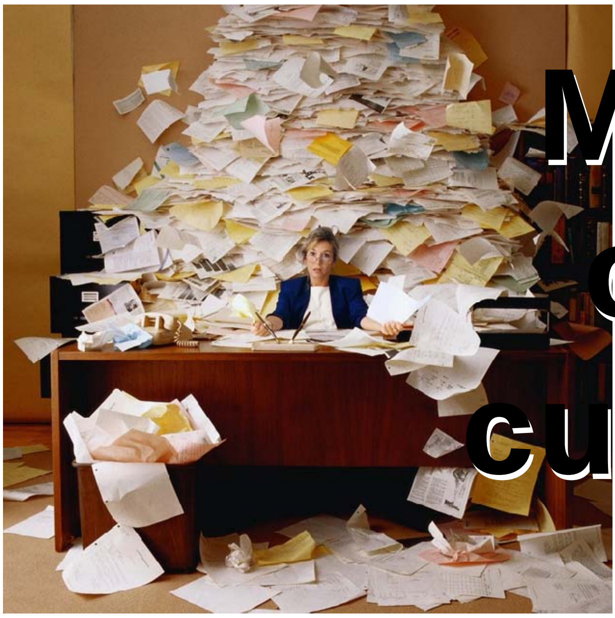


Maintenance of wholesale customer data

A guide for UK investment firms

January 2010

CDMG
A JWG Workgroup

JWG
Making sense of financial services regulation

About this research:

This guidance is based on JWG's analysis of:

1. Detailed requirements mapping of 1,000 pages of financial services regulation related to the treatment of customer data
2. The reference process for acquiring and maintaining wholesale customer data
3. The reference wholesale customer data set
4. Common customer data processing issues for firms
5. UK customer data processing costs
6. More than 15 workshops with industry practitioners
7. Over 30 individual interviews
8. 4 detailed industry guidance discussions with the FSA in 2008 and 2009
9. Comments received on previous guidance drafts published in March 2009

We would like to thank those who kindly gave their time to review and comment on earlier drafts of this guidance.

About the CDMG and this document:

The Customer Data Management Group (CDMG) is a special interest group (SIG) hosted by JWG, a think-tank of senior professionals with extensive experience in Financial Services (FS) operations and technology implementation.

It was established in response to comments by participants at JWG's 2008 FORUMS which identified that improving customer data was a top priority. It is defining the reference operating models required to meet the principles-based demands of customer data management.

CDMG membership is drawn from senior operations, risk and compliance officers from major firms and their suppliers. CDMG includes member firms of the Futures and Options Association (FOA) and the Association for Financial Markets in Europe (AFME) and the Centre of Investigation for Financial Electronic Records (CiFER).

The group is examining the impact of new legislation as it appears – this is not just an IT issue, this is for all people that manage the many functions affected by the regulations.

This guidance will help senior managers understand the issues and aid with prioritisation of resource allocation. Using the guidance as a benchmarking tool to align practices will provide a greater understanding of your firm's particular challenges.

JWG seeks to be recognised by regulators, financial institutions and technology firms as the independent analysts to help determine how the right regulations can be implemented in the right way

For more information, please see www.jwg-it.eu.

Contents

This guidance does not purport to be a definitive guide, but is a set of non-exhaustive statements and recommendations that firms may wish to consider utilising as a benchmark tool or adopting to assist in complying with the various requirements (including in-house policies) relating to the maintenance of professional or eligible counterparty customer data.

Disclaimer

JWG has taken all reasonable care and skill in the compilation of this guidance, however JWG shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising as a result of errors or omissions or the use of this publication by the users, whomsoever they may be.

JWG recognises that some of the terms appearing in this report are proprietary. All such trademarks are acknowledged and every effort has been made to indicate them by the normal UK publishing practice of capitalisation. The presence of a term in whatever form does not however affect its legal status as a trademark.

The analysis and views expressed within this guidance are those of JWG and the CDMG based on their experience and recent discussions in the marketplace relating to the implementation, in respect of customer data management, of global regulation. These views are, by their very nature, evolving on a constant basis.

1 Executive summary

At JWG's 2008 FORUMS in London, Frankfurt and Milan, some 300 FS participants agreed that a key priority was for firms to have standards relating to the maintenance of customer data to enable them to mitigate risk in a principles-based trading environment. The top priority, as identified by 55% of attendees, was improving the quality of products and customer data.

Over 40 companies are removed from the UK Companies House register every business working hour – a 31% increase since 2003[1]. All types of customers, from big corporations to small hedge funds, are frequent generators of changes to their Companies House reference data sets. Firms that have incomplete or out-of-date customer data risk breaching anti-money laundering or counter-terrorism legislation, financial sanctions obligations, regimes and or regulatory requirements, such as those in relation to systems and controls or suitability and appropriateness. In addition, there has been a number of high profile cases relating to customer data security breaches and the reputational damage and regulatory fines that have accompanied these have been significant and well-publicised.

Defining and maintaining quality customer information is complicated due to the number of different components in the customer data set, the multiplicity of data sources for each data entity (i.e., the type of data that describes an aspect of the data category), the rapidity with which the information can and does change and the requirement required to link the information across the breadth of functions in the firm – and its supply chain - that are involved in managing it. The challenge for firms is to establish policies and operating model procedures which not only collect the correct information when the relationship starts, but ensure appropriate mechanisms are in place to maintain an up-to-date view of the customer across the many touchpoints between customer and the firm. Firms' departmental needs for customer data may vary, but it is crucial that data is current, reliable and readily accessible.

