A-TEAM GROUP

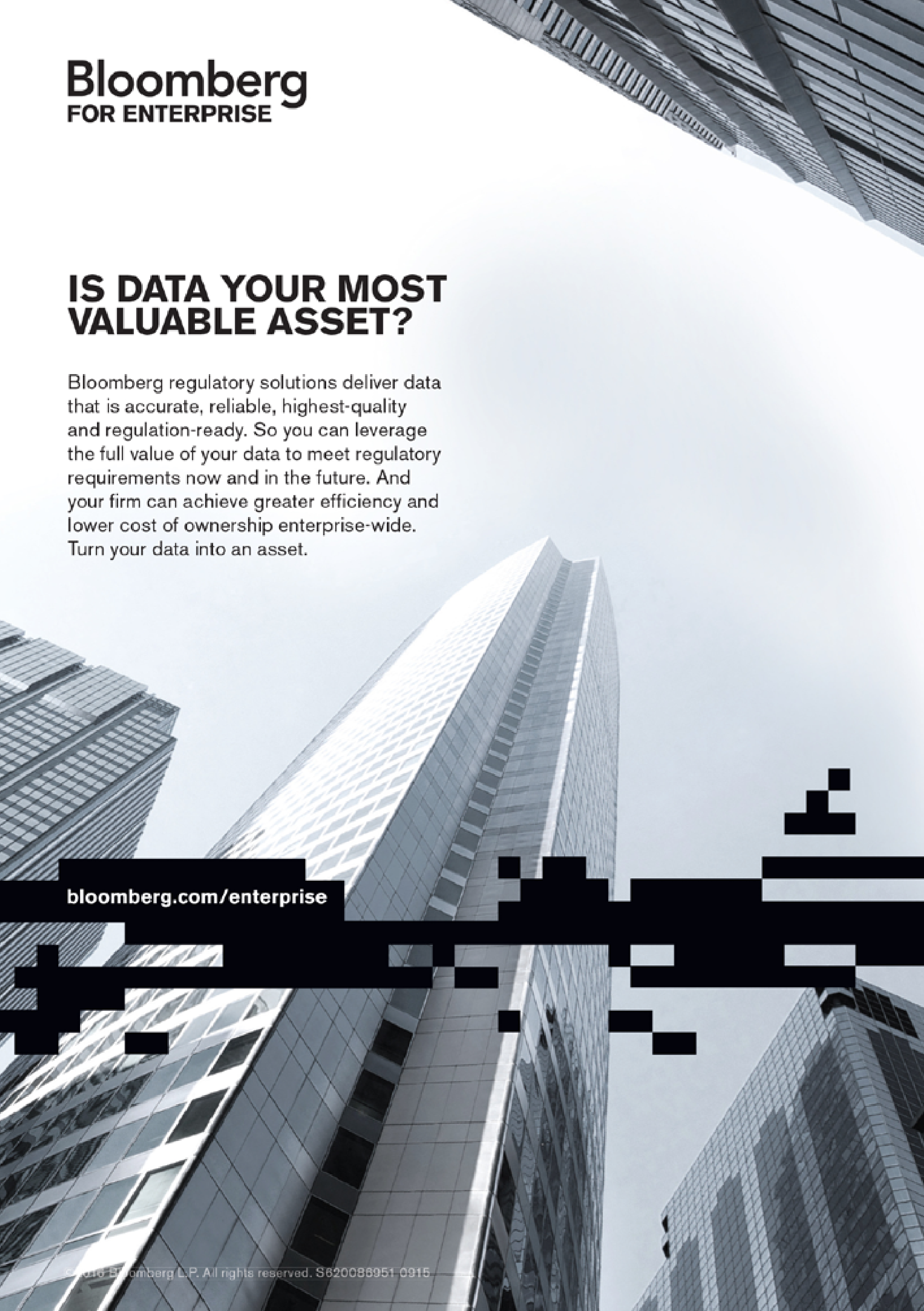
REGULATORY DATA HANDBOOK

FOURTH EDITION

2016/17

Sponsored by

SmartStream



REGULATORY DATA HANDBOOK

A-TEAMGROUP

Publisher
Angela Wilbraham
angela@a-teamgroup.com

Managing Editor
Andrew P. Delaney
andrew@a-teamgroup.com

Editor
Sarah Underwood
sarah.underwood@a-teamgroup.com

A-Team Group

Chief Executive Officer
Angela Wilbraham
angela@a-teamgroup.com

President & Chief Content Officer
Andrew P. Delaney
andrew@a-teamgroup.com

Editor
Sarah Underwood
sarah.underwood@a-teamgroup.com

Sales Director
Jo Webb
jo@a-teamgroup.com

Marketing Operations Manager
Leigh Hill
leigh@a-teamgroup.com

Director of Event Operations
Jeri-Anne McKeon
jeri-anne@a-teamgroup.com

Events Content Manager
Lorna Van Zyl
lorna@a-teamgroup.com

Client Services Manager
Ron Wilbraham
ron@a-teamgroup.com

Production Manager
Sharon Wilbraham
sharon@a-teamgroup.com

Design

Graphic Designer
Victoria Wren
victoria@wr3n.com

Postal Address
Church Farmhouse,
Old Salisbury Road,
Stapleford, Salisbury,
Wiltshire, SP3 4LN
+44-(0)20 8090 2055
info@a-teamgroup.com
www.a-teamgroup.com
www.datamanagementreview.com
www.intelligenttradingtechnology.com

Turning Regulatory Compliance into Business Opportunity

Welcome to our fourth edition of the A-Team Group Regulatory Data Handbook – still our most popular download ever from the Data Management Review website.

The growing list of regulations and their compliance requirements continues to put pressure on financial institutions across the buy side and sell side. New regulations on our radar include the fourth Anti-Money Laundering Directive (AMLD4), European Market Infrastructure Regulation II (EMIR II), FIDLEG – or the Swiss Financial Services Act, Fundamental Review of the Trading Book (FRTB), General Data Protection Regulation (GDPR), Market Abuse Regulation (MAR), the Network and Information Security Directive (NIS), Packaged Retail and Insurance-based Investment Products (PRIIPs), Section 871(m) of the Internal Revenue Code, and Securities Financing Transactions Regulation (SFTR).

We have also touched on Brexit, which leaves all European financial regulations in place until negotiations on the UK's new relationship with the EU are completed.

