of an ADC, just like any system, continues past the implementation phase. In comparing the costs for each of the solutions, it is important to consider the Total Cost of Ownership of the system over three to five years. While costs in the initial year are typically easier to estimate, and hopefully clearly laid out in the cost proposals from the vendors, costs for the second and subsequent years should anticipate enhancements to the system on top of the annual maintenance or support fee. Additionally, it is critical that 'like is being compared with like', both from a functional standpoint but also financially, where vendors have used different costing models. For instance, it is tempting to conclude that SaaS or revenue share models are much cheaper than upfront licensing when only transaction levels for the first couple of years are considered, but these figures can quickly change as volumes and usage increase over time. Computing the TCO compares the financial evaluation for the buy, build, or rent options.

The TCO should include the following:

- The solution's license fee and/or usage fee for a 'rent' option.
- Implementation cost.
- Integration cost – both to the CBS and to any third parties that will be included in the channel.
- Travel and accommodation costs (if needed).
- Hardware cost and/or hosting cost.
- Initial and recurring connectivity cost (data, SMS, and USSD).
- Supporting licenses cost (operating system and database licenses).
- Cost of devices and/or peripherals.
- Annual maintenance (or support) fee.
- Revenue share (if applicable).
- Vendor daily fees for customizations/ enhancements after the first year.

Of course, the financial decision can also be based on other criteria such as the payment terms. The FSP (based on strategy and/or cash flow) may prefer a solution that costs less initially as opposed to the one with the lesser TCO.

Request demonstrations and seek references

The proof of vendor quality lies in the ability to demonstrate the functionality of the system, but also to provide clear evidence of satisfied customers using the systems. This is therefore a critical step in the evaluation process and due care should be taken to ensure that it is carried out properly. Demonstrations of the systems should ideally be done in person, as this also gives an opportunity to interact with the vendor and get a sense of the ability to respond to *ad hoc* questions. However, in this connected world, many vendors can provide online demos, provided that clear expectations are set regarding what should be covered during the course of the demonstration. While it may not be possible to demonstrate all of the functionality requested in the RFP, the core requirements should be shown so that the selection team can get a good impression of both the front and back end of the solution. Those participating in the demonstration should be prompted to give feedback to the selection team, noting their impressions of the system and any concerns that they have.

Obtaining references from existing customers will help the selection team evaluate the quality of the solution as well as the quality of the implementation and ongoing support services. A strong demonstration without corresponding positive references should be of concern. Nevertheless, new vendors are emerging continuously and FSPs should be aware that taking a calculated risk to go with a newcomer who may not have a long list of referees can at times pay off.

9 STEP 9:
Contact the vendor

Once a full analysis of the proposals and vendors is complete, a preferred vendor can be contracted. Where a preferred vendor can be identified, the final stage involves agreeing on contracting terms for the product/service. Contracts need to be reviewed with care, with specific attention paid to deliverables, payment terms, responsibilities on both sides, and support level agreements after the 'go live' stage. Sufficient time should be budgeted for the negotiation phase, as these legal agreements typically require review at different levels within each respective organization, with input from legal teams. Commercial negotiations can be drawn out if there is a significant gap between the quoted price and the FSP's budget.

Sometimes though, the selection process may not yield a clear winner. In this case, the FSP may need to reassess its requirements, by either adjusting these in line with what is actually available in the market, or by carefully considering the 'build' option to develop a solution in-house.

FROM A TECHNOLOGY PERSPECTIVE

As discussed above, to prepare a comprehensive RFP document, the FSP would need a good understanding of the technical systems involved in ADC platforms. This involves the front-end applications, back-office administration modules, and the integrations between these systems and the CBS as was previously introduced in Figure 5. While this handbook is not a comprehensive guide on each of these areas, we will attempt to introduce the main areas that are relevant so that this information can be referenced during the requirements gathering step.

Front-end applications

We have discussed in some detail in Chapter 3 the different technologies available for front-end applications, including USSD, mobile apps, Web platforms and bespoke systems such as POS or ATMs. Irrespective of which technology is selected for the front end, certain functionality and features should be present and, if deemed relevant, reflected in the RFP. This includes:

1. **Compatibility with devices/models** – The FSP has to clearly state what their expectations are in terms of compatibility of the front-end application with the devices available in the market. For mobile-based systems, this is typically stated as a compatibility with operating systems and versions of that system, i.e. Android version 4.0 and above. For Web, the expected Web browser and minimum version supported are also useful. For bespoke applications where the device model has been identified, this should also be mentioned (that is, compatibility with Ingenico POS or NCR ATMs).

2. **Transaction types** – The functionality supported by the front-end application must be clearly stated in the RFP so that vendors can confirm availability of this functionality and also gauge the implementation efforts adequately. This would ideally include a list of different types of transactions expected to be supported, perhaps with some phasing to show what would be deployed initially versus later. So, for example, if the FSP needs the ADC platform to support non-financial transactions such as customer registration, photo capture, and biometric enrollment, it is worthwhile to list these. While support for transaction types should be provided at the front, middle and back end, at this point we are considering how the end-user interacts with the system to initiate and complete the transaction.

3. **Registration** – Most ADC solutions need to provide some support to cover the registration of users on the system. This is typically initiated via a back-office administration system and then completed through some interaction between the front-end application and the end-user. For example for a channel such as mobile banking, a customer would typically request access to the channel through an online application form. The FSP's back-office staff would then process this request by putting in the details into the registration module of the ADC solution.

   FSPs should be clear about their expectations in terms of this registration process, which typically overlaps with the capture of the agreed mode of customer authentication such as a biometric registration or PIN creation. Where customer-driven registration is required, the registration process needs to carefully consider the limitations of the technology used; for example, if using USSD, the amount of data that can be input should be minimized to avoid sessions being disconnected before completion of the process.

4. **User interface** – Although somewhat difficult to specify in a quantifiable way, the usability of the application needs to be considered, particularly where end-users or third parties are interacting with the front-end application. Within the RFP it may be wise to mention any specific design criteria, usability metrics or expectations that the FSP has in terms of how user friendly the application should be. This should include any language preferences/translation requirements and whether the interface needs to be designed for low-literacy target markets as this can influence the design considerably.

Back-office systems

The back-office systems for ADCs are the systems which are used to administer the products and services offered via the channel and which support all processes associated with their use. These systems are typically accessible only to the FSP staff, most often the IT department responsible for the administration of the systems. Some examples of such systems include: agency management, an ATM device management system or the administration of an Internet banking platform which would be used to subscribe customers for the service. When considering selection of the back-office components of an ADC solution the FSP should consider the following functionalities, some of which are generic to all ADCs while others are relevant only for some channels.

1. **Registration** – As discussed above, the functionality to register customers or agents typically involves both front and back-office applications. From the back-office perspective, particularly for mobile channels, functionality should be available to confirm the customer's phone number, either directly with the customer or with another source of information such as an MNO database. Registration of agents may include this same phone number verification step, but typically also involves linking the agent to a float account that will be used as the contra account for all transactions posted by the agent. Registration of agents also involves defining what operations they can access on the system and very often defines the hierarchy by which they will be managed- i.e. master agent, aggregator. Lastly, the registration of agents, which is typically bundled as an agent management solution, must also help to define the limits that are applied to agent-initiated transactions and the commissions that they should be paid for conducting these transactions.

   Registration at the back office is closely linked to user management, which involves the administration of access rights and roles for end-users of the channel, as well as administrators of the system. Both back- and front-office systems must adhere to best practice in terms of user access roles and rights to ensure that all different types of users – from customers to agents and system administrators – have appropriate access to perform their roles. The chosen back-office solution must be able to standardize this user administration task, and of course ensure that all access and use of the system is supported by a detailed and accessible audit trail.

2. **Fee management** – Back-office systems should also provide the necessary configuration tools to administer the products and services

being offered over the channel. This is likely to include fees associated with different transactions, and must be flexible enough to cater for changes over time and a range of different computation rules. Furthermore, these systems should be parameterized, allowing an administrator to change fees with a user-friendly interface rather than requiring expensive changes by the vendor with hard coding. Finally, the calculation and initiation of payment of agreed fees should be automated through integration with the CBS with the flexibility to set payments at the point of transaction or at a pre-defined interval. Depending on the CBS in use, the fee calculation can possibly be done in the CBS itself with the ADC just triggering this charge, rather than calculating it. In such cases the requirements for the back-office ADC system is reduced.

3. **Commission management** – Specifically for agent management systems, functionality is typically required to define and calculate commissions due to the agent. Much like the fee definition module, this needs to be flexible for the system administrator to adjust these settings over time, ideally without a dependency on the vendor. Rules associated with commission payments can often be complex and while a FSP need not define these in full at this RFP stage, it should ideally have some idea of the calculation basis that will be used.

4. **Device management** – For certain ADCs, including agency banking, ATMs, and extension services, a system would ideally be present to help control the access to and usage of the devices used in the channel. These systems will differ depending on the technology platform used but roughly can be divided between Mobile Device Management solutions and pure device management associated with ATMs and POS devices.

   The MDM solutions in the market help not only to secure the devices, but also to monitor and support mobile devices deployed by an institution. Such solutions can allow for a remote deletion of data, which may be particularly important if sensitive data is stored on the device as is often the case if solutions work in offline mode. Additionally where the channel involves merchants/agents or staff using devices remotely, functionality should be available to map a device to a specific user so that access is tied to the use of a specific device. This can be done either by registering a device serial ID or an International Mobile Equipment Identity code, which will be validated as part of the log on process and used to track GPS location of the device.

   By comparison, the device management systems for ATMs and POS are much more complex in that they ultimately drive the functionality of the devices, controlling the screens and status of the machines, as well as handling all processing of transactions and the associated cash management. These back-office systems provide administrators with an operational management and monitoring system that must include reconciliation and fraud processing. Where ATMs/POS devices are part of a wider network such as VISA or MasterCard, these systems will also be responsible for routing, or switching, the transactions to the issuing bank.

5. **Card management** – For FSPs planning to use cards, the major decision will be whether or not to manage the cards in-house or to outsource this function. This decision will be influenced by a number of factors including the volume of cards required, availability and costing of outsourcing options, in-house resources to operate card services (applications, printing, distribution and help desk), required turnaround time for new and replacement cards, and the type of card that the FSP wants to issue (private label vs. international network). While no hard rule exists about which is better, an observed trend is for FSPs new to cards to initially outsource this function and only bring this in-house when volumes increase. Some networks supply the full suite of outsourced cards and ATM network management for many FSPs. The risk here is that the FSP does not have control of the ATM functionality. Hybrid models also exist whereby only the card production/printing is outsourced and all other functions are handled in-house**.**

For FSPs that do decide to bring this function in-house, a Card Management System will be required to support the following functions at a minimum: card setup, application, production, management (black listing, account blocking, and card status changes), setup of system codes, fees, limits, and very often complaints management. The CMS will need to be connected to a HSM or SSM, which is responsible for generation and verification of PINs, generating encrypted card values such as Card Verification Values, encryption key generation and management. The HSM is typically connected to a designated printer for PIN Mailers and typically both printer and HSM should be purchased in duplicate for redundancy purposes. CMS systems very often contain a customer management or issue management system for use by the help desk running a card center to record and manage the customer service side of card services.

For those FSPs that opt for outsourcing, a CMS can be eliminated although it may still be necessary for some system, either the back-office administration system or the CBS, to record card numbers allocated to customers for reference purposes. Additionally, a robust process needs to be agreed on with the partner to ensure that the application process is seamless and completed in the shortest possible time. If only the card production process is outsourced then the CMS is still required and will need to generate a card production file that is compatible with the card producer.

6. **Settlement and reconciliation** – Any solution that includes transactions passing through more than one system will need a reconciliation process to ensure that all information is matching between the various systems. While systems should be available to support reconciliation, the extent to which this process can be automated will depend on the availability of a unique identifier stored in all of the reconciling systems. Ideally, back-office systems will include such automated reconciliation support, or at the minimum, the reports to support the manual reconciliation process.

   Functionality to support the settlement process will be required for ADCs involving merchants or third party card transactions. Settlement can either be done manually using reports as a means of identifying funds due/owed followed by manual transfers. Alternatively where a settlement bank is in place, with all parties holding an account at this bank, settlement could be automated as long as rules and schedules are clearly established between all parties. Functional requirements surrounding settlement will really depend on the role of the FSP in the network and whether they are the issuer, acquirer or payment service provider.

7. **Reporting** – All ADC systems need to contain a suite of reports to help the administrators and managers monitor the channel usage and performance. These reports will differ per system and FSP but could roughly be grouped as follows:
   - » **Audit reports** – Used to trace the usage of the system and help the FSP support team track any problems which may occur.
   - » **Channel performance reports** – Show the volumes of transactions on the platform, ideally by transaction type and in both a summarized view and a detailed listing. Additional metrics include the number of users registered, transaction growth rates, and other metrics to measure channel uptake. These reports will be key for management to measure the success of the channel, based on a set of KPIs.
   - » **Security/suspicious transactions** – The ADC platform should contain reports to show any suspicious transactions which could be extracted, either based on AML standards or using custom definitions, and escalated for further analysis by the FSP's risk management team.
   - » **System administration reports** – Used to show platform availability, up time, and transaction performance.