The CDMG's objective is to provide guidance that describes the characteristics of the policy and the operating model for customer data management for wholesale customers. CDMG considers that there is a substantial business case for developing customer data management capabilities which reduce operational risk and provide management with greater insight into firms' risk profiles.

1.1 Summary business case

Preliminary research conducted by the CDMG indicated that the cost to UK firms of managing customer data updates is over £1 billion per annum and that any efficiency savings are therefore likely to be significant.

- Cost saving could be understated when taking into account EU and other international dimensions
- Financial institutions of all sizes may benefit from a consideration of this guidance either as a benchmarking tool or to initiate and implement customer data management policies
- Customer data management is an important agenda item for firms and its relevance to risk management controls has been heightened by the recent market turmoil.

CDMG recognises that cost savings will take time to materialise but believes that the possible business benefits may provide immediate results including:

- Increased customer protection
- Better firm risk management
- Improved customer data transparency

[1] JWG analysis of UK Companies House register statistics

- Flexibility for future changes in customer data management
- A common language for practitioner and auditor.

Up-to-date and accurate customer data can also help a firm to maximise business opportunities, protecting and improving brands, along with better customer communications and service levels, e.g., more 'straight through processing' (STP).

1.2 Operational risk

Different customer data information transparency across different jurisdictions can add complication and increase operational risk. For example, in some jurisdictions, the governmental/official companies' registers will not be publicly available, online or otherwise, or the authority/registrar may be unwilling to handle direct enquiries. Furthermore, differences in interpretation, due to differences in language, culture or law, can easily mask the true risks to firms. Both regulatory and language differences compound operational risks as customer data repositories are prone to be distributed geographically and across the supply chain.

Many operational risks can arise from failure to capture changes to customer data and in communication of the changes between the many different departments and functions within a firm. Examples include incorrect confirmation details delaying trades, missing notifications to customers leading to inappropriate trading activity or customers in sanctioned countries not being adequately reviewed.

1.3 Risk management

The knock-on effects of inaccurate customer data are more evident in times of financial turmoil. The intricacies of the many legal entities of Lehman Brothers made it difficult for firms to determine their exposures quickly - as German bank, KfW, discovered when transferring 300,000,000 Euros to Lehman's shortly after their collapse. The fraud cases of Bernard L. Madoff (and his investment firm, Bernard L. Madoff Investment Securities LLC) in December 2008 and of Robert Allen Stanford and his three companies (the Antiguan-based Stanford International Bank (SIB), Houston-based broker-dealer and investment adviser, Stanford Group Company (SGC) and investment adviser, Stanford Capital Management) in February 2009 demonstrate the importance of having accurate customer data to assess risks.

2 Recommendations overview

There is no detailed regulation of what specific customer data maintenance is required *per se*, but successive waves of regulation over the past two decades have created an holistic set of requirements. The first focused on establishing customer data management standards via money laundering statutes and data protection regimes. This was then supplemented by detailed systems and controls requirements which asked firms to produce (and follow) a comprehensive set of procedures to maintain the information.

In the last decade, a regulatory drive to define the way business should be conducted and monitored between counterparties has placed additional obligations upon firms. Enhanced information, for example, on customers, customer classification, resource levels and structure, was introduced in 2007 by the Markets in Financial Instruments Directive in Europe and similar legislation elsewhere.

By the end of 2009 it was clear that the next regulatory wave would require firms to correctly identify relationships between their customers as part of new standards. This requirement has at its core an assumption that firms can consistently link information about counterparties across business lines, products, geographies, time periods and the contexts in which it interacts with them.

Taken in aggregate, this mix of regulatory principles and prescriptive standards create a patchwork of customer data information requirements which spell out the service levels required across many different functions within the firm; the front-office, operations, compliance, legal, risk, audit and senior management all have roles to play.

As there is no agreed mechanism for the information requirements to be defined in advance of new regulation, the CDMG has developed the recommendations in this guidance to help the firms define the impact of new requirements and provide management frameworks to deal with them. CDMG's work to date has considered the relevant rules introduced up to the end of 2008. The CDMG will extend the guidance to cover 2009 and 2010 requirements.

2.1 Regulation

The regulatory requirements for customer data are contained in the European Third Money Laundering Directive (2005/60/EC and AMLIII 2006/70/EC) and the Markets in Financial Instruments Directive (2004/39/EC and 2007/73/EC). They have been implemented in the UK's FSA Handbook. Other legal requirements include the Data Protection Act, Proceeds of Crime Act, and Counter-Terrorism Act, etc.

Industry materials relevant to customer data have been published by groups such as the Joint Money Laundering Steering Group (JMLSG), Wolfsberg Group, agencies such as the International Standards Organisation (ISO 15489, 2700 series) and the British Standards Institute (BIP 0008).

2009 saw the introduction of the Financial Services Compensation Scheme 'single customer view' requirements (FSCS SCV PS09/11), a set of policies from the Committee of European Banking Supervisors (CEBS) on tracking large exposures (CP26) and the UK's introduction of new liquidity management standards (PS09/16). All of these require that the firm knows, and is able to prove that it knew, about its customer.