Regulatory pressure is a driving force for many data management decisions and budgets, but being driven by fear of non-compliance and consequent penalties is not good for business.

Now, attention is turning to how financial institutions can leverage investment being made in data management for compliance in order to support business transformation and growth.

This is a topic A-Team has been covering across its content and we will continue to track progress throughout the year. We've delved into the pain points data managers face, the approaches they are taking, and the technology and data solutions that are available to help them both comply and build on their businesses.

If you find the overviews in this handbook useful, you may also value our more in-depth coverage on the impact of regulations on data management. You can find this on our website at www.datamanagementreview.com by browsing these sections:

- Surveys and white papers
- Webinars
- Additional handbooks
- Data Management Summit events in New York and London.

I hope you enjoy this latest version of our Regulatory Data Handbook.

Angela Wilbraham
Chief Executive Officer
A-Team Group

CONTENTS

Introduction	3
Foreword	7
AIFMD	8
AMLD4	10
Basel III	12
BCBS 239	16
Benchmarks Regulation	18
Brexit	20
CCAR	21
Corep	23
CRD IV	24
Dodd-Frank	26
EMIR and EMIR II	29
FATCA and GATCA	33
FIDLEG	37
Finrep	39
FRTB	40
GDPR	44
IFRS	46
KYC	48
MAR and MAD	54
Margin Requirements – BCBS/IOSCO	56
MiFID II	58
MiFIR	63
NIS	65
PRIIPs	66
SEC Form PF	68
Section 871(m)	70
SFTR	72
Solvency II	73
UCITS	76

Foreword

By Dr Darryl Twiggs, EVP Product Management, SmartStream

In recent years, numerous regulations have been published demanding the introduction of new controls, greater transparency and more frequent reporting. Many of the regulations originate from G20 mandates and provide global, standardised controls, but some have more regional origins and have been implemented via national laws in different jurisdictions, sometimes causing overlap or differences in the way requirements are applied.

The regulatory landscape is certainly complex and likely to become more so as further rules are implemented. It will also become larger as new regulations extend to cover previously exempt business lines and organisations. For financial institutions, regulation is having a profound effect on daily operations from data management to regulatory reporting. The cost of compliance is high, but so too is the cost of failure.

At the heart of solving the regulatory conundrum at an affordable cost are flexibility and the ability to handle complexity. These requirements can be met by emerging technologies that sustain business operations while supporting compliance with stringent controls, data aggregation demands, risk management requirements and reporting schedules.

SmartStream has shaped its solutions to assist clients as they respond to increasing regulation. The solutions are architected on a single technical stack, support all asset types and are founded on flexible workflows to enable easy adoption of processes associated with new regulatory requirements. They also provide real-time processing with intra-day control points and fulfil the critical factor of meeting regulatory deadlines quickly, accurately and efficiently.

To ease the burden of cost, SmartStream solutions are deployed on-premise, hosted or delivered as managed services, providing attractive options to firms subject to regulatory control, monitoring and reporting. Among the solutions is a unique reference data management utility that provides on-demand, high quality data to banks' front, middle and back offices, ensuring the best straight through processing rates while minimising errors and costly disputes.

As increasing regulation puts pressure on firms to implement necessary controls, the ability to achieve rapid deployment of regulatory responses at the lowest possible cost is a significant advantage.

AIFMD

At a Glance

Regulation: Alternative Investment Fund Management Directive (AIFMD)

Regulatory Regime/ Authority: EU

Target Market Segment: Alternative investment funds

Core Data Requirements: Identification of asset types, third-party valuation of fund assets, reporting

Significant Milestones

July 21, 2011: Adopted by the European Commission

July 22, 2013: Directive comes into force

July 30, 2015: ESMA publishes advice on extending passport system to six non-EU countries

July 18, 2016: ESMA publishes advice on extending passport system to a further six non-EU countries

Description and Data Requirement

The Alternative Investment Fund Management Directive (AIFMD) is an EU directive that focuses on data and transparency requirements in alternative fund managers' fund registration, valuation and reporting processes.

The goal of the directive is to set regulatory standards and create a level playing field for the operation of alternative investment funds in Europe through the use of reporting and governance requirements. It requires firms to establish 'appropriate and consistent' procedures to allow for the independent valuation of a fund's assets. To achieve this, the valuation must be performed either by an independent third party or by the asset manager, provided there is separation between the pricing and portfolio management functions.

AIFMD also aims to facilitate regulatory systemic risk monitoring by improving transparency. To this end, funds must register with national regulators and provide disclosure on their risk management systems and investment strategies in order to present a clear picture of their overall risk and data management capabilities. Finally, AIFMD introduces capital requirements for firms acting as third-party administrators for alternative investment funds.

As with many other regulations, firms within the scope of AIFMD need to maintain the accuracy and quality of their reference data, and support any standards requirements for the identification of instruments. Firms must also manage Market Identification Codes (MICs) and Legal Entity Identifiers (LEIs).

One of the most challenging data management aspects of the regulation is completing Annex IV, a broad and prescriptive transparency reporting requirement that must be fulfilled by alternative investment fund managers. The annex includes a reporting template that comprises more than 40 questions, requiring managers to provide information including instruments traded, exposures, assets under management,

AIFMD (cont.)

liquidity profiles, a breakdown of investments by type, geography and currency, and stress test results.

The reporting frequency for Annex IV is determined by assets under management. Firms managing between €100 million and €500 million must file Annex IV reports annually, while those managing between €500 million and €1 billion are expected to file on a semi-annual basis, and those running in excess of €1 billion must submit reports on a quarterly basis.

A contentious problem for data management is the requirement for alternative investment funds to use an EU-domiciled depositary bank, which must also provide transparency into its own operations. The ability to provide data quickly, accurately and in the correct format to support the transparency and reporting requirements of AIFMD can also require significant investment in data management.

While AIFMD initially covered alternative investment fund managers and funds registered in the EU, providing them with a passport system that allows fund managers and funds registered in one EU member state to market products to other member states, the European Securities and Markets Authority (ESMA) has been investigating whether the passport system should be extended to non-EU alternative investment fund managers and funds.

In July 2015, ESMA published initial advice on the application of the passport system to six non-EU countries, namely Guernsey, Hong Kong, Jersey, Switzerland, Singapore and the US. More recently, in July 2016, ESMA extended its advice on the application of the passport system to a further six countries, namely Australia, Bermuda, Canada, Cayman Islands, Isle of Man and Japan. ESMA's advice on all 12 non-EU countries will be considered by the European Parliament, Council and Commission before any decisions are made on extending the passport system.