While the back-office systems are necessary to support the operations of the channel, they also play a key role in the risk management of the channel. In many cases these are the systems that are used to monitor the suitability of the controls put in place to protect the channel. Risk managers and auditors should be conversant with each of these systems, both to ensure that they are configured according to best practice and as such do not introduce new risk, but also so that they can extract the required audit reports as part of risk monitoring and testing of controls.

Integration components

The final component of ADC platforms involves integration between the various systems involved in the ADC platform. Introducing ADC technologies in most cases requires some level of integration between the FSP's back-office systems and the technology driving the channel. In many cases, ADC solutions also require multiple integrations with third parties (m-wallet providers, bulk SMS providers, and national switches), as well as several in-house systems (m-banking software, agency banking modules, accounting software, and CBS).

The starting point for this discussion should be the fact that integration interfaces can be categorized into two types: real-time or batch processing. As the name implies, real-time processing ensures that transactions initiated at the ADC customer interface are updated in the FSP's CBS immediately at the point at which they were initiated. For batch interfaces, on the other hand, there is a delay between the point of transaction and the time when the transaction is reflected in the CBS. Batch integrations are achieved through the transfer of files, either manually or using the File Transfer Protocol, and though cost-effective, are not ideal for financial transactions.

Real-time integrations to the CBS can be achieved through the use of Application Programming Interfaces, which specify how two different systems can communicate with each other through the exchange of 'messages'. Several different types of APIs exist, including those based on the Web, TCP communication, and direct integration to a database, or proprietary APIs written for specific systems. Discussions about APIs very often overlap with the mention of messaging protocols, which are the series of rules that govern this exchange of messages sent via the API. These rules may include the sequence in which messages must be sent and will be defined independent of the language used to write the message. Table 5 provides some examples of APIs and protocols that are commonly found in the financial sector, the most common of which will be further described in the section below.

Table 5: Integration APIs for ADCs

	EXAMPLE USED IN FINANCIAL SYSTEMS
API	*Web service, TCP, database level, proprietary*
WEB SERVICE/WEB API	*REST, SOAP, XML-RPC*
MESSAGING PROTOCOL	*ISO 8583, ATM management protocols (NDC, AANDC, DDC)*
LANGUAGE	*XML, JSON, Java, C#, JavaScript, Delphi*

ISO8583

ISO8583 is a standard messaging protocol used for exchanging electronic transactions between financial systems, primarily used with card-based systems. The protocol provides the message format and communication flow for different systems to exchange transaction requests and responses, and consists of a series of Message Type Indicators which describes the function of the message. For instance, the MTI0100 refers to an authorization request. Each message consists of 128 fields, some of which are pre-defined to contain certain data such as PIN, while others are configurable or optional. Several different versions of ISO8583 are currently in use (1987, 1993 and 2003) and so with each integration project the version and exact usage of the protocol must be agreed between the integrating parties. While ISO8583 provides a commonly used standard in the industry, it has some limitations, primarily related to the exchange of non-transactional data which may require systems integration to consider combining ISO8583 with other APIs to fully achieve the desired level of integration.

HTTP / web APIs

Where integration is required not only for transactional data and/or when ISO8583 interfaces are not available, more open Internet-based APIs are typically employed. These are most commonly referred to as Web services and can be used for two systems to exchange information. APIs are typically defined as a set of Hypertext Transfer Protocol request messages that have defined structured response messages. These messages can be written in various different languages such as Extensible Markup Language or JavaScript Object Notation format.

EFT switches and middleware

Systems integration for financial institutions is increasingly being driven by the use of an Electronic Funds Transfer Switch or equivalent middleware. The primary function of these systems is to connect different ADC systems such as ATMs, POS, mobile and third parties with the CBS. This software application is specifically designed to help systems communicate and exchange information and will typically support one or more of the integration protocols and APIs described in the previous section. For many FSPs, investment in a switch will lay the foundation for multiple integrations all via the same platform, which can help standardize the integration approach and provide a single point of audit for external transactions posted on the CBS.

The switch will provide conversion services to translate messages received from one system to a format that is understandable to another. For example, if a FSP wants to integrate its CBS with an m-wallet provider, which has an API, then the switch or middleware would translate the transaction message received via the API to a format that the FSP's CBS can understand. This could be an ISO8583 standard, a Web service or a database level integration. While communication and translation of messages are the core functions of a switch, it can also provide other functionalities such as 'Store and Forward' options to ensure that channels remain available even while the CBS is offline for routine end of period processing. This functionality is delivered by copying all core data required for processing, such as customer balances, to the switch and transacting against this data up until the host system is available again, at which point these transactions are sent for posting. This is commonly used with ATM systems to ensure that the channel remains available during end of day processes. Lastly, with every ADC the topic of reconciliation, and in some cases, settlement, is critical. The EFT switch can provide either automated reconciliation, which will match transactions posted in the various systems using unique transaction IDs, or the required reports to manually reconcile all connected systems.

Other requirements

While the ADC front and back-office applications and integration require some specific functionality as discussed above, there are some more general features which must be reflected in the RFP and considered during selection. This includes:

1. **Hardware and networks** – Clearly all software applications must be installed in a supporting hardware and network environment. The choices regarding how and where to install the applications have evolved considerably from the traditional installation on the FSP's servers to external hosting in a data center or in the cloud. Disaster Recovery Sites has become a recommended base practice for institutions that have the resources to maintain an additional environment offsite. Table 6 shows some of the details for each of these options. Selection of an application hosting option need not overlap with the licensing model of the system. So while many cloud based systems are on a pay-per-use basis, it is perfectly feasible to install a licensed product on a cloud environment.

2. **Security** – Security should be considered at every level of a transaction system solution, from the front-end application to the database and CBS integration. Each of the available channels will have different methods to assure the security of the system. Below are some specific areas to consider:
   - **Application installation** – This deals with how to protect against users installing an application on unauthorized devices and is typically handled by a device management module.
   - **Application access** – This helps restrict access to only authorized users (via a user login, password, PIN, and biometric controls).
   - **Data transfer/network security** – This ensures that data transferred from remote devices is done securely through VPNs or channel encryption.

- **Database security** – This facilitates encryption of data and logic stored in a database with best practice applied for direct database access.
- **Versioning control** – This ensures that only an approved version of an application is circulated to users and prompts users to update to the latest version, if applicable.
- **Application level controls** – This refers to the processes that are built into the system, which must be done in a specific manner so as to minimize risk to the FSP. In many cases this involves introducing maker/checker concepts for processes which are deemed high risk and system-based controls to minimize the risk of data entry errors.

3. **Scalability** – Introduction of a new channel needs to carefully consider the potential scale at which the channel will be expected to operate to ensure that the performance remains acceptable as the usage increases. Performance standards should be stated both in terms of volumes and transaction response times so that the FSP can confirm with the vendor that the solution is capable of meeting these levels. Performance will always be influenced by both the hardware and software available so for in-house systems, the FSP will need to ensure that the required hardware is available to not hinder performance.
4. **Flexibility** – While difficult to measure directly, a FSP looking for a new ADC solution must try to ascertain the level of flexibility of the solution on offer. This could be done through system settings to introduce new products/ fees/commissions or it could involve getting estimated efforts for adding in new channels. The FSP needs to determine how much effort (and cost) would be associated with such changes and be confident that they will be able to respond to the market feedback on their channel in a reasonable amount of time. Flexibility should also be approached from the customer's perspective to ensure that any customer – regardless of which handset they use or which network they are subscribed to – is able to access the FSP's channel service.
5. **Availability** – As with all business critical systems, the FSP needs to protect against system down time through investment in a backup/ disaster recovery strategy. The complexity of these plans will vary considerably from one FSP to the next, and in general is directly related to the risk associated with system down time. While all would like to ensure zero downtime occurs, this comes at a cost that needs to be justified by the FSP in terms of the channel importance. During the selection process, the FSP needs to communicate its expectations regarding continuity to potential vendors, particularly where it is looking at a SaaS model which means that the responsibility for the disaster recovery environment will lie fully with the vendor. In cases where a licensing mode is being pursued, the responsibility for disaster recovery is typically with the FSP, although it will need to ensure that the vendors can comply with its disaster recovery plans and that all licenses will cover this secondary environment.

Table 6: Application hosting options

OPTION	DESCRIPTION	ADVANTAGES	DISADVANTAGES
IN-HOUSE SERVERS / DATA CENTER	*FSP would be responsible for the procurement of the servers, either through a direct purchase or leasing model. Typically, responsibility for maintenance is in-house, although there may be potential to outsource just the maintenance.*	• *Limited/no dependency on third parties so FSP has full control of the environment.* • *No requirement for connectivity to external hosting center and/or cloud.* • *No challenge with regulators, as database is stored locally; regulators are most familiar with this model, so no need to educate.*	• *Dedicated resources required to manage the hardware.* • *Risk that in-house resources not specialist in this area, opening the FSP to risk of systems unavailability due to hardware issues.* • *Costs are incurred upfront on procurement rather than spread over time based on usage.* • *Requires excellent planning to cater for growth and ensure that the servers are not limiting the system performance.* • *Planning and execution of systems to support disaster recovery lies fully with the FSP.*
EXTERNAL DATA CENTER	*FSP would contract server space through a third-party company who maintains a physical data center that they rent to the FSP. The FSP would then set up a reliable connection so that end-users can access these servers as if they were in-house.*	• *Skills to manage the servers is left with specialists with no need to bring in-house.* • *Generally is easier to scale up performance by just renting additional space/processing capacity.* • *Physical servers can be visited.*	• *Reliance on a third-party provider to ensure that business-critical systems remain available. Not all data centers are equal in quality, so this risk depends on the market/vendor.* • *Regulators may raise issues with systems not being in-house.* • *System availability dependent on connectivity to data center.*
CLOUD	*FSP contracts with a hosting company that provides access to servers hosted in the cloud. Like with a data center the FSP would then need a strong connection for end-users to reliably access the system. Unlike with a data center, these cloud servers cannot be physically accessed.*	• *Skills to manage the servers are left with specialists, with no need to bring in-house.* • *Generally it is easier to scale up performance by just renting additional space/processing capacity.*	• *Reliance on a third-party provider to ensure that business-critical systems remain available.* • *Regulators may raise issues with systems not being in-house and not being able to visit the physical data center.* • *System availability dependent on connectivity to cloud.*

CHAPTER 5

Implementation

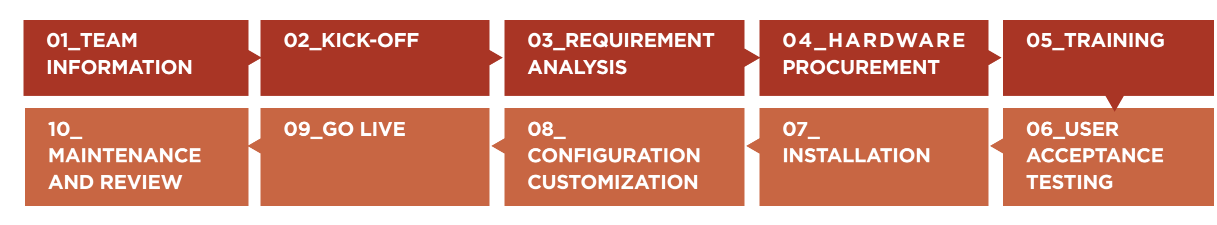
Following selection of a vendor, and equipped with all the information and decisions made in the previous steps, the FSP is finally ready to commence implementation of the channel solution and launch operations over that channel.

STRATEGY
TECHNOLOGY
SELECTION
IMPLEMENTATION

This phase of the project has two major components: the implementation of the technology solutions and the operationalization of that technology. The first component is largely driven by the technology vendor, who with input from the project team will work to install, configure, train and support the live deployment of the ADC systems. The second component will be driven primarily by the internal project team and will focus on all of the supporting activities such as agent recruitment, marketing, end-user/customer training, and setup of supporting structures for the channels, such as helpdesks and customer service lines. Given the technology focus of this handbook, we will put more emphasis on the first component, although it should be clear that one without the other will likely result in either a failed project or one which fails to meet its full potential.

Implementation methodology

The methodology followed during systems implementation is not specific to ADC solutions, and may vary slightly from one vendor to the next. The diagram below outlines one suggested implementation methodology that could be adjusted as required to fit a particular situation. For example, if the FSP has opted for a cloud based system, then the hardware procurement (step 4) will not be required. Alternatively, the implementation of a new system will always look slightly different from a project that replaces an existing system, with the latter requiring additional steps to cater for data migration. Lastly, where the implementation involves the introduction of a new channel, most FSPs opt to launch a pilot initially, with a closed group of users to test both systems and product offering. We will talk through each step in brief in the following section so all are clear on what tasks should be completed in each step, and potentially who is involved in each task.