FSA rules require firms to ensure sufficient customer information is collected and verified with obligations to maintain this data. Perhaps most importantly, the FSA has demonstrated that it is serious about holding firms to account for the results of their actions:

> *The focus of our philosophy, however, is not per se on our principles, but rather on* ***judging the consequences of the actions of the firms and the individuals we supervise****. Given this philosophy, a* ***better strapline would be 'outcomes-focused regulation'****."*

Hector Sants, Chief Executive, FSA. 2009 business plan. 12 February 2008

As signalled, the consequences for failure are rising. Fines for systems and control violations are increasing in both frequency and value. In January 2009, the FSA issued Aon Limited a £5.25 million fine for failing to take reasonable care to organise and control its affairs responsibly and effectively. In September 2009 the FSA fined Barclays Capital Securities Ltd and Barclays Bank PLC £2.45 million for inaccurate transaction reporting – including 7 million instances where the investment firm had failed to provide the appropriate code to identify the relevant counterparties for transactions.

2.2 Introduction to the guidance

The overall objective of the CDMG guidance is to define the minimum operational performance guidelines to mitigate customer, operational and regulatory risks that apply across the whole organisation. To that end, seven recommendations were formulated to provide an industry benchmark, as shown in Figure 1.

1. Policy creation. Firms should create an internal policy for maintaining wholesale customer data that is aligned with existing control policies (the 'maintenance policy')

2. Governance and metrics. The maintenance policy should outline the operating model controls for selecting and managing the customer data set

3. Regulation-based data set. Customer data sets should be defined in the maintenance policy and linked to regulations and legal requirements

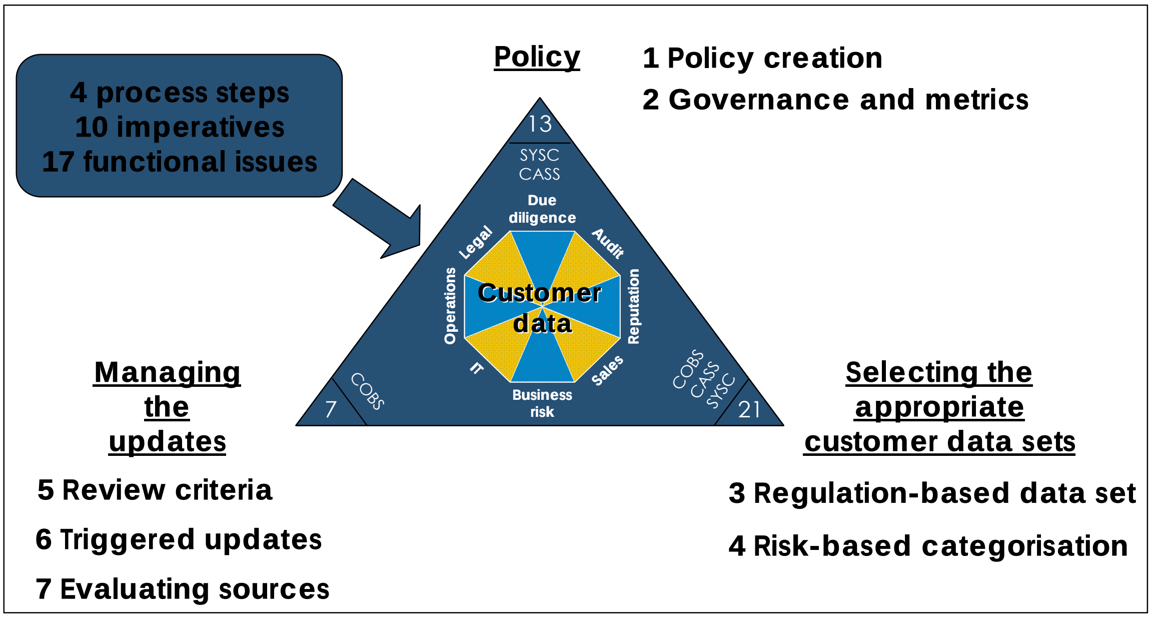
4. Risk-based categorisation**.** Customer data sets should be categorised and prioritised based on the nature, scale and complexity of the activities of the financial institution

5. Review criteria. The maintenance policy should define criteria, frequency and rigour for periodic reviews aligned with risk-based customer data categorisation of recommendation 4

6. Triggered updates. The maintenance policy should outline the events that impact the regulation-based customer data set defined in recommendation 3

7. Evaluating sources. The maintenance policy should outline the minimum performance, quality and service level standards required to approve customer data sources as 'fit for purpose'.

Figure 1: **CDMG recommendations overview**



3 CDMG recommendations

CDMG recommendations constitute neither a 'minimum checklist' nor a set of 'good practices.' Rather, they are detailed considerations for firms of all sizes to take into account when forming a view of how to establish policies and operational performance guidelines which mitigate their customer, operational and regulatory risks across their organisation. An overview of each follows.

3.1 Policy creation

The three key aspects of customer information that need to be considered are:

1. the distribution of customer data
2. the security of customer data
3. record keeping implications.

Disparate internal policies (security, business continuity, record keeping, etc.) need to be aligned to ensure appropriate management of operational risks. The CDMG believes that the creation of an internal policy specifically focused on the problems of customer data maintenance will help address the management challenges of this important industry asset.