Dates for Diary

July 2017: European Commission to review directive

Key Links

Full Text:
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1474883233433&uri=CELEX:32013R0231

FAQs:
http://europa.eu/rapid/press-release_MEMO-10-572_en.htm

ESMA Q&A
https://www.esma.europa.eu/sites/default/files/library/2016-568_qa_aifmd_april_2016.pdf

AMLD4

At a Glance

Regulation: Fourth Anti-Money Laundering Directive (AMLD4)

Regulatory Regime/ Authority: EU

Target Market Sector: Financial institutions

Core Data Requirements: Customer data due diligence, identification of PEPs, beneficial ownership data

Significant Milestones

December 15, 2005: Third AML Directive takes effect

February 10, 2015: AMLD4 approved by European Council

May 20, 2015: AMLD4 adopted by European Parliament

July 5, 2016: European Commission adopts proposal to amend AMLD4

Description and Data Requirements

The fourth EU Anti-Money Laundering Directive (AMLD4) updates the EU's third AML Directive and aims to prevent use of the financial system for purposes of money laundering and terrorist financing. It strengthens rules on AML and counter terrorist financing (CTF), improves consistency of rules across EU member states, and aligns with recommendations from the Financial Action Task Force that are broadly considered to be global standards.

AMLD4 was adopted by the European Parliament in May 2015 and was due to take effect on June 26, 2017, but recent terrorist attacks in the EU and the revelations of the Panama Papers led the European Commission to adopt a proposal on July 5, 2016 that amends the AMLD4 framework, provides more stringent rules on AML and CTF, and brings forward the effective date of the directive to January 1, 2017.

The penalties for non-compliance remain the same, with fines for financial institutions of at least €5 million or 10% of annual turnover.

At a macro level, AMLD4 clarifies the need for policies and procedures to mitigate AML and CTF risks at the EU, national and business level. It also calls on companies to report suspicious transactions.

At a more granular level, the directive extends customer due diligence, requiring firms using simplified due diligence to evidence why they have considered customer risk to be low enough to use this type of due diligence. It also extends the scope of Politically Exposed Persons (PEPs) to include domestic PEPs, who are defined as prominent public people in the EU.

To improve transparency, AMLD4 requires financial institutions to verify the identity of their customers and the beneficial owners of their customers, and make this information readily available to national authorities.

On a broader scale, member states must set up registers that record the ultimate beneficial owners of businesses. While AMLD4 initially made these registers accessible to national authorities, entities such as banks doing due diligence on customers, and others who can demonstrate legitimate interest in gaining access to the information, the European Commission's July 2016 proposal goes further, requiring member states to provide public access to beneficial ownership data.

AMLD4 (cont.)

Similarly, AMLD4 has been amended to require national registers to be interconnected, allowing national authorities, financial intelligence units and obliged entities to identify beneficial owners easily and efficiently.

To achieve faster detection of suspicious money laundering and terrorist financing transactions, a further amendment requires member states to set up automated, centralised mechanisms that can quickly identify holders of bank and payment accounts. Member states' enhanced customer due diligence measures for high-risk countries will also be harmonised to remove the option of making transactions in jurisdictions with less stringent regulations. Reflecting the rise of cryptocurrencies, AMLD4 has been amended to bring virtual currency exchange platforms and custodian wallet providers into scope, and allow national authorities to better monitor currency transfers.

From a data management perspective, AMLD4 requirements around beneficial ownership information will stretch many financial institutions' current capabilities, while changes to customer due diligence and the definition of PEPs will require institutions to adjust existing data management processes.

Dates for Diary

January 1, 2017:
Compliance deadline

Key Links

Proposal:
http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf

Summary:
http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L0849

Text:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849

Basel III

At a Glance

Regulation: Basel III

Regulatory Regime/ Authority: BCBS and national supervisory authorities

Target Market Segment: Global financial institutions

Core Data Requirements: Disclosure of capital adequacy, risk profile

Description and Data Requirements

Basel III is a Basel Committee on Banking Supervision (BCBS) regulation that includes a comprehensive set of reforms designed to strengthen the supervision, stability and risk management of the banking sector. The reforms focus on market standards for capital adequacy, stress testing and liquidity risk with the aim of improving the ability of banks to absorb shocks arising from financial and economic stress, including mass withdrawals from bank reserves, and improve risk management, governance, transparency and disclosure.

Basel III continues the theme of previous regulations based on the initial Basel Accord. Like Basel II, it is based on three pillars covering capital requirements, risk management and disclosure, but it pushes up capital requirements, includes a minimum leverage ratio and introduces liquidity requirements.

The regulation focuses on common equity and requires financial institutions to meet a minimum capital requirement of 4.5% of risk-weighted assets, up from 2% in Basel II, and Tier 1 capital of 6% of risk-weighted assets, up from 4% in Basel II. Capital buffers are also introduced to ensure a 2.5% capital conservation threshold.

There is also a discretionary counter-cyclical buffer of up to 2.5% of common equity that can be imposed by authorities if credit growth causes an unacceptable build-up of systemic risk. The risk-based capital requirements are backed up by a minimum leverage ratio that is calculated by dividing Tier 1 capital by a bank's average total consolidated assets, but must be maintained above 3%.

Finally, the regulation introduces liquidity requirements, including a Liquidity Coverage Ratio (LCR), to make sure banks have sufficient liquid assets to cover cash outflows for 30 days. The LCR does this by ensuring that a bank has an adequate stock of unencumbered high-quality liquid assets that can be

Basel III (cont.)

Significant Milestones

December 16, 2010: Basel III rules text published

June 1, 2011: Revised version of rules text published

June 1, 2013: Guidelines updated to include LCR

January 1, 2014: Revised NSFR put in place

October 1, 2015: Risk requirements take effect

January 1, 2016: LCR minimum requirements set at 80% and increase 10% a year to 100% in 2019

January 1, 2016: Capital conservation buffer introduced

converted into cash easily and immediately in private markets to meet its liquidity needs for a 30-day liquidity stress scenario.