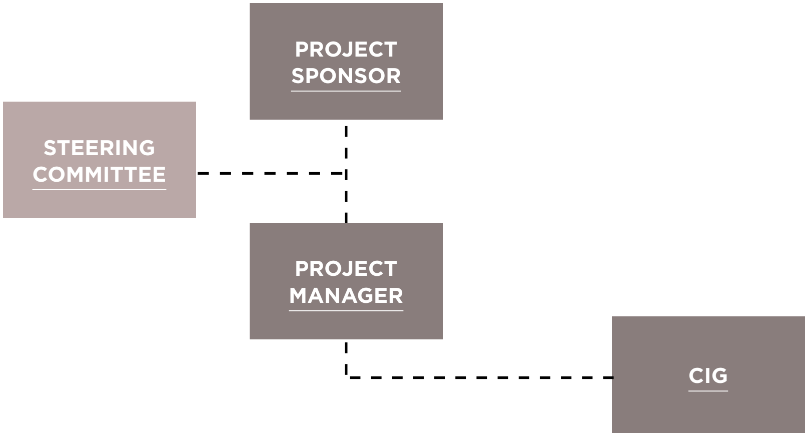


Most financial institutions opt to launch a pilot initially, with a closed group of users.

10 STEP 10:
Prepare kick-off and analysis

The purpose of this step is to identify the Core Implementation Group who will likely consist of members from the project team that participated in the selection stage, as well as relevant representatives from finance, IT, customer service, marketing, operations and audit. This operational group will be involved in training, requirements analysis, and testing of the systems, and typically form a group of 'super users' or champions of the system. Where the vendor adopts a 'train the trainers' approach, this group will receive this training and be responsible for end-user training prior to going live. The CIG will take most of the day-to-day decisions regarding the project and work directly with the project manager and team appointed by the vendor.

Figure 11: Project team structure



In addition, a project steering committee should also be in place, headed by a project sponsor to whom final and more critical decisions should be escalated. This person typically will have a reporting line to the board if the project is tracked at this level, and will weigh in on decisions regarding budget, "go live" and any other critical decisions that need to be taken during the course of the project. The CIG and steering committee need to decide at the outset how decisions will be made and project status communicated. Taking these simple foundation steps regarding the team structure, decision-making process and communication can help prevent project delays and disturbances as things progress and obstacles arise.

Project kick-off

This is an official meeting to mark the start of the project and takes place once the contracts with the vendor have been finalized and the team driving the project has been identified. From the vendor's side, the project kick-off meeting is an opportunity to introduce the project manager and team assigned to the project. The kick-off meeting agenda should focus on introductions of the teams, with clear assignments of roles and responsibilities. The implementation methodology should be presented by the vendor and agreed with the internal team, as well as a high-level project plan if possible, although most vendors can only confirm on this plan after the detailed requirements analysis phase is completed. The vendor may also wish to introduce specific policies on change management or systems used during User Acceptance Testing. Lastly, an escalation process should ideally be discussed at this early stage to resolve any issues that may arise.

Requirements analysis

Throughout the whole ADC implementation process, requirements for the solution have continually been refined, starting with the high level channel strategy and culminating with this implementation step where final decisions on the configuration and customization of the ADC take place. This is reflected in Table 7 with an example of how it is applied to a channel, in this case agency banking.

Table 7: Levels of requirements analysis

DEVICE OPTION	REQUIREMENTS ANALYSIS	EXAMPLE
CHANNEL STRATEGY	*What do we want to do? Define the products and services that should be available over the channel.*	*Introduce agent banking to reach rural customers and mobilize savings.*
TECH PLATFORM IDENTIFICATION	*Which technology is best suited to our strategy?*	*Agents to be given smartphones running an application and connected to a biometric device for authentication.*
SELECTION PROCESS	*What exactly do we expect the ADC solution to do, both for short- and longer-term planning?*	*Support both financial and non-financial transactions with biometrics. Provide a full agent management system. Integrate to the CBS using available web APIs.*
IMPLEMENTATION	*How do we configure / customize the solution for the initial implementation? Define the project phases and scope of each.*	*Agents to be organized into a three-level hierarchy. Allowed transactions restricted to cash in / out and customer registration. Phase 1 with Phase 2 to include loan applications.*

From the vendor's side, the project kick-off meeting is an opportunity to introduce the project manager and team assigned to the project.

The requirements analysis work done at the implementation phase is typically led by the vendor, as they will know what their system is capable of doing and should advise on the best way to map this to the FSP's products and processes in a gap analysis exercise. For some ADC projects, particularly those that involve the introduction of new channels, the requirements analysis done in the previous stages of the overall project will be a critical input to this phase. If such requirements are not available, this requirements analysis with the vendor can easily become a prolonged exercise and at worst result in the vendor rather than the FSP driving the channel implementation. Suffice to say that this is one of the most critical steps in the implementation process, with many failed projects attributed to a poor requirements analysis stage. It is imperative that at the end of this step, the CIG is comfortable with the functionality that will be delivered and whether this will entail configuration of existing system parameters, customization of new functionality or a mixture of both. Appendix 1 provides some guidance on the key decisions to be made during this phase.

Different vendors will employ different methods to extract the FSP's needs; some may employ presentations or demos, others may conduct a gap analysis and others still may come with a blank slate. A gap analysis workshop is preferable, as it helps ensure that the FSP is aware of the existing functionality of the system and can simply overlay new needs onto this system, thereby minimizing customization, which is always a risky and often costly task. Investing time in this initial workshop will not only help understand fully the implications of decisions made in this specification phase, but will also be a foundation on which the training for UAT can build.

At the end of this phase, a detailed specification document should be available and must be signed off by the vendor and the FSP, as it will form the basis against which delivery will be measured in the later phases of implementation. Changes may arise at a later point, but these should be tracked separately, usually through a change request process. The specification document should ideally contain the information listed below, and in general the more detail available the better as it will limit the risk of misunderstandings between the FSP and the vendor.

1. **Process workflows that will be used with the system** – Touches on how a transaction will be initiated, validated and processed.
2. **Configuration settings to be made** – Relates to the products, fees, commissions, user roles, workflow, and screens that should be configured.
3. **Customizations** – Functional description of how the system will be customized to meet the FSP's requirements.
4. **Reporting** – List of expected reports from the system, ideally with detailed specification as to what information is contained.

At the end of this phase, the vendor should be able to provide the FSP with a final project plan, since up until this point all plans were based on assumptions rather than clear requirements. Many a project faces its first obstacle at this point when the vendor provides a delivery date beyond the FSP's expectation. If so, a compromise may be reached by splitting the project into phases, which is recommended so that requirements can potentially be revisited or revised based on inputs from live use of the systems. For many new channels, it is difficult for the FSP to envision exactly which functionality will be most important and how users and customers will respond, and hence a phased rollout will provide an opportunity to incorporate feedback from live operations rather than building systems based on expected usage.

Hardware procurement

For those ADC systems that require the FSP to procure supporting hardware or implement new networks, this project phase should clearly identify these requirements and follow through with the necessary procurement. The specific hardware needed will clearly depend on the ADC technology being implemented, which can typically be split between front-end devices, used by customers and staff, versus the back-office servers hosting the applications. Care must be taken to ensure that the vendor of the ADC applications has fully tested these devices and can confirm that they are compatible with the software. Additionally, with an increased number of options on the market, compatibility with the vendor's solution or other systems in use by the FSP can be a serious challenge.

Procurement requirements for front-end devices will also be heavily influenced by the strategy the FSP has decided to take with regards to the ownership of these devices. Where agents will be required to procure their own devices, the responsibility of the FSP will be less, although the issues of compatibility may be more pressing given that the FSP will have less control over which specific device is used. In many cases where this ownership strategy is desired, the FSPs may discover that hardware/devices still need to be provided to agents to conduct the pilot or beta testing. This will not only provide an opportunity to test the solution working on different models but will also give these users the opportunity to appreciate the potential benefits that the system can bring to them, hence convincing them of the need to invest in the device. For staff users, it is typically the FSP that provides the required devices, although some have created incentive schemes or staff loans for the device to be owned by the employee as a means of encouraging users to take care of the devices. For agents, both models are observed and the decision will really depend on the types of agents that are available in the market, their willingness to either invest some funds as a precondition to becoming an agent, or their existing access to phones/tablets/laptops prior to signing up as an agent with the FSP.

For the back office and for ADC systems that will be installed in-house, the implementation team will need to identify or procure servers to host the system. While many FSPs may have requested these hardware specifications during the RFP process, these may be confirmed at this stage as it is only at this point that the vendor will have a very clear sense of how the FSP intends to use its system, and hence can provide accurate sizing requirements. In the preparation of these specifications and associated procurement needs, the implementation team needs to consider not only the hardware needed for production environments, but also for backup/disaster recovery as well as training. Typically most mid to large FSPs will require all systems to be available in triplicate: one for production, one for backup/disaster recovery and another for UAT or training. Lastly, procurement of servers needs to take into account the estimated transaction volumes expected over this channel. Ideally this information will be available from the channel strategy and associated business case, but may need to be revised based on the final decisions taken regarding configuration/customization.

ATM and other channels reliant on the use of cards will require some specific hardware ranging from the front-end ATM itself to the HSM and card printers in case cards are being produced in-house. For all of these systems, the FSP will need to research the available vendors and with inputs from the vendor, confirm on which to procure. Disaster recovery or replacement systems need also to be considered to ensure that the channel remains reliable and available for the end-users.

STEP 11: *Configure and confirm the system*

Based on the output of the requirements analysis phase, the vendor may need to configure or potentially customize the ADC system to meet the agreed specification. For the FSP, this phase may not require active involvement, although constant communication needs to be maintained between the implementation team and the vendor to ensure that progress is being made as expected and to handle any arising issues. By the end of this phase, the vendor should be ready with a version of its software that is fully configured to meet the FSP's requirements, with all configurations and customizations tested by the vendor's quality assurance team.

Where the channel requires integrations with third parties, this step will help to accomplish this task, which typically requires direct communication between the ADC solution vendor and the third party. This integration work will require decisions regarding integration protocols, a topic discussed later in this chapter.

The FSP should also prepare UAT test cases at this stage. Test cases need to be as detailed as possible to avoid missing out on bugs or issues. For example, a test case to check that a customer withdrawal is functioning properly would outline the expected debits and credits, any fees or commissions to be calculated and posted, and any reports to be generated.

Data migration (if applicable)

Projects that involve replacement of an existing system will also need to consider how data will be migrated from the legacy system during the requirements phase. The implementation team and vendor should agree on the data to be transferred, and cut-off dates. During this analysis, it is not uncommon for some FSPs to encounter issues with compatibility, particularly of authentication data such as biometric records or PINs. This data is normally stored as encrypted data, which may complicate the extent to which the new vendor can access and migrate it to its systems. Difficult decisions may need to be taken regarding resetting of PINs or re-registering of biometric data.

Installation

For ADC systems that will be installed on the FSP's infrastructure, the installation of systems need to be done after the vendor confirms that the version is fully configured or customized and has passed through a quality assurance testing and the FSP has procured the required devices, if applicable. This installation is typically done by the vendor although ideally the FSP's IT resources will be trained on how to do this installation at the same time, so that for future releases the task can be done in-house with less dependency on the vendor.

User acceptance testing

Once the vendor has installed the system, the CIG can commence testing the system to confirm it meets the agreed specifications using the test cases prepared. These test cases must include both positive cases (that is, the system behaves as expected when correct criteria is input) and negative cases (the system does not allow operations if incorrect input) to ensure that the system is fully compliant with the FSPs requirements. Prior to this UAT, some training is typically required, so that those involved in the testing are equipped with the skills to adequately test the system. Additionally, some FSPs may choose to have a smaller team prequalify the system before bringing on-board a larger UAT team. This can help make the testing more efficient and really focus on pulling in end-user feedback rather than have the UAT team interrupted by critical bugs which may prevent it from completing its task. It is important to realize that this step will be the first presentation of a working system to a group of end-users, and the way in which this introduction is managed will influence the buy-in and uptake of the system. Prolonged UAT which is constantly interrupted by bugs and change requests will deflate the UAT team and sow seeds of doubt in team members' minds about the ability of the system to deliver, which will likely propagate throughout the business.

UAT is a notoriously difficult exercise for both FSP and vendors to navigate. Inevitably, changes or omissions from the specification stage will arise once the system is in front of the users and the team can finally visualize and interact with it directly. Assumptions of what the system is expected to do, and possibly cannot do, may arise

12 STEP 12: *Pilot and go live*

and lead to disappointment within the implementation team and between the vendor and FSP. Having an agreed change control process from the kick-off meeting will help to navigate this process. Additionally, pilot projects with phased delivery can help to schedule issues arising to later phases, ensuring that the project can continue albeit with some compromises in terms of functionality in the early deployment. Lastly, clearly establishing the objectives of the UAT exercise at the outset of this step will help ensure buy-in to the process and provide guidance should issues arise that perhaps could derail the task.

Training

Following UAT, the system is ready to be introduced to the end-users, which could be staff, agents or customers depending on the ADC being implemented. For customers, this training should be presented in an easily accessible format, either through marketing materials that guide them on how to register and use the channel or online tutorials for channels based on the Web. Field demonstrations by staff or temporary sales teams are very effective. Irrespective of how it is delivered, users will need not only initial training but ongoing support for use of the channel, and this need has to be catered for ideally through a dedicated help desk function as well as a customer support service if the end-user is a customer or third party agent network.