Customer data distribution

There are many 'copies' of customer data to be found in firms, including for business continuity, test and analysis purposes. These repositories could be located in many places within and outside the UK and data may not necessarily be in its original form (e.g., information obtained from a database now held in a spreadsheet). Secure storage and easy retrieval of customer information is vital to ensure a firm can continue to function in the event of an unforeseen interruption. To minimise the operational risks, data governance policies should identify and designate authorised customer repositories, their locations and usage across the organisation.

Security

The FSA's data security review concluded that "*poor data security is currently a serious, widespread and high-impact risk to our objective to reduce financial crime*". Poorly secured customer data repositories can lead to multiple problems for financial institutions. Not only can they bring about data loss and leakage, loss of customer trust, misuse of the data (as in the case of identity theft) and regulatory fines, but poor security could threaten the integrity of customer data and, in extreme cases, its availability, e.g., deletion of customer data.

Users of 'test data' may not be aware of the full content nor appreciate the sensitivity of the customer data. Multiple repositories increase the possibility of data loss as owners of the various systems might not fully understand the security implications or the integral nature of customer data across all repositories. Security risks due to unintended access being granted can quickly arise when customers of UK and non-UK authorised firms are managed within the same repository. This risk is heightened if temporary staff (including external vendors) have access to systems or if temporary systems are created for periodic reviews or clean-up exercises. Failure to establish authenticity from a security perspective can lead to unauthorised system access.

To minimise security risks, policies should outline the controls which are appropriate for both primary customer data repositories and for any copies made from those repositories, regardless of purpose or use.

Record keeping

With customer data distributed across multiple repositories, keeping track of appropriate changes across all will be paramount. Audit trails of changes to customer data, together with details of who made the changes, will be vital to reduce operational risks and ensure the integrity of data. Record keeping is not just a technical issue; the governance aspects of ensuring that customer data maintains its integrity are equally important. For example, without appropriate access controls, data could be changed mistakenly as well as maliciously. Failure to establish authenticity of customer data from a record keeping perspective could compromise the long-term integrity of the data making it less reliable as evidence in litigation.

Therefore, record keeping policies need to outline how changes to disparate customer data sets are recorded, along with the applicable controls to ensure that such changes were authorised and could not have been altered retrospectively.

3.2 Governance and metrics

The maintenance policy needs to set out, at least at a high level, how the customer data will be maintained, how changes will be noted and implemented and how these can be tracked and reported.

Ownership

Effective maintenance of customer information is particularly challenging if customer data is updated and maintained by many different people and departments within a firm. For several reasons, customer data is also likely to be maintained in a variety of systems that reside in more than one location or jurisdiction. Some data may go through multiple changes depending on each department's use and may no longer reflect the original, and verified, change. Without transparent ownership and accountability, the operational risk of inaccurate data may not be adequately monitored. Responsibilities for specific activities should be described in the firm's operating model.

Controls

As businesses design, develop, test and deploy new systems, or make changes to existing ones, fundamental design flaws could lead to data integrity problems. For instance, changes to source or target systems could create data errors for downstream usage. Sometimes these changes are inadvertent, such as when an administrator adds a new field or code value and then neglects to notify the managers of connecting systems about the changes. In other cases, front-line staff could reuse existing fields to capture new types of information that were not anticipated by the application designers. Appropriate incentives could play an important part in ensuring effective controls are implemented. The maintenance operating model should outline the design authority that ensures alignment of changes across the organisation in order to maintain integrity and confidence in customer data.

Metrics

Without appropriate tracking and measurement of customer data quality, controls can easily become ineffective. Data quality metrics are a good measure of the effectiveness of implemented customer data maintenance controls. CDMG has identified 10 characteristics (see Figure 2) of customer data quality. The maintenance operating model should incorporate the metrics that need to be tracked and the thresholds that are acceptable to the organisation before further investigation is required. The frequency of reporting against the metrics and the acceptable thresholds should take into account risks to customer data and should also be outlined in the maintenance operating model.

Figure 2: **Data quality attributes**

Attribute	Summary definition
1. Accuracy	The degree of conformity of a measured or calculated value to its actual or specified value
2. Completeness	The degree to which all required data is known
3. Consistency	The degree to which a set of data is equivalent in redundant or distributed databases
4. Currency	The degree to which data represents reality from the required point in time
5. Believability	Credibility based on the information itself or the history or reputation of the source
6. Security	Preventing unauthorised persons from having access to information that is safeguarded
7. Availability	The ease of obtaining and using information
8. Timeliness	The degree to which data is available when 'knowledge workers' or processes require it
9. Maintainability	Probability that an item will be retained in, or restored to, a specified condition over a specified time period
10. Verifiability	Process of checking that a product, service or system meets specifications and that it fulfils its intended purpose

Change management

Although policies and procedures may be appropriate at the inception of any customer data initiatives, changing business and regulatory circumstances could quickly render them ineffective. There are many reasons for this, including changes in personnel, reorganisations, system upgrades and decommissioning. Therefore, the maintenance policy and operating model, themselves, need to be kept in line with current practices. The frequency of maintenance procedure updates will depend to some extent on changing circumstances, but should include results from the review of metrics, the changes in customer data set and the associated risk levels and the changes in the mechanics of keeping the data up-to-date, as outlined in this guidance.