A Net Stable Funding Ratio (NSFR) ensures provision of enough stable funding to cover a one-year period of continued financial stress by requiring banks to maintain a stable funding profile in relation to on- and off-balance sheet activities. This should reduce the likelihood that disruptions to a bank's regular sources of funding will erode its liquidity position in a way that could increase the risk of its failure and potentially lead to broader systemic stress.

One of the major data management challenges of Basel III is meeting guidelines on risk data aggregation and analysis. The regulatory mandate requires firms to collect and analyse more data than previously from their risk management systems, and to report information in a timely manner across all business units to present an holistic view of risk exposure.

Disclosure includes details of regulatory capital and its reconciliation to reported accounts, and comprehensive explanations of how banks calculate regulatory capital.

Basel III was introduced to address concerns raised by the 2008 credit crisis and requires banks to work towards the provision of complete and accurate data, as well as data that is readily accessible to facilitate a rapid response to any future market crises. Banks with business models based on data silos will have to overhaul data management infrastructure to optimise risk data aggregation and ensure they can present a comprehensive view of risk data for full compliance.

While Basel III was initially scheduled for introduction in early 2013, changes introduced in April 2013 pushed back full implementation until March 31, 2019. This may be some time away, but some authorities are already acting on the regulation's principles.

Basel III (cont.)

For example, UK regulators have opted to take a stronger stance on LCR than Basel III by increasing the percentage of LCR required at certain time points. The UK's Prudential Regulation Authority (PRA) required firms to reach 80% of LCR from the introduction of the new regime in October 2015 running through 2016, compared to Basel III recommendations of 60% for the fourth quarter of 2015 and 70% through 2016. The PRA target rises to 90% in 2017, against 80% under Basel III, and both reach 100% in 2018.

Like the PRA in the UK, authorities in other jurisdictions are expected to expand on the regulation as they carry out their own implementations.

To ensure the regulation produces desired outcomes, BCBS is monitoring the impact of elements of Basel III, including the framework for more resilient banks, leverage ratio and disclosure requirements, the LCR and NSFR, on a sample of banks. This exercise is repeated semi-annually with end of June and end of December reporting dates. The monitoring workbook, accompanying instructions and a list of frequently asked questions are publicly available.

Dates for Diary

January 1, 2018: Leverage ratio becomes mandatory

January 1, 2018: NSFR ratio introduced

March 31, 2019: Full implementation

Key Links

Full Text: http://www.bis.org/publ/bcbs189.pdf

Overview: http://www.bis.org/bcbs/basel3/b3summarytable.pdf

LCR Text: http://www.bis.org/publ/bcbs238.pdf

NSFR Text: http://www.bis.org/bcbs/publ/d295.pdf

Leverage Ratio and Disclosure Requirements: http://www.bis.org/publ/bcbs270.pdf

BCBS 239

At a Glance

Regulation: BCBS 239

Regulatory Regime/ Authority: BCBS and national supervisory authorities

Target Market Segment: Global financial institutions

Core Data Requirements: Risk data aggregation and reporting

Significant Milestones

June, 2012: Consultation paper released

January 9, 2013: Regulation published

January 1, 2016: Compliance deadline

Description and Data Requirements

BCBS 239 is a regulation issued by the Basel Committee on Banking Supervision (BCBS) and is designed to improve risk data aggregation and reporting across financial markets. It is based on 14 principles that cover disciplines ranging from IT infrastructure to data governance and supervision, and came into force on January 1, 2016.

The principles are interdependent, designed to underpin accurate risk aggregation and reporting in normal times and times of crisis, and split into four sets.

The first set of principles covers data governance and IT architecture requirements necessary to risk data aggregation and reporting. The focus here is on top-down methodology and oversight by bank executives. The second set details effective risk data aggregation across a bank, outlining a framework for automated aggregation of complete, accurate and timely data that can support on-demand reporting.

The third set of principles aims to improve risk reporting, and with a push to establish clear and useful reports, it addresses the requirement for frequent and well distributed reports that can be tailored to business needs across departments. The fourth set requires supervisors, including regulatory authorities, to determine whether the principles are achieving desired outcomes and define any necessary corrective action.

BCBS 239 is a supplement of the capital adequacy requirements of Basel III, which consider whether firms have enough resources to monitor and cover risk exposure. Like Basel III, BCBS 239 has a significant effect on data management, requiring firms to improve risk data aggregation capabilities according to the principles and present accurate risk data for reporting.

Risk data must be captured across a bank, which means consistent data taxonomies need to be established, and the data needs to be stored in a way that makes it accessible and

BCBS 239 (cont.)

easy to understand, even in times of financial crisis. While many banks adhered to some of the principles of BCBS 239 due to other regulatory obligations before the compliance deadline, most had work to do to ensure compliance with all the principles, particularly those covering data governance, risk data aggregation and reporting. As with other regulations, compliance can be eased by breaking down data silos and creating a single enterprise-wide view of risk.

While BCBS 239 was originally published in January 2013 with the intent that global systemically important banks (G-SIBs) should be compliant by the January 2016 deadline, many G-SIBs struggled with the automation of risk data aggregation and were not fully compliant when the regulation took effect. Instead, they were either materially compliant and able to show regulators a small subset of risk reports, or able to show substantive plans, a commitment to compliance and a timetable for completion.

Domestic systemically important banks (D-SIBs) will be advised, rather than required, by national supervisors to adhere to the principles of BCBS 239, although some are expected to act ahead of regulatory intervention, acknowledging the potential advantages of BCBS 239 compliance including better customer service, improved business decisions based on accurate and timely information, reduced operational costs and increased profitability.

Key Links

Full Text:
http://www.bis.org/publ/bcbs239.pdf

Publications:
http://www.bis.org/bcbs/publications.htm

Progress Report:
http://www.bis.org/bcbs/publ/d308.pdf

A-Team Group BCBS 239 Handbook:
http://bit.ly/bcbs239handbook

Benchmarks Regulation

At a Glance

Regulation: Benchmarks Regulation

Regulatory Regime/ Authority: EU

Target Market Sector: Global financial institutions

Core Data Requirements: Index and benchmark data management, data governance

Significant Milestones

September 18, 2013: European Commission proposes regulation

June 30, 2016: Regulation comes into force

August 13, 2016: Implementing regulation comes into force

Description and Data Requirements

Benchmarks Regulation, or Regulation on Indices used as Benchmarks in Financial Instruments and Financial Contracts or to Measure the Performance of Investment Funds, is an EU regulation that came into force in June 2016. It aims to make benchmarks more reliable and less open to manipulation by improving how they function and are governed.