Whether piloting or going for a replacement system with full-scale rollout from day one, the "go live" process must be carefully managed. A series of tasks needs to take place in a coordinated fashion to move the final UAT version to the production environment, which may involve third parties doing similar migrations at the same time. Once this migration has been done, a final check should be performed to ensure the systems are still working as expected and that nothing has been lost from the migration process. Where applicable, existing systems will be switched off and services migrated to the new platform. This may require some outage time for the channel, which should be communicated to users in advance. Depending on the decisions taken regarding migration, customers may be required to reset their PIN or re-enroll for the channel, all of which has to be communicated and coordinated during this phase.

'Go live' typically requires all hands on deck, both from the FSP and the vendor. Initial usage of the system needs to be carefully managed to ensure that nothing has been overlooked in the testing and that if any critical issues arise, they are dealt with promptly to avoid end-users reaching conclusions that the channel is unreliable.

A "go live" approach based on an initial pilot can provide many valuable lessons for a FSP, particularly those launching a new channel. These are typically designed to operate with a restricted closed group of users, perhaps staff only, to gain confidence in the systems before introducing them to the wider public. Deploying the systems in this manner will also give the opportunity to test the systems fully before expanding them to the mass market, and will provide time for in-house support teams to ensure that they are fully equipped to support the end-users of the ADC. The duration and success criteria for the pilot should be pre-defined with the vendor and project team so that all are clear on how it will be measured and what will be required to migrate to a fully live environment.

Maintenance and review

The end of the implementation journey is the beginning of a new journey to support, maintain and enhance the system over time. Transitioning from project implementation mode to ongoing support must be managed carefully to ensure that end-users, whether customers, agents or staff, receive prompt feedback to channel-related issues. Additionally, ADC systems very often need some adjustments in the early days to cater for feedback or enhancements identified by the users. Clearly if the "go live" was just on a pilot basis, these enhancements can be pulled into subsequent phases of the project or at the time of full commercial rollout.

Projects don't end with "go live" but rather transition to a new phase that will require daily operational monitoring and support. This phase often sees the vendor migrate the project from an implementation phase to a support contract, whereby a dedicated helpdesk team is available to respond to the FSP's issues. At this point the implementation team conducts a post-implementation review to derive lessons learned, assess the work that is still outstanding and to evaluate the project against agreed objectives. It is important that all parties are open in this review and work towards mitigating project challenges and risks in the future. A support team should assume the responsibility of actively monitoring the system to ensure that the system is operating effectively from a technical standpoint. A set of reports and metrics can be used to support this role. Most institutions also have a business team in place to monitor the operational and commercial performance of the channel and measure the performance of the channel against a set of pre-defined metrics or strategic goals, which should refer back to the ADC strategy discussed in Chapter 2. These teams should report back to the implementation team or project sponsor with results of their analysis and any recommendations for improvements or enhancements based on their observations.

Implementation tips

Implementation of new or replacement IT systems is a notoriously difficult process and unfortunately ADC systems are no different in that respect. Fortunately many lessons have been learned about how to manage the risk associated with these projects. While the next chapter of the handbook presents the wider ADC lessons learned, here we discuss some of the implementation-specific lessons that a FSP may wish to bear in mind as it embarks on these projects:

1. Take time to be trained on the software you have purchased to understand how it works and what features are/aren't there. While many are keen to see the system live in the shortest period of time, investing a decent amount of time in these preparatory stages will not only help safeguard against a failed implementation, but can make subsequent steps in the process more efficient.
2. Hold workshops and meetings internally to gain consensus on aspects of the implementation process. Project teams must have representatives from operations, credit, finance, and audit, as well as IT, to ensure all angles of the business are considered during implementation.
3. Where possible, try to phase the deployments to allow staff time to adjust to new processes, and also to give customers and other end-users time to react to the changes and to incorporate their feedback into subsequent phases.
4. Be sure to define fully the business processes surrounding the new technology prior to taking decisions on configurations and/or customizations.
5. Do not underestimate the time required to integrate with third parties and be sure to consider the impact of the CBS and any planned projects for that system before you start integration
6. As with all projects, UAT is critical and conducting this phase diligently will help protect the FSP from systems not behaving as they need to on initial launch, which can be damaging in terms of reputation and uptake of the channel.
7. ADCs will in almost all cases require setup of a help desk or support line for customers to contact in case they have difficulties using the channel. For some channels, this support may need to be available outside of office hours, particularly for card-based channels.

FROM A TECHNOLOGY PERSPECTIVE

During the course of the implementation, and particularly during the requirements specification step, some key decisions need to be made. Table 8 lists some of the bigger decisions to be made during the implementation process of ADCs.

Table 8: Decisions made during the implementation process of ADCs

TECHNOLOGY	KEY IMPLEMENTATION DECISIONS
SMS	• *Which bulk SMS provider to use for both sending SMS and short code (required for pull mesages).* • *Confirm maximum message length for SMS from the bulk SMS provider.* • *If short code needs to be accessible across multiple networks, need to identify which authority can allocate a single number.* • *Where to store customer's phone number: in CBS / mobile banking system or other system.* • *How to register / subscribe customers for the service? Automatically versus on request.* • *Where to configure fees if charging for the service: in CBS of mobile banking solution.* • *SMS message definition – decide what text to send, when to send it and in which languages.* • *How to add / change messages over time.*
ATM	• *Join existing third party ATM network or launch own.* • *Closed user group or integrate to other payment networks: national switch, Visa, MasterCard.* • *Which system to apply the authorization policy and the rules of this policy.* • *Which system to store business logic such as limits and fees.* • *If own network: decide re hardware procurement, device management systems, liquidity management.* • *Configuration of card management – card production, administration, support, authentication management, HSM, card printers.* • *Reconciliation and settlement – policy and systems used to support.* • *Definition of screens and states (and in what languages).* • *Setup of an ATM help desk.* • *If joining other network: how to integrate> What connectivity required and how to test and settle / reconcile.*

INTERNET BANKING

- *How to do customer authentication: one factor, two factor, security tokens, TANs, pictures, passwords.*
- *How to register customers for the service.*
- *What systems to support on-going administration of channel i.e. help desk.*
- *Workflow automation for processes originated via internet – check book requests, loan applications, high value transactions, currency exchange.*

AGENCY

- *Whether to print transaction receipts or use SMS .*
- *How to manage the devices used by remote users: MDM versus other device management system.*
- *How to manage agents including limits, commissions, access rights, liquidity and float accounts.*
- *Whether to support both online and offline processing: offline for non-cash, all cash online.*
- *If offline, what criteria to use to sync data: loan officer, region, other.*
- *KYC implications on remote account opening.*

M-WALLET INTEGRATION

- *How to match incoming payments to the correct customer account i.e. which identifier: phone number, national ID, account number.*
- *What business rules to apply to incoming payments: overpayments, group accounts, split to savings.*
- *Outward payments – how to validate a customer's phone number: one-off registration versus confirmation at time of sending.*
- *How / when to reconcile payments between the systems: automated versus manual, daily.*
- *Receipting payments received via M-wallet: manually versus SMS versus no receipt.*
- *How to handle group loans over this channel: individual versus batch.*

M-BANKING

- *How to register customers for the service.*
- *Where to store customer's phone number: CBS or m-banking system.*
- *How to support PIN setup and administration.*
- *Where to configure fees if charging for the service.*
- *Process flow per transaction type.*

BIOMETRIC CARD

- *Enrollment process – new and historic customers.*
- *Maker / checker versus one person enrollment.*
- *Accessibility of bio verification across all systems – CBS + channels.*
- *Exception process – what happens if it does not work.*
- *Deduplication process – when to run these checks, process to follow up if duplicate found.*
- *Which fingers to capture.*
- *Which model of reader to use.*
- *Number of allowed attempts to authenticate.*
- *FAR / FFR thresholds**
- *Catering for change to business process: who to capture, cashier processes.*
- *Different types of cards – smart, mag, EMV.*
- *Card administration as the application, processing and on-going management of the card for the customer.*
- *Card production is the physical creation of the card, which is often done by an entity other than the one doing administration.*
- *First decision is who will administer and produce the cards.*
- *Pre-printed versus customized-pros / cons.*
- *PIN management – HSM, PIN mailers.*
- *Card helpdesk support.*

** Using biometrics in any business requires an appreciation of the performance metrics by which the systems are measured, particularly the False Acceptance Rate and False Rejection Rate. FAR, also known as False Matching Rate, is the rate at which the system incorrectly accepts the wrong person at the point of verification. By contrast, FRR is the rate at which the right person is wrongly rejected by the system due to a failure to match their authentication details with the stored record. FAR and FRR rates have an inverse relationship with one another. In other words, the more selective the biometric system is (a better FAR rate), the more likely it is that the system will also begin to occasionally reject the correct fingerprint. Biometrics systems will need to be configurable to decide the best setting to use to balance these two rates, which is both a function of the size of the database as well as some individual system factors that a vendor will need to advise on.*

x x x x

PIN

- *Registration.*
- *Who / where to reset PINS.*

Integration

Given that most ADC solutions require integration of different systems and that this integration can often pose problems during implementation, we wanted to focus on the topic in more detail. We introduced the types of integration in Chapter 3 as either batch or real time, but now want to dive into more detail of the real time integration options, explaining at a high level the protocols that exist, how each of them works and their pros and cons. Table 9 provides an overview of how systems integration can be achieved either via bespoke protocols specifically designed to exchange certain types of data, such as ISO8583, or through more generic formats which we roughly class as APIs.

Table 9: Systems integration protocols

FORMAT / PROTOCOLS	EXAMPLE	ADVANTAGES	DISADVANTAGES
File transfer (local or FTP)	*Various file format batch or semi-real time.*	• *Typically easy to organize and to maintain.* • *Low cost.*	• *Errors on upload typically requires follow up manually resolution.* • *Dependent on the file structure work.* • *Typically lower security as the files can be compromised as they are waiting for processing.*
Low level TCP	*Such as ISO 8583, SMPP, SMTP, ATM management protocols (NDC, AANDC, DDC), HSM protocols.*	• *Immediate notification in case of errors.* • *Fastest network integration protocol.*	• *The standards are implemented in various ways by the vendors.* • *The communication is not human readable which makes it difficult to trace problems.* • *Dependent on constant network availability.*
Database	*Usually stored procedures.*	• *Immediate notification in case of errors.* • *No requirements for additional middleware / system.*	• *Requires access and deep understanding of the database.* • *Lower security due to the access to the database.* • *Dependent on the database type / dialect.*
HTTP-web services	*Such as REST, JSON, XML, SOAP.*	• *Immediate notification in case of errors.* • *Not dependent on the programming language.*	• *Not suitable for big data processing (relatively slow).* • *Dependent on constant network availability.* • *It is adding processing overhead.*
Other API's	*Usually integration with vendor libraries (DLL, operating system API).*	• *Immediate notification in case of errors.* • *As it is provided by the vendor it should be the best and most robust way to integrate with the system.*	• *Usually propriety.* • *Requires vendors to provide detailed documentation.* • *Hard to trace problems as it acts as a 'black box'.* • *Very often it is dependent on the programming language.*

Ultimately the decision of which protocol to use will be a negotiation between the two integrating parties, which could be the FSP and a third party or the ADC solution vendor and the CBS provider. In general, a FSP need not be heavily involved in these technical decisions regarding protocols as long as it is assured that the required information is exchanged at the agreed frequency. In general, often one of the integrating parties will be limited in terms of the types of integration that they can support and hence this factor ends up dictating the integration for the other party.

All ADCs require some type of CBS integration and so FSPs need to be aware of what format or protocol its CBS supports. The market is increasingly seeing CBS containing APIs as a standard which makes for easier integration, although FSPs should be aware of costs associated with the use of these APIs and limitations of the APIs since the mere fact that one exists does not imply that it will support the required functionality. To help gather information about CBS integration, the FSP should ensure it is equipped with the following information before it commences any integration:

1. Determine the types of integrations supported by the system (real-time or batch).
   - If real time, what protocols are supported?
   - Obtain documentation on these APIs.
2. Identify the functionalities supported by the interface either through a review of available documentation or through consultation with the CBS vendor. Check that both financial and non-financial operations are supported if required for the channel.
3. Understand how existing licenses will be affected by use of an API/Interface.

While agreeing protocols is one of the more important steps for integration projects, it is only the first step in actually connecting up systems. Once the protocol is agreed, the business logic governing the interface must also be discussed and may contain topics such as how to handle exceptions or rollbacks, fees and rules associated with the two channels and how reconciliation and/or settlement will be done. For example, for ATMs this business logic must describe how the systems should behave in case a transaction is interrupted without completion. Equipped with this information, which should be supported by a signed document between the parties to lay out the responsibilities and agreements reached, the parties must configure their systems. Once this is completed both parties must work together to test the various messages that will be sent over the interface, to ensure that both systems respond as required during the exchange of information.

Conclusions and lessons learned

This final chapter provides some of the observations or lessons learned with regards to ADC projects so that FSPs benefit from the experiences of others who have travelled ahead of them in this area. These are compiled from the authors' experiences across multiple projects, several continents, and from a range of different types of FSPs. The intention is only to share some insights based on institutional knowledge gained from past ADC projects rather than dictate ADC strategies or projects, and these lessons must be applied carefully to the context of the FSP embarking on ADC projects.