Communications

Although a maintenance policy with appropriate links and governance may be in place, monitoring and tracking performance of the operating model against the metrics will be a common method of keeping policy-makers and management informed. The applicable service levels and escalation should be in place to ensure relevant owners are notified of changes. However, supplementing both the systems and the data maintenance processes with clear communication and ownership can help cement the quality required to mitigate the risks of inaccurate data.

3.3 Regulation-based data set

The customer data requirements can be categorised into five data sets:

D1. Account structures: A customer's organisational and regulatory structure(s)

D2. Ownership and personnel: Specified individuals within a customer's organisation

D3. Customer profile: The nature of business conducted with a customer

D4. Ratings: The views of a customer from an internal and external perspective

D5. Operational: Information required for interacting with a customer.

The frequency, management and oversight of the customer data maintenance will follow a risk-based approach. However, acceptable levels of risk and their related impact are likely to change due to shifting market conditions, regulatory obligations or risk appetite. As a result, the defined minimum data set will need to be updated to align with the new conditions.

Data types

Customer information is comprised of different data types which are used for distinct purposes by different functions. For example, account structure (D1) data contains information fundamental to a firm's understanding of the customer's legal form and status. This information is vital to those concerned with understanding what type of business can be done with a customer (e.g., sales, compliance, legal, etc.). The customer profile data (D3) contains information required to assess the suitability and appropriateness of a particular transaction that is undertaken. This information may be used by functions similar to those using D1 but would also include traders and risk personnel. The operational information in D5 is most likely to be needed by those in the back-office. Just as the firm may have different personnel involved in maintaining and using this data, so will their counterparties. In summary, there are many people referencing many pieces of the same customer data jigsaw. CDMG acknowledges that customer data can exist in many durable media[2] and recognises that a there is a variety of systems used to create, process and store customer data. This guidance does not attempt to detail how to maintain customer data but concentrates on *what* customer data should be maintained.

[2] As defined by FSA glossary for 'durable medium'

Monitoring and reviews

With many different facets of customer data, it is not always clear what needs to be monitored regularly or which data should form the basis of regular reviews. Monitoring and reviewing ALL data may be an option but this may be impractical and could mask important changes that do need to be carried out. The CDMG has reviewed constituent customer data types and identified the most common entities, which could form part of a rolling or periodic review of customer data. This list is not intended to be a comprehensive dictionary of all customer data; rather a guide to be used in defining a policy which meets the scope of the outcomes-based regulations. For each data entity, a high-level definition has been agreed and the scope and considerations which should be taken into account by policy-makers have been identified. The minimum wholesale customer data[3] model within the scope of a rolling review policy is summarised below in Tables 1 through 5.

Table 1: **Account structures (D1) data entities, definitions, scope and considerations**

Data entry	Definition	Scope and considerations
Customer legal name and address	Customer's legal name and address information	All customers
Customer type	Legal status or standing of the customer, e.g., a body corporate , partnership, trust, natural person etc.	All customers
Country of incorporation	Country in which the legal status was granted. For customers with no formal legal standing, this would default to the domicile country	All customers
Regulated	Indication as to whether customer is regulated by a government appointed regulatory body,[4] along with the name of the regulatory body	All regulated customers
Listed on exchange	Indication of whether customer is listed on a regulated market and the name of the regulated market. Inclusion of additional regulated markets for multi-listed customers need to be considered	All customers listed on a regulated market
Business type	The business sector and/or primary business focus of the customer, e.g., governmental standard industry sectors	All customers
Corporate/parent name	Customer's immediate parent and/or ultimate parent's legal name	Any customer with a parent

[3] As defined by FSA's COBS 3.5 Professional clients and COBS 3.6 Eligible counterparties

[4] 'Regulatory body' as defined in FSA glossary – '*any authority, body or person having, or who has had, responsibility for the supervision or regulation of any regulated activities or other financial services, whether in the United Kingdom or overseas.*'

Table 2: **Ownership and personnel (D2) data entities, definitions, scope and considerations**

Data entry	Definition	Scope and considerations
Primary contact(s)	Name of the primary customer contact(s) with whom the firm interacts to obtain or confirm information	All customers
Beneficial ownership[5]	Name(s) of the 'true' owner of the customer	As defined in regulations
Shareholders	Name(s) of the shareholder(s) of the customer	All 'listed' customers with shareholders whose shareholding above 3% requires public disclosure[6] and named shareholders for non-listed customers
Controllers	Name(s) of key individuals. These individuals are not necessarily limited to the customer and may be part of a third party organisation	All customers
Intermediaries	Any intermediaries on whom a customer relies upon to instigate or complete transactions, e.g., investment managers, prime brokers, clearing brokers, etc.	Any customer who relies on an intermediary
Source of wealth	Indicator that there is an understanding of the source of funds, e.g., rights issue, inheritance, sale of a business or other assets	All customers

[5] As defined in Regulation 6 of UK Money Laundering Regulations 2007 and article 3(6) - Third Money Laundering Directive 2005/60/EC (AMLIII)

[6] As defined in FSA's Disclosure rules - DTR 5.1.2(1) Notification of the acquisition or disposal of major shareholdings

Table 3: **Customer profile (D3) data entities, definitions, scope and considerations**

Data entry	Definition	Scope and considerations
Customer classification	Information required to categorise a customer (i.e., eligible counterparty, professional or retail)[7]	All customers
Suitability and appropriateness	Information required to assess suitability of any recommendations/advice[8] or appropriateness for non-advised services	Any customers to whom recommendations and/or services are given
Client money	Indicator that the customer has instructed the firm to hold 'client money'[9]	Any customer holding client money
Account segregation	Indicator that customers' client accounts are segregated[10]	Any 'intermediary' customer who conducts business[11] on clients' behalf