Regulation of benchmarks was initially proposed by the European Commission in September 2013 following alleged manipulation by financial firms of benchmarks including the London Interbank Offered Rate (Libor), the Euro Interbank Offered Rate (Euribor) and other benchmarks such as those for foreign exchange and commodities.

The June 2016 regulation was followed by a European Commission implementing regulation establishing a list of critical benchmarks used in financial markets. The implementing regulation came into force in August 2016 and allows supervisors to make use of certain provisions of the Benchmarks Regulation in advance of its application in January 2018.

Euribor was the first benchmark to be included in the list, which will be reviewed and updated by the European Commission on a regular basis and will include, in due course, other benchmarks that fulfil the criteria of critical benchmarks.

The provisions in the implementing regulation that can be used ahead of the 2018 Benchmarks Regulation compliance deadline ensure supervisors can allow the continuation of critical benchmarks where their cessation would have a severe adverse impact on market participants and undermine the integrity of markets.

In particular, classifying Euribor as a critical benchmark allows supervisors to request data contributions from banks if they deem it necessary to ensure the representativeness of the benchmark.

Benchmarks Regulation contributes to the accuracy and integrity of benchmarks by ensuring contributors to benchmarks are subject to authorisation and ongoing supervision.

It also improves the governance of benchmarks, for example providing provisions for the management of conflicts of interest, and requiring greater transparency of how a

Benchmarks Regulation (cont.)

benchmark is produced. Finally, the regulation will ensure appropriate supervision of critical benchmarks.

The regulation affects all firms using benchmark data, including banks, pension funds and insurance companies. These firms must access, store, manage and distribute growing volumes of index and benchmark data stemming from a diverse and increasing number of sources.

Firms that customise or create composite benchmarks will become benchmark administrators and will need to implement data governance policies to ensure they comply with the regulation, a task that will become onerous as these types of benchmarks are more widely adopted and create the need to manage increasing volumes of bespoke data.

Dates for Diary

January 1, 2018:
Compliance deadline

Key Links

Text:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R1011

FAQs:
http://europa.eu/rapid/press-release_MEMO-13-799_en.htm

Brexit

At a Glance

Issue: Brexit

Regulatory Regime/ Authority: UK Government

Market Segment: Financial institutions in the UK

Significant Milestones

June 23, 2016: Referendum on EU membership

Dates for Diary

Early 2017: UK Government expected to invoke Article 50

2019: Expected end of negotiations with the EU

Key Links

EU Referendum: https://www.gov.uk/government/topical-events/eu-referendum

Economic Impact: https://www.gov.uk/government/publications/hm-treasury-analysis-the-immediate-economic-impact-of-leaving-the-eu

Description

The UK referendum on membership of the EU took place on Thursday June 23, 2016. By Friday morning, it was clear that the campaign to leave the EU had won the vote and Brexit became a reality.

While there is no certainty on when and how the UK will exit the EU, there is certainty that EU financial regulations will endure until negotiations are complete either within or outside the two-year time window provided by Article 50 of the Lisbon Treaty. The UK Government is expected to send Article 50 to the European Council in early 2017, triggering the start of negotiations on the UK's new relationship with the EU.

The government could rebuild a unique relationship with the EU, or it could implement a bilateral model similar to those agreed between the EU and countries such as Canada, Switzerland and Norway. From a financial services perspective, the Canadian and Swiss options would not give financial institutions the same access to the single European market as they have now. The Norwegian model provides access to the single market through Norway's membership of the European Economic Area, but the country has to comply with EU regulations and has no say in how they are made.

Key EU regulations already in place include European Market Infrastructure Regulation (EMIR), the Alternative Investment Fund Management Directive (AIFMD), and Solvency II. Looking ahead, the Markets in Financial Instruments Directive II (MiFID II), which will transform trading and transparency across EU financial markets, is scheduled to take effect in January 2018.

While Brexit could release firms in the UK from the requirements of these regulations, the government is more likely to write equivalent regulations that, if approved by the EU, will allow financial institutions in the UK to continue trading in the single market.

The worst case would be EU withdrawal of access to the single market and the end of the financial passporting system. The best option in this situation would be to set up a trading business in an EU member country and trade from there.

Whatever the timing and outcome of Brexit, financial institutions across the UK are considering scenarios that could result from Brexit and putting together governance frameworks designed to help them manage events as they unfold.

CCAR

Description and Data Requirements

The Comprehensive Capital Analysis and Review (CCAR) is an annual exercise carried out by the Federal Reserve to assess whether the largest bank holding companies (BHCs) operating in the US have sufficient capital to continue operations throughout times of economic and financial stress, and have robust, forward-looking capital planning processes that account for their unique risks.

The Federal Reserve issued the CCAR capital plan rule in November 2011, requiring BHCs with consolidated assets of $50 billion or more to submit annual capital plans for review. The regulation has since been expanded to cover BHCs with consolidated assets of $10 billion or more and foreign banks with US operations exceeding $50 billion in assets.

The Federal Reserve capital plan rule specifies four mandatory requirements that span both quantitative and qualitative factors. The first requirement is an assessment of the expected uses and sources of capital over a nine-month planning period. The assessment must include estimates of projected revenues, losses, reserves and pro forma capital levels and capital ratios over the planning period under baseline conditions, supervisory stress scenarios, and at least one stress scenario developed by the BHC and appropriate to its business model and portfolios.

Under this requirement, a BHC must also: show how it will maintain minimum regulatory capital ratios and a pro forma Tier 1 common ratio above 5% under expected conditions and stressed scenarios; show the results of stress tests required by law or regulation; provide an explanation of how the capital plan takes these results into account; and provide a description of all planned capital actions over the planning period.

The second requirement calls for a detailed description of a BHC's process for assessing capital adequacy, while the third requirement covers a BHC's capital policy, and the fourth requires a BHC to notify the regulator of any changes to its business plan that are likely to have a material impact on its capital adequacy or liquidity.

The Federal Reserve can object to a capital plan if it has either quantitative or qualitative concerns about the plan or underlying elements such as governance, internal controls, risk identification and management, management information systems, and assumptions and analysis that support the capital planning process.