LESSON 1

Use existing networks/ platforms to test out new channels

Where possible, build on existing networks rather than launching your own, especially if this is the first foray into ADCs. This may mean looking for integrations to third-party networks/providers such as ATMs, agents or m-wallets rather than launching these services yourself. Integrations to existing networks are not only cheaper in terms of technology, but also allow you to observe responses from the market to see if the uptake warrants the larger investments required for proprietary solutions. This same lesson could easily be applied to the decision of whether to rent, buy, or build. SaaS models can provide options to test out new channels using partner platforms, which make commercial sense while transaction volumes are low. However, one should be careful of lock-in periods which are sometimes applied with these costing models. Nevertheless, establishing a proprietary network may be justified when customer experience with existing networks is poor, for instance due to poorly trained agents, high prices, or frequent network downtime.

LESSON 2

Challenge your current processes to maximize impact

To get maximum benefit from ADCs, a FSP must be ready to really challenge existing processes or ways of doing business and to include business process reengineering as part of the implementation process. FSPs need the courage to leave old processes behind in order to enhance the customer experience and take full advantage of potential cost and time savings, as well as to optimize operations. This is especially necessary for extension service channels whereby third parties or remote users are now embedded in processes that were either branch or paper-based before and now have the potential to be fully digitized. Change management is critical for such projects so that key users and decision makers are involved in the redesign process and buy into the need to change the status quo. Despite the tendency to blame failed ADC projects on technology, in many cases deeper investigation often reveals the root cause as poor change management, with internal factors preventing the overall success of the project. Addressing this resistance to change, which may exist within the organization at the outset of the project and continually through implementation, will help minimize the risk of project failure due to a lack of buy-in from within the FSP.

LESSON 3

Pick partners carefully

Most ADC projects require some type of partnership between the FSP and other parties, such as m-wallet providers, USSD aggregators, MNOs, or a technology vendor. The success of the ADC may ultimately depend on the strength of these partnerships, making it a worthwhile investment to spend time in the initial selection process and to continually review these arrangements over time. A critical review of four MFS implementations around the world revealed the importance of ensuring that the business model for the channel sustains all parties involved and of ensuring that competitive forces are aligned for the greater good of the partnership. The same study showed that partnerships must be both patient enough to cope with slow growth initially and yet flexible enough to adapt and scale in response to the market over time. Additionally, partners need to consider both direct and indirect value that may arise from the ADC, such as the additional revenues earned by agents who find customers purchasing goods from their shops/kiosks at the time of cash out. Lastly, the role of regulations and the restrictions they impose on partners can undermine a partnership, providing competitive advantage to some partners over others, and hence must be considered in the formulation of any partnership. While it may be challenging to strike successful partnerships in MFS, other ADCs such as outsourced ATM/POS networks provide good examples of how partnerships can be designed to work for all involved. FSPs need to invest time and resources to critically assess compatibility, strategic focus, and commercial alignment to create a win-win partnership.

LESSON 4

Prioritize flexibility and scalability

Although flexibility is important in all IT systems for FSPs, it is perhaps even more critical with respect to ADCs, as in many cases the FSP does not yet know how the market will respond or what will be needed in future. Parameters such as fees, commissions, and types of operations can be altered over time in response to feedback from the market. A foundation infrastructure built around a centralized integration platform or switch can ease the burden of adding new channels or integration partners over time and give the FSP assurance that integrations are done against a common standard. Having catered for this level of flexibility, it is important for the FSP not to adopt new technology too quickly, but rather take the time to see which technologies are proving themselves in the market before incorporating

CASE STUDY

AMK Cambodia

Angkor Mikroheranhvatho Kampuchea is a microfinance institution in Cambodia, operating 30 branches and 109 sub-branches to serve more than 400,000 customers. In 2011, AMK identified a challenge in mobilizing savings in the rural communities due to a lack of convenient access to cash in / cash out services for customers in remote locations. The existing operational model of visiting customers on a weekly basis for scheduled loan repayments did not provide sufficient access to savings customers, who desired a more convenient means to access their savings without having to go to the branch or wait for a loan officer to pay a visit. AMK assessed the market and explored the potential channel options available, concluding that an agent network that provided customers with greater access to their accounts in remote areas would achieve both organizational objectives and meet client demand, and would be cost effective to implement.

Although there was an m-wallet provider offering money transfer and bill payment services via a network of agents in the market at the time, a partnership with this organization was not feasible due to its exclusivity agreement with a multinational bank. After considerable research and analysis, AMK developed a channel strategy to launch an agent network that would offer customers convenient access to savings accounts as well as a money transfer service for both account and non-account-holding customers. The objective was to increase outreach to the unbanked, provide a convenient savings product to the rural clientele, and create a value-added service (money transfer). This new agent banking channel was not only intended to facilitate transactions, but also to enable remote account opening at the local agent, including distribution of 'no name' magstripe cards linked to a PIN for customer authentication.

When selecting a technology platform, AMK was faced with the challenge of a fragmented MNO sector, with 12 major providers in operation. This, combined with the absence of a USSD aggregator, ruled out the possibility of a channel based on USSD, as that would mean setting up separate USSD lines with each of the operators. On a positive note, the large number of providers meant that there was relatively high mobile coverage for both phone and data services available. Given that AMK was launching a proprietary agent network, it had the control to determine which handset would be used by the agent and selected a low-cost Nokia C1 feature phone, which has the capacity to run a J2ME mobile application.

In December 2011, AMK launched its agent banking system with a network of local agents empowered by a secure mobile application and through branch offices via a complementary Web-based portal. As of October 2014, the MMT network consisted of 1,020 agents serving 26,663 AMK customers, transacting an average of 85 deposits and 102 withdrawal transactions a day. Once the MMT system was up and running, AMK continued to monitor the performance of the channel, constantly listening to feedback from the agent network and tweaking the system based on lessons and suggestions for improved client experience.

After three years in operation, the agent network raised the suggestion of upgrading the agent mobile solution to a smartphone. Many agents had their own smartphones and were only using the feature phone for AMK transactions. This change represented an opportunity to upgrade the mobile application to a smart app to offer a better user interface. It was also an opportunity to reduce the upfront cost of setting up an agent with a transition to a 'bring your own device' model for the agent network. While AMK could not have predicted the penetration of smartphones at the time of its technology selection, the flexibility to respond to this request enables AMK to continue expanding the MMT agent network to meet the objectives of the channel strategy.

While maintaining regular operations, AMK has proceeded with the implementation of other delivery channels. In 2013, AMK launched an ATM pilot powered by an EFT switch solution and complementary card management system. AMK now offers its customers a broader range of outlets to transact, using a personal debit card to access an AMK account. AMK has implemented an SMS solution to deliver alerts and notifications to staff responsible for monitoring the ATM network and is expanding the functionality of this application to increase communication with customers via SMS. Today, AMK is considered an innovator in delivery channels for microfinance and has plans to continue enhancing the delivery of appropriate and viable microfinance services to improve the livelihoods of customers.

these in its ADC solution. A balance needs to be struck between staying in touch with the market demands of the customers and ensuring a stable and reliable transactional platform on which to extend services.

LESSON 5 Consider the context carefully

FSPs should remember that there is no 'one size fits all' in terms of channels. FSPs need to consider both the external and internal environments, as discussed in Chapter 2, and care must be taken to not presume that what was successful in one place will necessarily be successful in another place.

LESSON 6 An ever-evolving strategy

As with all strategies, periodic reviews are recommended to assess how the institution has performed against its goals and whether the strategy needs to be adjusted based on technology trends, changes in customer expectations, and other relevant feedback from the market and operational results. A change strategy should evolve with the clients' needs and expectations, the business and the external market in which it is operating. This does not mean reinventing the channel strategy on an annual basis, but rather making adjustments and enhancements to existing ADCs to align with new conditions. These reviews should be supported by pre-defined performance metrics or KPIs, which measure use, user satisfaction, volumes, down-time, and other relevant statistics which can be extracted via tools and reports that monitor channel operations over a period of time to compare trends and benchmark with other market data. Depending on the results of these reviews, FSPs may need to go back to the drawing board periodically to adapt to changes in technology, demand, and competition. The technology that makes up the ADCs should be dynamic and flexible enough to support this evolving channel strategy.

There is no 'one size fits all' in terms of channels.

Checklists

To help consolidate the information provided throughout the handbook, checklists have been prepared for each of the phases of the project. These are designed to be practical tips on what decisions or tasks need to be conducted at each phase and step of the project.

Chapter 2 Channel strategy

These guiding questions can help draw some conclusions as you navigate through the ADC strategy formulation process. Some are more general and others are relevant only as FSPs investigate the potential to use specific channels.

Step 1: Define the business objectives

1. Confirm the vision, mission and business strategy of the FSP.
2. What is motivating the consideration to implement a new delivery channel? What are our strategic objectives? What is the market opportunity we want to take advantage of?
   - Improve efficiency (no more batch processing, lower errors, instant processing, single-step data collection, or digital document management).
   - Reduce costs (no more driving around with cash, and no more manual parts).
   - Scale operations (serving people in new areas, particularly remote and rural areas, but also in security-poor urban zones).
   - Extend more convenient and/or more affordable financial services.
   - Reach new customers through agency banking to serve unbanked individuals.
   - Automate business processes and service delivery to gain efficiencies.
   - Leverage existing infrastructure (mobile or retail) to target new markets.
   - Enhance the security of existing systems through user authentication.
3. Who will be part of the channel strategy team?

Step 2: Assess the environments within which the FSP operates

1. External environment
   - *Customers' needs and demands* – Existing and new customers: execute client engagement exercises. What is client feedback communicating? Are customers satisfied with the current quality of service? What value is put on the product/service? Suggestions for improvement? What is the capacity to self-serve? Once you have a channel strategy in mind, come back to the client – does this meet the client's needs? Is this in demand or can demand be created? What benefits are available for the client?
   - *Competition* – Who is the competition? What is currently being offered? How is it being offered? At what price? What are your customers' impressions of the competition?
   - *Regulation* – What regulations exist for channels: mobile, agent banking, KYC,

or signature requirements? What indirect regulation could impact the design of a delivery channel (for example, signature, biometric, or national ID)?

- *ICT landscape* – What communications are available: SMS, USSD, mobile data services, Internet, LAN/WAN, IVR, or NFC? Review the availability, quality, and affordability of the communication options available to the target market. What devices are accessible to the target market? Is there electricity and connectivity in the locations where your target market is based?
- *Strategic partnerships* – Are there existing providers that we could partner with? Are potential partners operationally, technically, and commercially aligned?

2. Internal environment

- *Product and service offering* – What transactions, products, or services are currently offered, or do you have plans to offer in the short to medium term? Should these be self-service or OTC?
- *Current channel strategy* – How are existing channels performing with regards to use and efficiency? How are we performing against our goals with the current channel strategy? What are the opportunities for improvement? What bottlenecks exist in the current operations that would be resolved or reduced by an alternative channel? What adjustments are needed in the operations to make it happen?
- *IT environment and strategy* – Is the CBS stable, centralized, and capable of integration (is an API available)? How will the CBS support the addition of these channels, are upgrades or customizations required, what costs should be considered (for example, if paying per user, will each new agent be considered as a new user)? How does the current IT strategy impact the channel strategy and what internal security policies should be incorporated? How will the customer's identity be authenticated?
- *Capacity* – Financial: what is the budget allocated for this project (inclusive of technology systems, marketing, operations, and support)? Resources: what is the capacity of the IT team and IT infrastructure? Should the ADC technology be bought, built, or rented? What human resources and skills are required to support the project implementation and continue operations?
- *Internal risk and compliance* – What additional risk do ADCs expose the organization to? How can these risks be mitigated, controlled, and monitored? Are there any potential compliance issues which should be considered? To what extent will the business use paper versus digital for the operations supported? Do we still use paper account opening forms, do we need paper receipts for transactions? What do regulations say about going paperless?

Step 3: Define the channel strategy

Define the channel strategy, which must include the following information:

1. The business goals and objectives that the proposed channels are meant to address.
2. A market analysis, including market research, competitor, and regulatory reviews.
3. An analysis of the proposed channels and technology (device, application, and communication) and how they will meet business goals and customer needs.
4. A SWOT analysis of the proposed channels and technology.
5. A recommendation, based on the analysis above, of which ADC solution to pursue.
6. An operational, financial, and IT requirements analysis and a recommendation of whether to 'buy', 'rent', or 'build'.
7. A high-level timeline and project plan, including the roles and responsibilities of key stakeholders or internal teams.
8. A high-level budget, including the source and uses of funds.
9. A risk analysis, including potential impact and mitigation.

The matrix in Table 10 provides channel-specific questions and considerations for each of the channels discussed in Chapter 1. The selected channels will be justified by the channel strategy document, which summarizes the objectives, market analysis, and initial project plan detailing the operational, financial, and IT requirements and a high-level project plan.