NOTE: Ratings (D4) and operational (D5) data listed below are likely to form part of the ongoing monitoring but may not necessarily form part of a periodic or rolling review

Table 4: **Ratings (D4) data entities, definitions, scope and considerations**

Data entry	Definition	Scope and considerations
Credit	Any information required to manage credit and counterparty risks[12] as defined in policies	All customers
Reputation	Any information that is required for reputational ratings as defined in policies	All customers
External ratings	Any information that may alter the risk sensitivity of a customer as defined in policies, e.g., sovereign or company ratings, sanctions lists, etc.	All customers

[7] As defined in COBS 3.4 Retail clients, 3.5 Professional clients and 3.6 Eligible counterparties

[8] As defined in 'Personal recommendation' glossary section of FSA Handbook (referencing Article 52 – MiFID implementing directive 2006/73/EC)

[9] As defined in paragraph 2A under 'client money' glossary section of FSA Handbook

[10] As defined in CASS 7.4 Segregation of client money

[11] As defined in CASS 7.1.1 Client money rules: Application

[12] As defined in SYS 7.1.9 – 7.1.12 Credit and counterparty risk

Table 5: **Operational (D5) data entities, definitions, scope and considerations**

Data entry	Definition	Scope and considerations
Payment settlement instructions	Payment details required to transfer funds to/from customers that have not been confirmed as part of a trade	All customers
Confirms	Information that enables notification of completed transactions to a specific destination to be communicated to customers	All customers
Product and service details	Products and/or services that customers are allowed to conduct business in	All customers

Although money laundering requirements outline some of the customer data that needs to be maintained, the operational and other regulatory aspects of customer data are equally important for managing risk. By implementing recommendation 3, firms should be able to organise and control their customer data more effectively.

Tracking and updating data set changes

Specific customer data is likely to change over time due to many factors, including market events, change in business focus and risk appetite fluctuations. Likewise, data quality will degrade over time, so a maintenance policy needs to consider:

- Some customer data is more likely to change than others;
- Customers will not always notify firms of changes; changes will come from many internal and external sources; and
- Data that is monitored for changes need not be the same data that is periodically reviewed for accuracy and completeness.

Monitoring and identifying changes to the minimum data set(s) is likely to require updates to the processes and procedures involved in maintaining customer data. Revisions to minimum data set(s) could also trigger reviews of existing customer data to ensure this remains aligned with regulatory and business priorities. By regularly reviewing the minimum data set(s), customer data is more likely to remain aligned with business priorities and risks.

3.4 Risk-based categorisation

A risk-based approach is fundamental to monitoring and maintaining data appropriately. There are several considerations for firms defining their approach.

Different regulatory requirements

In defining a firm's rolling review policy, the customer's type of organisation/structure, global spread or other nature of the business, risk levels and a number of other factors will help form a data management regime that is appropriate. For example, customers which have offices or branches in many different jurisdictions are likely to be reviewed differently as the regulatory obligations of doing business with them will be more onerous, e.g., application of the US PATRIOT Act[13], which may require

[13] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

more frequent or deeper due diligence beyond the scope of what would be required for a purely UK-based customer.

Not all data are created equal

Even within a category of data, all the customer data are not created equal. Certain data has a greater regulatory, reputational or operational impact. The customer risk factors include location (e.g., country of domicile), legal form (e.g., corporates, partnerships and trusts); business activity (e.g., arms dealer, charity, casino); product or service utilised (e.g., financing, trading commodity derivatives); other external (e.g., market) events or internal (e.g., risk appetite) factors. Operational risk factors include payment, intermediary and products/service details. Regulatory risk factors include data needed to report information to the regulators and other authorities or the market in a common form, such as company registration identifiers.

Setting risk levels

Three risk levels can be set for each of the five data categories:

- Low: Data for low-risk customers and those deemed to have a low level of operational or regulatory impact

- Medium: Data for medium-risk customers with moderate level of operational or regulatory impact

- High: Data for higher risk customers with high operational or regulatory impact.

The CDMG's view is that, whilst it is possible to have more risk levels, three should be sufficient. Fewer than three levels would be extraordinary but might be appropriate in certain circumstances (e.g., a firm only dealing with a limited scope of customers could limit these levels to high-risk or no-risk business).

In general, it will be necessary to review more data entities within the higher risk categories. In addition, reviews of higher risk category data will include data defined in lower risk categories. It is expected that certain higher risk categories of operational risk data, such as payment settlement instructions, will have tighter security and controls when requested changes or amendments are made to firms' data records.

Firms define their own risk levels

Although different firms are likely to categorise the customer data according to their own particular circumstances, defining the associated risk levels aligned to the data entities can add further clarity. For instance, firms may categorise business type as a review category for all their customers if they operate specifically in a higher risk sector, such as gambling.

Complying with FSA's SYSC requirements - updates

As changes are identified through monitoring and reviews, updates will need to be performed. To ensure systems and control regulatory requirements are adhered to, firms will need to:

- Ensure changes are valid, appropriate and acted upon accordingly

- Assess impact of changes, e.g., urgency, complexity, ease of verification and risk levels

- Identify all related data item dependencies and perform timely updates.