At a Glance

Regulation: Comprehensive Capital and Analysis Review (CCAR)

Regulatory Regime/ Authority: US Federal Reserve Board

Target Market Segment: Large bank holding companies

Core Data Requirements: Financial, risk and reference data, data aggregation, reporting

Significant Milestones

March 18, 2011: first CCAR conducted

November 22, 2011: Federal Reserve issues final rule on capital plans

CCAR (cont.)

Dates for Diary

June 2017: Federal Reserve releases results of CCAR 2017

Key Links

Overview:
http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20110318a1.pdf

CCAR 2016:
http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20160629a1.pdf

From a data management perspective, CCAR requires data sourcing, analytics, risk identification, risk data management and risk data aggregation for stress tests designed to assess the capital adequacy of BHCs and for regulatory reporting purposes. Data must be accessed, validated and reconciled across a BHC, often requiring data to be managed across several siloed systems, to provide consistent and accurate data. Financial, risk and reference data must then be integrated to fulfil the regulation's annual reporting requirement.

The extent of data required for compliance and the Federal Reserve's focus on risk identification and its link to capital planning and scenario generation, as well as on enterprise risk management and data governance, call for a move away from siloed systems and investment in a robust and automated regulatory framework and a flexible reporting solution.

CCAR is complemented by Dodd-Frank Act stress testing (DFAST), a forward-looking exercise that is supervised by the Federal Reserve and designed to help assess whether institutions have sufficient capital to absorb losses and support operations during adverse economic conditions. CCAR and DFAST are distinct testing exercises, although they do rely on similar processes, data, supervisory exercises and requirements.

Corep

Description and Data Requirements

Common Reporting (Corep) is a standardised reporting framework issued by the European Banking Authority (EBA) for reporting under the Capital Requirements Directive IV (CRD IV). The framework includes a number of templates to support the reporting of credit risk, market risk, operational risk, own funds and capital adequacy ratios.

The regulation has been adopted by most European countries and covers all banks, building societies and investment firms, essentially firms covered by the Prudential sourcebook for Banks, Building Societies and Investment Firms (Bipru). It requires these firms to make a substantial review of the quantity, quality and frequency of data disclosures they make as part of their regulatory reporting regimes.

For many institutions, Corep means altering processes, implementing management oversight of reports and reviewing reports for accuracy in a timely manner. The increased granularity of information required for reports increases the volume of data that must be managed, while reports must present an enterprise view of data, often requiring finance and risk functions to work together to provide consistent underlying data. Additionally, the quality and robustness of data may need to be enhanced to generate more frequent reports and firms must ensure their systems can support the XBRL taxonomy that is mandated by Corep for reporting.

Corep also introduces new schedules, such as Immovable Property Losses and Group Solvency, that firms may not be familiar with, so understanding these categories and definitions prior to reporting is crucial to ensure reports are filed correctly.

Corep was due to be implemented alongside CRD IV and the corresponding Capital Requirements Regulation in 2013, with firms within its scope submitting capital adequacy reports within 30 days of the end of each quarter. However, UK firms have only been using Corep for regulatory reporting since January 2014 and a few European countries have still to adopt the standardised reporting format.

At a Glance

Regulation: Common Reporting (Corep)

Regulatory Regime/ Authority: EBA

Target Market Segment: European financial institutions

Core Data Requirements: Risk and capital adequacy reporting

Significant Milestones

August 27, 2012: Close of consultation period

September 17, 2013: Revision of final draft

January 1, 2014: UK starts Corep reporting

Key Links

Guidelines: https://www.eba.europa.eu/regulation-and-policy/supervisory-reporting/guidelines-on-common-reporting-2011-

Explanatory Notes: https://www.eba.europa.eu/documents/10180/109739/Explanatory-notes.pdf

XBRL Taxonomy: http://www.eba.europa.eu/documents/10180/502670/COREP+FINREP+XBRL+Taxonomy+v2.0.0.pdf

CRD IV

At a Glance

Regulation: Capital Requirements Directive IV (CRD IV)

Regulatory Regime: EU

Target Market Segment: European banks

Core Data Requirements: Risk profile and disclosure of capital adequacy

Significant Milestones

January 1, 2014: Effective data

July-October 2015: Public consultation

Description and Data Requirements

Capital Requirements Directive IV (CRD IV) is the fourth version of a European Commission regulation that implements Basel III type standards covering market liquidity risk and bank capital adequacy across the EU.

The directive is divided into two parts: the Capital Requirements Regulation, which applies to all firms in the EU and includes most of the Basel III provisions in a single rulebook; and the Capital Requirements Directive, which is implemented by national law and includes provisions for transparency, governance and capital buffers.

CRD IV applies to investment firms and credit institutions within the scope of Markets in Financial Instruments Directive II (MiFID II) and focuses on improving the quality and quantity of their available capital. It builds on previous capital requirements directives, extending corporate governance and supervisory requirements, and adding sanctions for non-compliance.

It also introduces capital requirements based on risk-weighted assets (RWAs), capital buffers designed to protect firms from potential market upheaval, and liquidity and leverage requirements to ensure firms can meet cash outflows and handle stress testing scenarios. Reporting is standardised using Financial Reporting (Finrep) and Common Reporting (Corep).

Brokers, traders and asset managers that must comply with CRD IV face a number of data management challenges. From a reference data perspective, CRD IV requires extensive detail to support capital, liquidity and RWA calculations.

To meet the regulation's risk requirements, firms may need to break down data silos to improve risk data aggregation and gain a comprehensive view of their assets and exposures. As CRD IV transposes many Basel III requirements into EU law, firms also need an understanding of this latter regulation.

CRD IV (cont.)

CRD IV came into effect on July 1, 2014 and from July to October 2015 was the subject of a public consultation set up by the European Commission to consider issues such as the effect of the regulation on the level of capital held by banks, whether the regulation's requirements are proportionate to the risks they address, and whether some of the requirements could be simplified without compromising their objective of ensuring the financial stability of banks. A summary of responses from the consultation was published by the European Commission in December 2015.