Table 10: Channel-specific Considerations

CHANNEL	MODEL	QUESTIONS AND CONSIDERATIONS
ATM	*n/a*	• *Availability and cost of joining existing third-party networks.* • *Number and location (branch-based versus public) of ATMs currently available in market.* • *Interoperability available or desired (that is, proprietary system, open but with closed user group, national or international).* • *Resources to manage proprietary network.* • *Card production and management (Who is available to do this? Should you do in-house or outsourced?).* • *What types of cards (EMV or other) to use.* • *Cash servicing: in-house versus outsourced.*
Internet banking	*n/a*	• *Access to Internet and Internet-enabled devices.* • *The proportion of the market that represents SMEs who typically have a higher demand for online banking from PC rather than mobile (for example, processing bulk payments for salaries).* • *Clients involved in value chain that require online transaction facility.* • *Regulatory position on initiating and securing transactions done over the channel.*
Agent/merchant banking	*n/a*	• *Availability and quality of existing third-party agent networks.* • *Availability of potential agents considering factors such as float/cash, infrastructure, training, and security.* • *Investment required for agent recruitment, branding, training, and support.* • *Liquidity/float management: options available to ensure agents have access to cash/float.* • *Communication infrastructure at potential agent locations.* • *Existing devices available at potential agent sites (that is, PC versus mobile versus POS).* • *Customer acceptance of transacting with third parties.* • *Availability and cost of bulk SMS and short codes.* • *Client literacy levels and handset availability.* • *Market acceptance of SMS as an alternative to a physical receipt.* • *Security level required for this channel: risk of information going to wrong person.* • *Regulatory requirements and impact on services.*
Extension services	*Field staff*	• *Ability to handle cash operations versus non-cash. What functionality available from this point of service?* • *Communication infrastructure: the need for online versus offline.* • *Physical devices available/affordable.* • *Security environment: will users be safe carrying tablets/phones/cash.* • *Printing, signing, and authentication requirements.*
	Mini branch	• *Ability to handle cash operations versus non-cash. What functionality available from this POS?* • *Communication infrastructure: the need for online versus offline.* • *Existing devices available at mini-branch locations.* • *Printing, signing, and authentication requirements.*

	Bank on wheels	• *Number of locations and potential clients that could be serviced (Where would the vehicle go? How often?).* • *Communication infrastructure: the need for online versus offline.* • *Level of security required both in terms of the vehicle and the escorts required for cash security.* • *Existing devices available at mini-branch locations.* • *Printing, signing, and authentication requirements.*
Mobile banking	*n/a*	• *Availability of mobile devices with clients, with percentage of smartphones versus feature phones.* • *Availability of USSD in country: is this service interoperable, what is the cost, what is the quality, and who will provide access?* • *Availability of payment and channel aggregators to have a single point of contact to connect to all MNOs and frequently used billers.* • *Client comfort level with mobile: will they know how to use it?* • *Linkage/dependencies to other channels: withdrawal from m-wallet requires customer-initiated transaction, hence m-banking required.* • *Willingness of clients to pay for the service.* • *Revenue model of m-banking service providers: SaaS, revenue share, on-premise solution.*
E-wallet	*n/a*	• *Availability, quality, and cost of existing m-wallet providers.* • *Services (both client side and FSP side) available from existing m-wallet providers considering P2B, B2P as well as reconciliation.* • *Types of integration supported by m-wallet provider.* • *Quality of existing m-wallet providers' agent network (agent numbers, location, and level of activity).* • *Willingness to partner.* • *Motivations and regulatory requirements to introduce bank-led m-wallet.*
Call center		• *Access to phone services and coverage in the markets.* • *Availability of IVR in local languages of target market.* • *Cost of services by IVR vendor.* • *Client's comfort level with phone banking.*

Step 4: Define the business case

Create a business model with high-level financial scenarios based on initial assumptions related to the operational model, partnerships, a product roadmap, customer adoption and usage projections, and technical platform costs. Business and financial models differ widely by institution, so it is very difficult to recommend a specific template. However, all implementers need to understand the key drivers – often transactions – and their costs and revenue potential. Ultimately, regardless of the model used, the channel strategy document should include a summary table for at least five years, with the following details:

1. **Key indicators:** This section should give an indication of the use and growth of the proposed channel(s) over time.
2. **Pricing:** Identify the payment and pricing models.
3. **Benefits:** Quantify all benefits, including a) the reduction in administration costs; b) the reduction in the cost of funding; and c) the additional revenue from a higher rate of up-selling/cross-selling. Identify the non-monetary benefits, including a) faster loan turn-around time; b) higher customer satisfaction/convenience; c) better quality of evaluations; and d) smooth introduction of product updates.
4. **Costs:** This section provides a snapshot of potential costs for the channel(s) for the FSP to quantify all costs, including information obtained from the external analysis component to reflect actual costs (for example license and transaction fees).
5. **Net revenues:** This section helps assess and compare the net revenues accruing to the FSP *vis-à-vis* its partners and vendors. Net revenues for other partners are based on what the FSP is expected to pay to each of these potential partners for their services.
6. **Analysis:** Evaluate the financial impact in terms of ROI, IRR, and the break-even point.

Test the model to ensure it is generating appropriate outputs.

Consider multiple scenarios based on the profile of the agent: staff, managed network, and third party.

Table 10: Channel Business Case Summary

CHANNEL BUSINESS CASE SUMMARY TABLE	*Year 0*	*Year 1*	*Year 2*	*Year 3*	*Year 4*
KEY INDICATORS					
Core customers/accounts (#)					
Customers/accounts using the channel (#, %)					
Number of access points/outlets/ATMs/agents (#)					
Txn per customer per day/week/month (#)					
Txn per channel per day/week/month (#)					
Average txn volumes per day/week/month (#)					
Average txn values per day/week/month ($, LCU)					
REVENUES ($, LCU)					
Financial revenues – from loans					
Channel revenue – from commissions and fees					
Interest on float					
Other cost savings					
COSTS ($, LCU)					
Financial expenses – cost of funds					
Channel expenses – from commissions and fees					
Interest on float					
CAPEX (investment costs)					
OPEX (operating costs)					
NET REVENUES – ECOSYSTEM					
FSP (Insert name)					
MNO partner (Insert name) if applicable					
Agent/merchant (Insert name) if applicable					
Aggregator (Insert name) if applicable					
Vendor (Insert name) if applicable					
Switch (Insert name) if applicable					
Acquirer (Insert name) if applicable					
Issuer (Insert name) if applicable					
Partner (Insert name)					
Partner (Insert name)					

Chapter 3 Technology platform selection

These guiding questions can help draw some conclusions as you decide which technologies are most appropriate for your channel strategy and operating context.

Step 1: Know what options are available

1. **What applications are available** – For the channel(s) selected, review the options available in terms of software applications. What are the benefits and disadvantages of each option in your specific context? Are any automatically ruled out due to regulatory requirements, socio-economic conditions, or communication limitations?
2. **What devices are available** – For the channel(s) selected, review the options in terms of devices available in the market and/or already with the target users of the channel. What are the benefits and disadvantages of each option in your specific context? Are any automatically ruled out due to regulatory requirements, socio-economic conditions, or communication limitations?
3. **What types of communications are available** – Determine what communication infrastructure is available to support the channel(s). What are the benefits and disadvantages of each option?

Step 2: Understanding the influencing criteria

1. **Types of transactions** – What transactions (financial and non-financial) will be offered over the channel(s)?
2. **Security levels** – What means of security will be implemented to protect both the client and the institution from risks such as fraud and theft of identity, information, and value?
3. **Mode of authentication** – What will we use to identify and confirm the identity of both customer and agent if we do proceed to use ADCs: bio versus card versus PIN? What existing infrastructure can be leveraged to facilitate identification?
4. **Quality / availability / cost of communication channels** – Review the quality, availability, and cost of the communication channels available. Read the fine print. Reach out to partners to improve the quality of service where needed.
5. **Handset availability in the market/ target market** – Research the types of devices available in the market and used by the target users. Base the analysis on cost, security, and durability. Who will provide the device to the user?

Step 3: Select the platform

Decide which *application, device, and communication* are best suited to the channel. Multiple options may exist at each level to fully cater for the market and the range of users that will be targeted.

Chapter 4 Vendor selection

These guiding questions can help draw some conclusions as you navigate through the ADC strategy formulation process. Some are more general and others are relevant only as FSPs investigate the potential to use specific channels.

Step 1: Initiation

- Identify stakeholders from relevant business units and establish roles and responsibilities.
- Engage with stakeholders to establish a communication channel within the group and ensure alignment. Define the selection process, the scope of work, and selection timelines.

Step 2: Identify functional and technical requirements

To assist with the extraction of requirements for the functionality components of ADC solutions, Table 11 lists some of the common areas to consider and questions to ask during this requirements identification process.

Table 11: Questions to assist with general functional requirements

REQUIREMENT	RELEVANT FOR WHICH ADCs?	DESCRIPTION
Registration	*Potentially all*	*1. How will customers be registered to transact over the channel?* *2. For mobile, how will the customer's phone number be confirmed?*
Fees	*Potentially all*	*1. What types of fees should be charged for registration and transactions on the channel?* *2. How are fees calculated and applied?* *3. Where will these fees be configured?*
Settlement and reconciliation	*All*	*1. Which systems will need to be reconciled?* *2. What type of reconciliation is required?* *3. What will be the rules governing settlement?*
Interoperability	*Primarily mobile and ATM*	*1. What level of interoperability will be required from a user's perspective?* *2. What operating systems should be supported for mobile and Web platforms?* *3. If biometrics are to be used, how to ensure compatibility?*
Reporting	*All*	*1. How will the channel activity be monitored?*
Scalability	*All*	*1. What are the expected transaction levels with projections for five years?* *2. What number of users will be accessing the system?*
Flexibility	*All*	*1. What is needed in terms of flexibility?*
Standards	*All*	*1. Does the channel strategy dictate any specific standard that must be adhered to (for example, EMV or ISO)?*
Online/Offline	*Potentially all*	*1. For extension services, what systems, or functions, should be available in offline mode?* *2. What should be the behavior of the ADC when/if the CBS is offline for end of day/ month?*
Integration/ Middleware	*All*	*1. What front-office and back-office systems will need to be integrated?* *2. What type of integration? Batch or real-time?* *3. What functionality must each interface support?*
Security	*All*	*1. What systems are required to support the preferred mode of customer authentication? Are these systems going to be external from CBS or within it?* *2. How will the physical devices used for data entry be secured (agency or extension services)?* *3. How will the communication networks required be secured?* *4. What security measures are expected from the ADC back-office systems?* *5. What support is required to fully audit the ADC and monitor the controls in place (system-based controls, audit reports, and additional systems – AML)?*

REQUIREMENT	RELEVANT FOR WHICH ADCs?	DESCRIPTION
Agent management	*Agent/merchant*	1. *In which system will the agents be defined?* 2. *How and where will limits on agent transactions be defined?* 3. *Will float accounts be used and if so which system will be used to define these accounts and then map them to the agent user?* 4. *What commissions will be due to agents, where to define these and when to pay?* 5. *Is there a hierarchy that needs to be enforced in the agent network?*
ATM/POS management	*ATM (in-house)*	1. *Which system will drive and manage the ATM/POS devices?* 2. *What system will be used for CMS?* 3. *Which Security Module will be used? HSM vs SSM?*

Step 3: Vendor selection

1. Prepare the RFP

- Brief background about the FSP.
- Business and channel strategy (may include a phased approach).
- Overview of project: objectives, scope, and related projects.
- Selection process and deadlines.
- Criteria for decision making, including preferences on different licensing structures (license versus SaaS versus revenue share).
- Expected content and format for the response.
- Functional requirements with weighting to reflect priority.
- Technical requirements (overview of CBS and current infrastructure).
- Project timing.
- Expected services from the vendor.

2. Vendor shortlist

- What criteria are being used for pre-qualification?
- Which vendors are serving or have a presence in this market, most likely working with your competitors or FSP peers?
- Which vendors have a reputation for providing the type of product/services that are required?
- Confirm with the vendors who will be participating and clearly communicate the timeframe for the process so they can plan accordingly.

3. RFP issue

- Decide who to invite to the RFP and whether they should be pre-qualified.
- Issue the RFP with clear instructions to vendors on the information required and the deadlines.
- How will the responses be evaluated? Specify the criteria before the process begins so there is no bias.
- Request an estimated price based on the requirements in the RFP to test financial proposals against the business case.
- Request contract templates to get familiar with payment, service, and support terms.

4. Evaluation

- Calculate the scores based on proposals, references and demonstrations.
- Evaluate the proposals received considering the match to the requirements, the financial costs, and feedback from demos /references.

Step 4: Contracting

1. Review the contracts with due care and pay specific attention to:

- License terms
- Project deliverables
- Milestones
- Payment terms
- Responsibilities on both sides
- Support level agreements after ‘go live’.

2. Negotiate and sign the required contracts with the vendors, considering both initial implementation and ongoing support. It is advised that FSPs allocate sufficient time for contracting. This process typically takes longer than expected and can delay the project start if terms cannot be negotiated in a timely manner. FSPs should consider that not all vendor contracts are identical and contracting multiple technology vendors will require a resource to be responsible for vendor management.

Chapter 5 Implementation

These guiding questions can help draw some conclusions as you navigate through the implementation process and plan for ongoing maintenance, support, and evaluation.