The volume of updates and the resources available to process them will govern how many updates can be carried out within any specific time period for any particular firm. To ensure updates are applied appropriately, a firm's policy should consider:

- Priority assessments: How do you establish a priority change? What minimum criteria should apply in determining priorities?

- Change impact assessment: How does one assess the impact of a change? What consequences are there if an update is not performed?

- Change interpretation: How does one know that a change is appropriate? What common definitions should be used for interpretation?
- Validation: What documents, or what types of authentication, are required to validate a change? Which documents require independent verification?
- Change linkage: What related changes are required?

Priority weighting and impact criteria

At any particular time, a firm will have a finite set of resources to interpret, assess and process customer information changes. The volumes and frequency of changes will vary based on many factors but are likely to be highest in periods of market and economic stress. To ensure timely updates are made in order to minimise risks, firms should prioritise the updates. These priorities are expected to be based on risk profiles of the data and the immediate impact of not applying the changes.

Firms could use many different approaches to deciding which customer or customer's data should be updated ahead of another's. Priorities could be weighted using the risk-based approach above.

However, some priority updates could require further data to confirm whether the change is valid and appropriate before being applied. The timeframes for receiving the required data could vary depending on the data source. Some related data may be 'indefinitely delayed' either through malicious intent or operational problems. A decision on whether to apply a partial change in these circumstances will be dependent on the regulatory and operational impact to a firm.

Awareness

Although it is incumbent upon investment firms to monitor customer data and keep it up-to-date, it is not clear to what extent a firm needs to be 'aware' that information is manifestly out of date, inaccurate or incomplete. However, logic would suggest that the more aware a firm can be, the more able it will be to avoid operational risk.

Changes to customer data can come from many sources (both direct and indirect) including, but not limited to:

- Clients
- Consequences of events, such as mergers and acquisitions
- Internal systems (e.g., payment defaults)
- Changes to data sources filtering through, for example, data supplied by a third party.

Many changes to customer data are not communicated to the investment firm and can only be identified through proactive monitoring, reviews and requests for updates.

Consistency with risk appetite

There are three distinct activities that firms need to perform in order to ensure their customer data remains consistent with their risk appetite and objectives:

1. Identify changes by conducting regular reviews
2. Be aware of triggers that could make information out of date
3. Evaluate the sources that provide changes to ensure changes are valid and appropriate.

3.5 Review criteria

Although rulebooks and standards require monitoring of customer data to keep it current, they do not define the data set that needs to be reviewed or how often. In theory, financial institutions could review all customers and their data on the same periodic basis. However, a 'one size fits all' approach is unlikely to be the best way to control the different types of risk presented by the data.

In order to conduct periodic reviews that align to the nature, scale and complexity of their activities, firms should design their maintenance policy to accommodate the risk profiles of their customers and customer data sets.

However, some specific questions arise when planning for diarised reviews:

- Should a diarised change control encompass all customer data or only a subset thereof (e.g., a representative sample)?
- How frequently should reviews be carried out?
- To what depth of completeness and accuracy should checks be carried out?

Quantity

Deciding what customer data to review on a regular or periodic basis can be particularly challenging due to the volumes of data involved. There are many approaches that could be taken in determining which customer data sets to review. Firms should select customers to review by utilising the regulation-based data set and their risk-based categorisation. For instance, a greater quantity of data would be selected for review for high-risk customers than for lower risk customers. However, firms should note that including a significant percentage of customers that have had recent updates in their samples may not be appropriate or effective. Further, firms that have customers primarily in one risk category are likely to have a greater percentage in their sample for that category than firms that have a more even spread across risk categories. The best approach for a firm would be to consider a combination of these methods to ensure that review sample sizes are appropriate for the different levels of risk.

Frequency

Although each type of customer could be reviewed with the same frequency, this may not be practical or effective. High-risk customers and data should be reviewed more frequently than lower risk customers or data. The frequency of reviews could also vary with sample size, i.e., more frequently for smaller samples, than for a large to ensure appropriate coverage of the population during the entire review cycle. However, financial institutions should recognise that certain data, which is more volatile and therefore subject to more frequent updates, e.g., settlement instructions (which are likely to be kept up-to-date as a natural course of conducting business), may not need additional periodic reviews.

Depth of accuracy and completeness

Due to the volume of data and changes, no customer data is likely to be 100% accurate or complete. Acceptable levels of inaccuracy and incompleteness will be driven by the regulatory or operational impact the data could have on any particular firm or market. Quality metrics will determine the acceptable levels of accuracy for a firm. Review of data can be based on sample quantity, with a frequency geared to risk. However, within these parameters, all data must have been reviewed at least once in a set period (e.g., 5 years) to ensure accuracy is maintained. Tracking the quality levels will help creation and improvement of the sample sizes and determine frequency of reviews.

3.6 Triggers

Changes to customer data can come from many sources (both direct and indirect). Many functions and departments within a firm will be alerted to changes in customer information. What may not be recognised is the nature of the indirect changes. Further, the scale and significance of these changes may not be apparent to any particular recipient. A 'trigger event' is an action which results in changes to customer information which may have implications for one or more functions of a firm.

What is a trigger?

The significance of trigger events may differ between firms. Therefore, each firm will need to customise and document the trigger events aligned to its business. For example, firms that do not have publicly listed companies as customers may not need to include corporate actions as a trigger event.