Dates for Diary

January 1, 2019: Full implementation

Key Links

Full Texts:

Regulation - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:321:0006:0342:EN:PDF

Directive - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0036

FAQs:
http://europa.eu/rapid/press-release_MEMO-13-690_en.htm?locale=en

Dodd-Frank

At a Glance

Regulation: Dodd-Frank Wall Street Reform and Consumer Protection Act

Regulatory Regime/ Authority: US Government

Target Market Segment: Global financial institutions

Core Data Requirements: Identification of issuers, clients and counterparties

Significant Milestones

December 2, 2009: Dodd-Frank is introduced to Congress

July 21, 2010: Effective date

July 16, 2015: SEC statement on the fifth anniversary of the regulation

Description and Data Requirements

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) is a US government regulation that was introduced in 2010 in an attempt to prevent the recurrence of events that triggered the 2008 financial crisis. The regulation largely covers the swaps market, which was previously unregulated, and is designed to promote the financial stability of the US by improving accountability and transparency in the financial system, monitoring companies deemed 'too big to fail', and protecting taxpayers and consumers from abusive financial services practices.

The extent of the legislation is evidenced by the large number of rules it mandates, most of which have been implemented by the US Securities and Exchange Commission (SEC), along with additional reforms designed to strengthen the nation's financial infrastructure, improve transparency and reduce risk. The SEC is generally charged with regulating security-based swaps, with input from the US Commodity Futures Trading Commission (CFTC), and the CFTC is generally charged with regulating non-security-based swaps, with input from the SEC.

The introduction of such widespread reform raised significant data management challenges for many financial institutions. One major challenge is the requirement to aggregate, analyse and report on large volumes of disparate data from across the financial services industry. The aim of the analysis is to provide better oversight of systemic risk, but with it comes the need to develop data architecture that supports stress testing scenarios designed to promote effective risk management, and timely and accurate reporting.

To support implementation, Dodd-Frank includes guidelines on managing and analysing data from a variety of sources, as well as guidelines on reporting formats. It also introduces a focus on data standardisation across financial markets that is manifested by the inclusion of the Legal Entity Identifier (LEI), a global standard for unique entity identification that is required

Dodd-Frank (cont.)

Dates for Diary

Ongoing: Full implementation – the SEC has completed 67 rule making provisions and has a further four to complete

Key Links

Full Text: https://www.sec.gov/about/laws/wallstreetreform-cpa.pdf

CFTC Final Rules: http://www.cftc.gov/lawregulation/doddfrankact/dodd-frankfinalrules/index.htm

Guidance and Questions: http://www.cftc.gov/LawRegulation/DoddFrankAct/GuidanceQandA/index.htm

by Dodd-Frank not only for reporting, but also as the basis for systemic risk oversight and improved transparency.

Adoption of the LEI has been relatively slow since its introduction in 2012, meaning firms must continue to use a variety of proprietary and data vendor identifiers to access data from different sources of entity data. This presents a significant cross-referencing challenge that will only decrease as adoption and use of the global LEI increases. Implementing the LEI can also be a challenge as data repositories may not be readily extensible and downstream systems that must use the LEI to assess risk and counterparty exposure may need investment to accommodate the identifier.

Dodd-Frank Act stress testing (DFAST) is a forward-looking exercise that is supervised by the Federal Reserve Board and designed to help assess whether institutions have sufficient capital to absorb losses and support operations during adverse economic conditions.

DFAST is complementary to the Comprehensive Capital Analysis and Review (CCAR), an annual exercise carried out by the Federal Reserve to assess whether the largest bank holding companies operating in the US have sufficient capital to continue operations throughout times of economic and financial stress, and have robust, forward-looking capital planning processes that account for their unique risks. DFAST and CCAR are distinct tests, although they do rely on similar processes, data, supervisory exercises and requirements.

EMIR and EMIR II

Description and Data Requirements

European Market Infrastructure Regulation (EMIR) is an EU regulation aimed at improving the transparency of over-the-counter (OTC) derivatives markets and reducing the risks associated with these markets.

To achieve this, EMIR requires OTC derivatives meeting certain requirements to be cleared using a central counterparty (CCP). The CCP must be listed in the European Securities and Markets Authority (ESMA) registry and authorised as described in EMIR so that it is recognised across member states. EMIR also introduces risk mitigation procedures for bilaterally cleared OTC derivatives and requires all derivatives transactions to be reported to a trade repository.

Under EMIR, both counterparties to a trade must ensure that data related to a concluded trade, as well as counterparty data related to the entities involved in the trade, is reported to a trade repository. Both OTC and exchange-traded derivatives must be reported, as well as lifecycle events such as give-ups and terminations. Firms have until the working day following the trade to meet reporting requirements, which presents challenges in ensuring the quality and accuracy of counterparty data, and its timely delivery.

Other reporting issues include the need for firms to conduct an analysis of all their counterparties so that they can fulfil the regulation's classification requirements. This raises data management concerns as firms should aim to maintain an accurate list of counterparties so that they can check their status and track any organisations that are exempt from regulation.

EMIR mandates the use of the Legal Entity Identifier (LEI) and the Unique Trade Identifier (UTI), which is common to both parties to a trade, for reporting to a trade repository. The combination of these identifiers in a complex reporting system

At a Glance

Regulation: European Market Infrastructure Regulation (EMIR)

Regulatory Regime/ Authority: EU

Target Market Segment: Global financial institutions

Core Data Requirements: Client, counterparty and trade identification, reporting

Significant Milestones

August 16, 2012: Effective data

February 12, 2014: First reporting deadline

June 21, 2016: First clearing deadline

September 1, 2016: First margin requirements deadline

EMIR and EMIR II (cont.)

Dates for Diary

December 31, 2016: ESMA to deliver guidelines on trade reporting including Unique Trade Identifiers and Unique Product Identifiers

February 11, 2017: Backloading deadline for OTC contracts entered before August 16, 2012 or after August 16, 2012 and before February 12, 2014 reporting deadline

2017-2019: Additional clearing deadlines phased in

2017-2020: Additional margin requirements phased in

can be difficult to manage. For example, as the LEI is not yet widely adopted, it must be mapped to proprietary and vendor identifiers used in counterparty and client data systems. To ensure correct mapping, many firms are centralising entity data and creating an entity master that will accommodate the LEI alongside other entity identifiers and entity hierarchy data.

The UTI poses different problems as EMIR requires all trades to have a UTI, but provides no standard mechanism for generating and communicating the identifier. The result is that UTIs are based on agreements between trading parties. If agreements are not made, the parties have to deal with reconciliation breaks at the trade repository.

Overall, EMIR reporting includes more than 80 fields with data divided between two tables, one containing data about the trading entity and the other listing common information, such as contract details. This data must be reported on both sides of the trade.