Step 1: Project team formation

Identify the full project team which includes:

- *Project managers* – Each implementation project that uses an external solution should have a minimum of two project managers, one for the FSP and one for the vendor. These individuals are responsible for liaising directly on all matters as the primary communication channel and for communicating with their respective teams as needed.
- *Core implementation group / implementation team* – Includes representatives from finance, IT, customer service, marketing, operations, risk, compliance, and audit.
- *Project sponsor* – Heads the steering committee and serves as direct line to the board in most cases.
- *Steering committee* – Provides support, guidance, and oversight of project progress. Members do not usually work on the project themselves. Responsibilities include:
    - » Providing input to the development of the project, including the evaluation strategy
    - » Providing advice on the budget
    - » Defining and helping to achieve the project outcomes
    - » Identifying the priorities in the project – where the most energy should be directed
    - » Identifying potential risks
    - » Monitoring risks
    - » Monitoring timelines
    - » Monitoring the quality of the project as it develops
    - » Providing advice (and sometimes making decisions) about changes to the project as it develops.

Step 2: Project kick-off

Project kick-off establishes the foundation for effective business requirements gathering by aligning expectations and engaging the people who have knowledge of the business needs and can determine the requirements. Recommended steps are:

- Introduce team members and assign responsibilities to create accountability.
- Agree on a high-level strategy for the solution.
- Agree on an implementation process and a high-level project plan.
- Establish relevant processes, such as project governance, change management, and escalation.

Step 3: Requirement analysis

This step is best completed with the vendor on site, as it is an opportunity to show the vendor the FSP operations in detail. Activities to include are:

- An overview of the products for the core team to begin learning the system.
- Confirmation on parameterization of the system.
- Identification of new system processes.
- Identification of any required customizations.

In order to analyze the requirements, a concerted effort should be made to gather all of the relevant requirements. We suggest the following methods and categories to be included in the process:

- Methods used for gathering requirements
    - » Brainstorming
    - » Focus group
    - » Business process reengineering exercises
    - » Obtain and analyze relevant documentation
    - » Interviews
    - » Active observation
    - » Prototyping
    - » Requirements workshop
    - » Use cases – maps user interaction.
- Requirements categories
    - » Institutional information
    - » Client information
    - » Credit management
    - » Deposit management
    - » Accounting process.

The output of this process is a Functional Specification Document, which outlines the following:

- Executive summary
- Document purpose
- Definition of key terms
- Information sources
- Solution overview
- Solution components

- Assumptions and dependencies, risks, and controls
- System users/players
- General navigation
- Core processes and workflows supported
- Configuration settings
- Customizations required
- Reports description
- Implementation considerations

Integration requirements

- Which systems need to be integrated? Which parties will actually be involved in the channel? (Third-party entities: bulk SMS providers, m-wallet systems, payment aggregators, and national or international interchanges.)
  - » What type of integration(s)?
  - » What protocol/format to use for real-time integration?
  - » How will settlement and/or reconciliation be done (automated or manual)?

Step 4: Hardware procurement

This depends on the ADC technology being implemented and includes:

Front-end considerations

- Who is furnishing the devices?
  - » FSP
  - » Third party
  - » Client
- Compatibility
  - » Testing hardware with software
  - » Testing with peripherals

Back-end considerations

- » What servers are required to host the system?
- » Preparation of all environments: production, testing, and disaster recovery
- » Additional channel-specific hardware (for example, HSM and card printer)?

Step 5: Configuration / customization

While the system is under configuration/customization, the FSP will need to do the following:

- Request regular status updates to monitor progress.
- Provide prompt responses to inquiries from the vendor to avoid delaying configuration or development.
- Participate in communications between vendors, partners, and third parties.
- Prepare UAT test cases to verify the exact functionality and expectations of the system according to the functional requirements documentation and agree to a test plan with the vendor.

Step 5b: Data migration (if required)

For those systems that require migration, the following tasks need to be completed:

- Decide on a data migration strategy – how data will be extracted, loaded, and reconciled between the source system and the new ADC platform.
- Perform a minimum of two sample data migrations to confirm all migration scripts are working as required.

Step 6: Installation

- Request confirmation that the solution has passed quality assurance testing before the system is installed.
- Include IT in the installation process to gain familiarity with the system.
- Install the system on all required environments.

Step 7: User acceptance testing

- Focus on completing all test cases (regardless of the success rate) so that the vendor is aware of all issues or bugs in the first round of testing.
- Provide details of how you discovered any issues and ensure that this can be recreated for investigation.
- Compile a list of all change requests and enhancements to be completed as a separate project once this release is delivered as expected.

Step 8: Training

- Who will attend the training? How will this training be delivered/communicated to the end-users?
- Consider using a 'training of trainers' approach.
- Train a helpdesk for users – internal and external.

Step 9: Go live

- Consider a pilot to test the channel and technology with live data to receive feedback from clients/end-users.

- Consider how the customer experience will change and prepare to engage with clients and be attentive and responsive to questions and learning to encourage uptake – first impressions have a lasting effect.
- Gain confidence in the systems before introducing it to the wider public.

Step 10: Maintain and enhance

- Distribute relevant documentation, user manuals, and administrative manuals.
- Offer continuous training and support to ensure adoption and use.
- Allocate resources for adjustments and additional support in the early days to cater for feedback or enhancements identified by the users.
- Create system support and a maintenance plan with a monitoring schedule and criteria to ensure that the system is operating effectively.
- Understand the helpdesk protocols and vendor support availability.
- Conduct a post-implementation review to see what lessons were learnt and what work is still outstanding, and start the assessment of whether the project has met its goals.
- Schedule regular maintenance of hardware and software items to ensure optimal performance.
- Establish reports and metrics to measure the performance of the channel against a set of predefined metrics or strategic goals to track the performance of the channel.
- Identify opportunities for improvement based on client feedback.

Glossary

TERM	DEFINITION
3rd Generation Mobile Network (3G)	*Third generation of mobile telephony (cellular) technology. 3G telecommunication networks support services that provide an information transfer rate of at least 200 kbit/s and a maximum of 3.1Mbps.*
4th Generation Mobile Network (4G)	*Fourth generation of mobile telephony technology, succeeding 3G and preceding 5G. As opposed to earlier generations, a 4G system does not support traditional circuit-switched telephony service, but all-Internet Protocol-based communication such as IP telephony, and provides higher download speeds relative to 3G.*
Agent	*A person or business contracted to process transactions for users. The most important of these are cash in and cash out (that is, loading value into the mobile money system, and then converting it back out again); in many instances, agents register new customers too. Agents usually earn commissions for performing these services. They also often provide front-line customer service, such as teaching new users how to complete transactions on their phone. Typically, agents will conduct other kinds of business in addition to mobile money. Agents will sometimes be limited by regulation, but small-scale traders, microfinance institutions, chain stores, and bank branches serve as agents in some markets. Some industry participants prefer the terms 'merchant' or 'retailer' to avoid certain legal connotations of the term 'agent' as it is used in other industries. (GSMA, 2014).*
Agent banking	*Banking services, often limited, carried out by an agent.*
Aggregator	*Servicer provider with existing integrations to a number of MNOs and/or PSPs to facilitate billing, technical, and operational relationships and interfacing across operators via one link to the aggregator, as opposed to separate integrations with each provider.*
Alternative Delivery Channels (ADCs)	*Channels that expand the reach of financial services beyond the traditional branch. These include ATMs, Internet banking, mobile banking, e-wallets and extension services.*
Android	*A Linux-based mobile operating system originally developed by Android and currently developed by Google. With a user interface based on direct manipulation, Android is designed primarily for touchscreen mobile devices such as smartphones and tablet computers.*
Anti-Money Laundering/ Combating the Financing of Terrorism (AML/CFT)	*AML/CFT are legal controls applied to the financial sector to help prevent, detect, and report money-laundering activities.*
Application Programming Interfaces (API)	*A method of specifying a software component in terms of its operations by underlining a set of functionalities that are independent of their respective implementation. APIs are used for real-time integration to the CBS/MIS, which specify how two different systems can communicate with each other through the exchange of 'messages'. Several different types of APIs exist, including those based on the Web, TCP communication, and direct integration to a database, or proprietary APIs written for specific systems.*

Automated Teller Machine (ATM)	*An electronic telecommunications device that enables the customers of a financial institution to perform financial transactions without the need for a human cashier, clerk, or bank teller. ATMs identify customers via either a magnetic or chip-based card, with authentication occurring after the customer inputs a PIN number. Most ATMs are connected to interbank networks to enable customers to access machines that do not directly belong to their bank, although some closed-loop systems also exist. ATMs are connected to a host or ATM controller using a modem, leased line or ADSL.*
Basic phone	*The most basic type of mobile handset available on the market. This phone has no data or GPRS capabilities and for MFS is only compatible with USSD and STK applications.*
Branchless banking	*The delivery of financial services outside of conventional bank branches through the use of retail agents and ICT. For the purpose of this handbook we have considered this term to be equal to ADC and e-banking.*
Call center	*A centralized office used for the purpose of receiving or transmitting a large volume of requests by telephone. In this context, as well as handling customer complaints and queries, it is also used as an alternative delivery channel to improve outreach and attract new customers via various promotional campaigns.*
Card Management System (CMS)	*The system used by businesses to manage the full administration and support associated with payment cards. A CMS will typically provide functionality to manage card product definition, application processes, production, and issuing, blocking, and managing transactions along with the card balances, if required. A CMS will be required for any FSP that wants to use either POS or ATMs with cards as the means of customer authentication.*
Channel	*The customer's access point to a FSP, namely who or what the customer interacts with to access a financial service or product.*
Core Banking System (CBS)	*The core system used by a FSP to manage all of its key business processes, including front- and back-office components. Most CBSs provide CRM functionality, loan portfolio tracking, accounting, and reporting. For the purpose of this handbook we have used the term synonymously with Management Information System.*
Core Implementation Group (CIG)	*A group of staff from the FSP charged with making the day-to-day decisions regarding the ADC project implementation. This group will be involved in training, requirements analysis, and testing of the systems and typically form a group of 'super users' or champions of the system.*
Electronic banking (e-banking)	*The provision of banking products and services through electronic delivery channels.*
Enabling technology	*For the purpose of this handbook we refer to the enabling technology as the underlying technology platform used to drive an ADC. It includes the hardware devices, software systems, and the technological processes that enable the provision of financial products and services over ADCs.*
Europay, MasterCard, and Visa (EMV)	*EMV stands for Europay, MasterCard, and Visa, a global standard for the inter-operation of integrated circuit cards (IC cards or 'chip cards') and IC card-capable POS terminals and ATMs, for authenticating credit and debit card transactions (Wikipedia, 2014).*
E-wallets/e-money	*Short for 'electronic money', it is stored value held in virtual wallets or cards. Typically, the total value of e-money is mirrored in bank account(s), so that even if the provider of the e-wallet service were to fail, users could recover 100 percent of the value stored in their accounts. Bank deposits can earn interest, while e-money cannot.*

Extensible Markup Language (XML)	*A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. The design goals of XML emphasize simplicity, generality, and usability over the Internet. It is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in Web services.*
Extension services	*Field-based banking services often performed by FSP staff. This includes remote data capture, mini branches and branch on wheels.*
Feature phone	*A mobile handset that is more advanced than a basic handset by the fact that it contains embedded data transfer/ GPS capabilities. A feature phone can be used to connect to the Internet or to run mobile applications dependent on data connectivity. Unlike smartphones, feature phones have no in built security and limited peripherals and applications.*
Financial Service Providers (FSP)	*A provider of financial services including credit unions, banks, non-banking financial institutions, microfinance institutions, and mobile financial services providers.*
General Packet Radio Service (GPRS)	*A packet-data technology that allows GSM operators to launch wireless data services, such as e-mail and Internet access, via a SIM card. This is a 2G grade of wireless communication with maximum download speeds of 114kbps.*
Global Positioning System (GPS)	*A space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.*
Global System for Mobile Communications (GSM)	*An open, digital cellular technology used for transmitting mobile voice and data services. It is the most common standard for mobile communication, with over 90 percent market share.*
Hardware Security Module (HSM)	*A physical device used as part of the payment card issuing and authentication process. The HSM is connected to the network hosting an ATM or POS, with the primary functionality of generating PIN numbers and in some cases storing encryption keys required to authenticate the PIN number provided.*
Hypertext Transfer Protocol (HTTP)	*An application protocol for distributed, collaborative, hypermedia information systems – it is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text.*
Interactive Voice Response (IVR)	*A technology that allows a computer to interact with humans through the use of voice and DTMF tones input via keypad. IVR allows customers to interact with a company's host system via a telephone keypad or by speech recognition.*
International Mobile Equipment Identity (IMEI)	*A unique 15-digit serial number, assigned to every single mobile phone. It can normally be found on the back of the phone, under the battery. IMEI consists of four groups of numbers. The first group identifies the type approval code, the second the manufacturer, the third the serial number, and the fourth group is a single digit (usually a zero).*
Internet banking	*An electronic payment system that enables customers to conduct financial transactions on a secure website operated by a FSP.*
iOS	*The operating system used with devices manufactured by Apple.*
J2ME app	*J2ME is a Java programing platform designed for building applications to run on mobile devices. It is commonly used to build mobile apps that need to run on devices with limited memory, display, and power capacity, such as feature phones.*