Triggered updates could result from changes related to a customer that necessitate changes to other data sets, or from changes to the external environment (e.g., war breaking) in which the customer operates that change the risk rating associated with the customer data. A further consideration is a change to a system-related characteristic (e.g., security of a component or jurisdiction of operation) that could lead to a change in the risk rating of associated customer data.

Failure to identify triggers

Failure to identify trigger events may result in specific updates being missed. There may also be a failure within the organisation to appreciate the significance, or risks, of a change to a data entity that might trigger a change to another, related, data entity. For example, a company reorganisation may result in a change in name and a domicile change. In itself, this change may not be important, but it may signify, for example, a move by a customer to a higher risk country.

Sharing information

Some of the updates resulting from the trigger events may be passed on to other business units or functions because it is explicitly recognised that there are dependencies, e.g., a change in domicile requiring a check against a country risk register. Some triggered customer changes may not, although there may remain implicit dependencies, e.g., increased risk in a particular sector due to negative news about a significant company in the sector.

Defining triggers in the policy

Outlining the specific events within the maintenance policy can help firms to maintain a holistic view of upcoming changes that may impact customer, operational or regulatory risks.

Some of the common events that could trigger data updates, and which could form part of a firm's maintenance policy, are listed below:

- Company reorganisations
- Corporate actions
- Negative company news, e.g., revised credit rating
- Change in country/industry risk indices
- International/regional/local law changes
- Natural expiry dates, e.g., certain information contained in annual returns
- Trading activity changes.

By aligning the trigger events to the regulation-based data set (as defined in recommendation 4), firms could identify important and higher risk changes on a more consistent basis. This consistency is likely to benefit overall customer data risk management and controls.

3.7 Data sources

Customer data changes derived from ongoing monitoring, regular reviews and trigger events will come from many sources, including customers and external sources. To ensure all the possible changes to customer data are monitored and kept up-to-date, firms will need to:

- Identify appropriate update sources;
- Identify appropriate data entities likely to change; and then
- Identify the probable source to update each data entity.

Is it valid?

Complications may arise when identifying whether a change from any particular source is valid and appropriate. It may be hard to identify the timeliness, accuracy and authenticity of the information as it comes to hand and may also be difficult to prioritise sources of information in cases of conflict. Complexity increases as each piece of information could also trigger the need for further checks and updates to related data. These complexities could mask important changes that need to be tracked to manage customer and operational risks.

The CDMG has identified two fundamental questions that firms could use to identify whether required updates are valid and current:

- Source reliability - how do firms know that the source is 'fit for purpose' and authoritative?
- Information currency – how do firms determine if the changes are current?

No 'golden source'

No single source is likely to be sufficient to provide all the customer updates required for a firm to manage its data efficiently. Accordingly, the CDMG believes that each firm should identify the sources that are right for their business, i.e., are fit for purpose. Due diligence is required to verify that appropriate controls are applied to the financial institution's review criteria and triggers.

It should be noted that information from some sources, for instance customer-supplied information, may require independent verification. The verification sources are likely to be governmental registrars and/or commercial data suppliers. The various data sources have inherent interdependencies, complexities and risks making judgements more difficult, as outlined below:

- Customer supplied data: Changes may be supplied directly by customers or indirectly by public notification. However, these changes will not necessarily be supplied to the relevant recipient within a firm. This information could be provided in a 'durable medium' or in verbal form. Although firms can rely on information provided by customers, unverified changes could expose a firm to unacceptable risks for some types of data
- Governmental registrars: Some customer data updates can be sourced directly from governmental registrars, e.g., information in annual returns and filings. Different regulatory requirements of multiple governments and jurisdictions result in differing data requirements and controls. Data normally available from one registrar may not necessarily be available in another jurisdiction. Accordingly, data gathering may not necessarily be standardised across different countries or regions. Applying the same criteria for all jurisdictions could increase operational risks as required customer updates may not be available
- Commercial data providers: Data supplied by providers will vary in its breadth, depth and quality. Data quality is dependent on a supplier's experience and resources, which can vary depending on the subject matter, location and standards being employed. Reliance on an inappropriate supplier, e.g., using a supplier specialising in UK customers for non-UK customer information, would not necessarily meet systems and controls objectives. As commercial providers may also provide information from governmental registrars, financial institutions will need to monitor and review the controls that have been applied to ensure they meet their requirements.

Conflicts and duplication

The different sources may have different approaches to the same data which could result in different updates being identified for the same change. Alternatively, data which may appear to be duplicated may actually be different. There are many reasons for these conflicts including transposition errors, timing differences and differences in interpretation. Firms need to be alert to these possible conflicts so as to determine which source may be most authoritative and which to use.

Documenting and using common criteria for assessing reliability and currency of a source's data should reduce the customer and operational risks associated with inaccurate data. These criteria will play an important part in defining quality metrics.

4 Conclusion

The recommendations in this document, whilst not exhaustive nor definitive, have been developed so as to assist firms aspiring to develop regulatory data policy and as a benchmark tool for those wishing to enhance their operating model. Due to the breadth, depth, cost and overall impact of customer data management, we hope that this guidance will help focus firms' attention – and particularly the attention of senior management – on some of the issues arising, and provide assistance in the development of customer data management policies.

JWG
Making sense of financial services regulation