JavaScript Object Notation (JSON)	*An open standard format that uses human-readable text to transmit data objects consisting of attribute–value pairs. It is used primarily to transmit data between a server and Web application, as an alternative to XML.*
Kiosk	*A computer terminal featuring specialized hardware and software that provides access to information and applications for communication, commerce, entertainment, and education. Integration of technology allows kiosks to perform a wide range of functions, evolving into self-service kiosks.*
Know your customer (KYC)	*Rules related to AML/CFT that compel providers to carry out procedures to identify a customer and that assess the value of the information for detecting, monitoring, and reporting suspicious activities.*
Local Area Network/ Wide Area Network (LAN/WAN)	*LAN is a computer network covering a small geographic area, like a home, office, school, or group of buildings. WAN is a computer network that covers a broad area (for example, any network whose communications links across metropolitan, regional, or national boundaries over a long distance).*
Magstripe/ magnetic strip card	*A type of plastic card which stores data about the customer on a machine-readable magnetic strip on the back of the card. Magstripe cards have been used with ATMs and POS devices, although they are slowly being replaced by EMV/ chip and pin cards.*
Merchant	*A person or business that provides goods or services to a customer in exchange for payment.*
Microfinance Institution (MFI)	*A financial institution specializing in banking services for low-income groups, small-scale businesses, or individuals.*
Mobile banking	*The use of a mobile phone to access banking services and execute financial transactions. This covers both transactional and non-transactional services, such as viewing financial information on a bank customer's mobile phone. Sometimes called 'm-banking'.*
Mobile Financial Services (MFS)	*A general term referring to the use of mobile technologies to access financial services. This includes mobile banking and mobile money / m-wallets.*
Mobile Money	*A service in which the mobile phone is used to access financial services (GSMA, 2014).*
Mobile Network Operator (MNO)	*A company that has a government-issued license to provide telecommunications services through mobile devices.*
Mobile Point of Sale (mPOS)	*A mobile application designed to mimic the same functionality offered by a traditional physical POS device. mPOS applications typically interact with a card reader and/or printer to replicate the full functionality of the traditional POS device.*
Mobile wallet (m-wallet)	*An e-money account that is primarily accessed using a mobile phone that is held with the e-money issuer. It is typically linked to a unique mobile phone number.*
Native apps	*Mobile applications that are manually installed on the phone and run in almost the same way as a computer program installed on a PC. Native apps can be categorized by the operating systems running on the mobile phone, with the most common being Google (Android) and Apple (iOS), and Windows for smartphones and Java/J2ME apps for feature phones. Native applications can be developed to serve as a user interface for a variety of business uses, including mPOS, agent apps or field-based data capture apps. Native apps can operate in either online or offline mode, depending on the design of the application and the quality of the communications available.*
Near Field Communication (NFC)	*A method of contactless card payment (without a PIN), which uses short-range radio signals to exchange information between a card or mobile device and a terminal.*

Offline	*Offline means not connected to the Internet or network connection. Some programs or applications are configured to operate offline or have the option to work offline when the connection is lost so that data entry is not interrupted, meaning the software continues to function on the device and stores data locally. However, no data can be transmitted to or from the device on which it is operating until a connection is established. Offline data can be synchronized with an online or central database when connectivity is re-established or the device is tethered to transfer data.*
One Time Passwords (OTP)	*A security protocol that works on the basis of one factor of authentication being generated only when needed, namely at log in or transaction posting, and acts as a single use password or PIN.*
Over The Counter (OTC)	*Channels that require the customer to interact with a member of the FSP staff or a third-party representative to transact.*
Point of Sale (POS) device/terminal	*Electronic device used to process card payments at the point at which a customer makes a payment to the merchant in exchange for goods and services. The POS device is a hardware (fixed or mobile) device that runs software to facilitate the transaction. The hardware used may vary.*
Premium Rate Service Provider (PRSP)	*An intermediary provider, licensed by the MNOs and usually the government, to offer bulk SMS, USSD, and short code services. The regulation governing these businesses will vary from country to country, with some places allowing for only a direct relationship with the MNOs for these services. Where regulations for PRSP exist, a FSP will need to contract with these parties in order to access bulk SMS and/or USSD channels, although these services will still require a tripartite agreement between the FSP, MNO, and PRSP. For this handbook we have considered a PRSP as the same as an Aggregator.*
Request for Proposal (RFP)	*A solicitation made by a company to initiate a bidding process to procure a commodity, service, or valuable asset from potential vendors who are requested to submit business proposals. The RFP should provide all the information and requirements that a FSP has identified as necessary or desirable to assist vendors to prepare a suitable proposal for their services and products.*
Self Service Channel	*A channel that is available to customers without any other human interaction.*
Short Code	*Short codes (also known as short numbers) are special telephone numbers, significantly shorter than full telephone numbers, that can be used either to initiate a USSD session or to request a pull SMS. Short Codes are issued either by the communications authority, MNO or, where applicable, the PRSP.*
Short Message Peer-to-Peer (SMPP)	*An open telecommunications industry standard protocol designed to provide a flexible data communication interface for the transfer of short message data. It is used to process bulk SMS messaging.*
Short Message Service (SMS)	*A 'store and forward' communication channel that involves the use of the telecom network and SMPP protocol to send a limited amount of text from one phone to another, or one to many.*
SIM Application Toolkit (STK)	*A standard of the GSM system which enables the Subscriber Identity Module, or SIM, to initiate actions which can be used for various value-added services.*
Smart app	*An application software designed to run on smartphones, tablet computers and other mobile devices.*
Smart card	*A smart card, chip card, or integrated circuit card is any pocket-sized card with embedded integrated circuits. Smart cards can provide identification, authentication, data storage, and application processing via an embedded microchip.*

Smartphone	*A mobile phone that has the processing capacity to perform many of the functions of a computer, typically having a relatively large screen and an operating system capable of running a complex set of applications, with Internet access. In addition to digital voice service, modern smartphones provide text messaging, e-mail, Web browsing, still and video cameras, an MP3 player, and video playback with embedded data transfer/GPS capabilities.*
Software as a Service (SaaS)	*SaaS is s software licensing delivery model in which software is licensed on a subscription basis and made accessible via the Internet as a hosted service, instead of installing and maintaining software.*
Transaction Authentication Numbers (TAN)	*A security protocol that works on the basis of one factor of authentication being generated only when needed, namely at log in or transaction posting, and acts as a single-use password or PIN. The term is interchangeable with One Time Passwords.*
Unstructured Supplementary Service Data (USSD)	*A protocol used by GSM mobile devices to communicate with the service provider's computers/network. This channel is supported by all GSM handsets, enabling an interactive session consisting of a two-way exchange of messages based on a defined application menu.*
User Acceptance Testing (UAT)	*The testing process that occurs at the end of a software development process whereby the actual software users test the software to make sure it can handle the required tasks in real-world scenarios, according to specifications. In this context, the ADC system would be tested to confirm it meets the agreed specifications and requirements of the FSP.*
Virtual Private Network (VPN)	*A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network.*
Web API	*A set of HTTP request messages that have defined structured response messages. These messages can be written in various languages such as XML or JSON format.*
Web app	*A software application that is created in a browser-supported programming language (such as the combination of JavaScript, HTML, and CSS) and runs in a Web browser relying on the browser to render the application. Web apps function very much as a standard Internet website using a URL, but the size and features are designed to display and interact better on a mobile device than on a traditional website.*
Wi-Fi	*Local area wireless technology that allows an electronic device to exchange data or connect to the Internet using radio waves.*

Reference documents

Basel Committee on Banking Supervision (July 2003). Risk Management Principles for Electronic Banking. *Bank for International Settlements Communications, Basel, Switzerland.* www.bis.org/publ/bcbs98.pdf

Global Technology Audit Guide 'GTAG', Fraud Prevention and Detection in an Automated World (December 2009) and Information Technology Controls (March 2005). The Institute of Internal Auditors Inc. (IIA), 247 Maitland Ave., Altamonte Springs, FL 32701-4201, United States of America. *www.theiia.org/*

CGAP Focus Note No 75. Bank Agent: Risk Management, Mitigation, and Supervision (December 2011). Kate Lauer, Denise Dias, and Michael Tarazi. www.cgap.org/publications/bank-agents-risk-management-mitigation-and-supervision

Digital Financial Services Risk Assessment for Microfinance Institutions Pocket Guide (September 2014). The Digital Financial Services Working Group, Washington, D.C., United States of America. https://lextonblog.files.wordpress.com /2014/09/dfs_risk_guide_sept_2014_final.pdf

Flaming, M, Mitha, A, Hanouch, M, Zetterli, P, and Bull, G (2014). Partnerships in Mobile Financial Services: Factors for Success. IFC: Washington, D.C., United States of America. http://www.mastercardfdn.org/wpcontent/uploads/Partnerships+in+Mobile+Financial+Services.pdf

http://www.ifc.org/wps/wcm/connect/113c8880418993f38c15bf8d8e2dafd4/Partnerships+in+Mobile+Financial+Services+PDF.pdf?MOD=AJPERES

Geraldine O’Keeffe

Geraldine is Chief Operating Officer and co-founder of Software Group, a company focused on providing delivery channel technology to the development finance sector. Geraldine has worked globally with financial service providers to consult, design, build and deploy technology solutions with the aim to improve efficiency, outreach and expand access to financial services. Previous experiences includes consulting for Arthur Anderson and CMP in London, IT manager for an MFI in Uganda, Director for an MIS vendor, and independent consultant. In the last 13 years, Geraldine has completed over 50 consultancy assignments and 30 successful software implementation projects. Geraldine has a Masters in Management and Information Systems from the University of Manchester and graduated with distinction.

Charlene Bachman

Charlene Bachman is a development finance professional working as the Business Development Manager for Software Group in Asia Pacific. With experience working with financial institutions across Latin America, Asia and the Pacific, Charlene promotes the use of delivery channels and technology solutions that aim to expand the reach of financial inclusion, increase operational efficiency and facilitate access to financial services. Prior to joining Software Group, Charlene worked in Global Investments at Accion International where she supported multiple impact investing funds targeting the MFI and Fintech sectors with a range of business development, investment analysis and portfolio management activities. Charlene holds dual bachelor degrees in Business Administration and International Studies from American University in Washington, DC.

Omoneka Musa Oyier

Omoneka is an Operations Officer in the IFC Financial Institutions Group Advisory Services team, and manages advisory projects for IFC clients looking to scale up mobile money and agent banking across Africa. Omoneka has a background in management consulting with experience providing technical assistance to banks, microfinance institutions, mobile financial services providers and policy makers. Omoneka has a Master’s Degree in International Relations and Economics from Johns Hopkins University’s School of Advanced International Studies (SAIS).

The Partnership for Financial Inclusion

The Partnership for Financial Inclusion is a $37.4 million joint initiative of IFC and The MasterCard Foundation to expand microfinance and advance mobile financial services in Sub-Saharan Africa. It brings together the intellectual and financial capital of the Foundation with IFC's market knowledge, expertise and client base. The Partnership is also supported by the Bill & Melinda Gates Foundation and the Development Bank of Austria (OeEB, Oesterreichische Entwicklungsbank AG), and collaborates with knowledge partners such as the World Bank and the Consultative Group to Assist the Poor (CGAP). An important objective of the partnership is to contribute to the global community of practice on financial inclusion, and to share research and lessons learned. This publication is part of a series of reports published by the partnership. To find out more, please visit www.ifc.org/financialinclusionafrica

Software Group

Software Group is among the leading global vendors of delivery channels solutions for Microfinance Industry with experience in over 50 countries. They are helping their clients to address the financial inclusion challenge by providing a variety of innovative delivery channel solutions that helps expand outreach and improve efficiency. Learn more about Software Group's products and services at www.softwaregroup-bg.com

The MasterCard Foundation

The MasterCard Foundation is an independent, global organization based in Toronto, Canada with over US$9 billion in assets. Through collaboration with partner organizations in 49 countries, it is creating opportunities for all people to learn and prosper. The Foundation's programs promote financial inclusion and advance youth learning, mostly in Africa. Established in 2006 through the generosity of MasterCard Worldwide when it became a public company, the Foundation is a separate and independent entity. The policies, operations and funding decisions of the Foundation are determined by its own Board of Directors and President and CEO. For more information on the Foundation, please visit: www.mastercardfdn.org

IFC

IFC, a member of the World Bank Group, is the largest global development institution focused exclusively on the private sector. Working with private enterprises in about 100 countries, we use our capital, expertise, and influence to help eliminate extreme poverty and boost shared prosperity. In FY14, we provided more than $22 billion in financing to improve lives in developing countries and tackle the most urgent challenges of development. For more information, visit www.ifc.org.

CONTACT DETAILS

Anna Koblanck
IFC, Sub-Saharan Africa
akoblanck@ifc.org

www.ifc.org/financialinclusionafrica

2015

SoftwareGroup
doing it right

The MasterCard
Foundation

IFC International
Finance Corporation
WORLD BANK GROUP