EMIR came into effect on August 16, 2012, with a reporting deadline of February 12, 2014. In August 2014, the regulation introduced a requirement for financial counterparties and non-financial counterparties to provide daily reports on mark-to-market valuations of positions and on collateral value.

The first clearing obligations were introduced in June 2016 for interest rate swaps, with credit default swaps following in February 2017 and all clearing requirements scheduled to be in place by 2019. Large institutions were obligated to meet margin requirements for non-centrally cleared trades in September 2016, with other institutions being phased in to meet margin requirements by September 2020.

Since the introduction of EMIR, ESMA has approved and registered six trade repositories for derivatives processing: DTCC Derivatives Repository, UnaVista, KDPW, Regis-TR, CME TR and ICE Trade Vault Europe. During 2014 and early 2015,

EMIR and EMIR II (cont.)

Key Links

Text Summary:
http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32012R0648

Q&A:
https://www.esma.europa.eu/sites/default/files/library/2016-1176_qa_xix_emir.pdf

Third-Country CCPs:
https://www.esma.europa.eu/sites/default/files/library/third-country_ccps_recognised_under_emir.pdf

Responses to Public Consultation:
https://ec.europa.eu/eusurvey/publication/emir-revision-2015

ESMA authorised 17 European CCPs to offer services in the EU in accordance with EMIR, and in 2015 added 11 third-country CCPs established in Australia, Hong Kong, Japan and Singapore to the list. In 2016, it added a further eight third-country CCPs in South Africa, Canada, Mexico, Switzerland, South Korea and the US.

In accordance with Article 85 of EMIR, the European Commission launched a review of the legislation in May 2015 that could result in EMIR II. The review started with a public consultation that ran from May 21 to August 13, 2015 and a public hearing on the review on May 29, 2015.

The purpose of these activities was to get feedback from stakeholders on their experiences of the implementation of EMIR and provide the European Commission with guidance to prepare a final report. The European Commission is expected to submit a final report to the European Parliament and Council, together with any appropriate proposals for change, in the third or fourth quarter of 2016.

FATCA and GATCA

Description and Data Requirements

The Foreign Account Tax Compliance Act (FATCA) is a US Government regulation that requires foreign financial institutions (FFIs) with US clients to carry the burden of tax reporting for those clients to the US Internal Revenue Service (IRS). FFIs must enter contracts with the IRS and obtain Global Intermediary Identification Numbers (GIINs) through the IRS registration portal. GIIN numbers are used to identify financial entities, counterparties and issuers that are FATCA compliant. FFIs interacting with counterparties that do not have a GIIN, and are therefore not FATCA compliant, can be penalised.

To enforce FATCA regulation, the US Government makes Intergovernmental Agreements (IGAs) with governments in other countries. So far, it has signed 76 Model 1 agreements, which require FFIs to report all FATCA information to their own governmental agencies that then report to the IRS, and eight Model 2 agreements, which require FFIs to report directly to the IRS. Several more countries that have negotiated IGAs, but not yet finalised them, are being treated as having an IGA in place following additional guidance set down by the IRS in April 2014.

FFIs could register with the IRS and gain a GIIN after the official opening of the registration portal on January 1, 2014. The first list of registered FFIs was published on June 2, 2014 and updated monthly thereafter. Withholding tax of 30% on US source income, such as dividends, interest and insurance premiums, was introduced as the regulation became effective on July 1, 2014.

For many firms, FATCA compliance is not an easy task and requires significant investment in data management. FFIs must classify clients using US indicia and determine any Specified US Persons that need to be identified as US tax payers.

As the regulation calls for sensitive client data, such as tax, residency, citizenship and account status information, to be

At a Glance

Regulation: Foreign Account Tax Compliance Act (FATCA)

Regulatory Regime/ Authority: US Government

Target Market Segment: Global financial institutions

Core Data Requirements: Client identification, data maintenance, reporting

Significant Milestones

March 18, 2010: Enacted as part of the US Hiring Incentives to Restore Employment Act

July 1, 2014: Effective date

December 31, 2014: Compliance deadline

March 31, 2015: First reporting deadline

FATCA and GATCA (cont.)

Dates for Diary

March 31, 2017: Next reporting deadline for FFIs in Model 2 IGA jurisdictions

September 30, 2017: Next reporting deadline for FFIs in Model 1 IGA jurisdictions

January 1, 2019: 30% withholding tax on sale after December 31st, 2018 of property producing US source income

Key Links

Overview:
https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca?_ga=1.6517492.797144261.1474889109

Guidance for FFIs:
https://www.irs.gov/businesses/corporations/fatca-regulations-and-other-guidance?_ga=1.206869845.797144261.1474889109

FAQs:
https://www.irs.gov/businesses/corporations/fatcafaqs?_ga=1.237139270.797144261.1474889109

gathered, the data management requirements of compliance include client onboarding, maintaining client data over time and supplementing existing data for reporting. These requirements are best met by integrating FATCA applications with Know Your Customer (KYC), client onboarding and tax systems.

From a data management perspective, dealing with complexities such as grandfathered obligations and material modifications adds to the burden. Grandfathered obligations, essentially obligations that were outstanding on June 30, 2014, are exempt from withholding, but material modifications may mean these obligations lose their exempt status. The data management problem is understanding what constitutes a material modification. While the IRS offers a list of material modifications, it is far from exhaustive and banks must review changes and consider what counts as a material modification.

GATCA

While most firms within the scope of FATCA are now compliant, they face the prospect of a global equivalent of the regulation, referred to as GATCA or Global FATCA. GATCA is based on the Convention on Mutual Administrative Assistance in Tax Matters developed in 1988 by the Organisation for Economic Co-operation and Development (OECD).

GATCA uses a model agreement similar to the FATCA Model 1 IGA and the OECD's Common Reporting Standard for the automatic exchange of tax information between countries.

All G20 countries, most OECD countries and a growing number of developing countries have signed the convention, with many planning to start the exchange of information by September 2017 and the remainder following by September 2018. Unlike FATCA, GATCA does not impose withholding tax on financial institutions that fail to comply, but it does add to the data management challenge already presented by FATCA.

FIDLEG

Description and Data Requirements

FIDLEG, or the Swiss Financial Services Act, is a Swiss Government regulation designed to reshape the regulatory framework governing Swiss financial markets. It covers all types of financial services provided by both regulated and unregulated entities. It also applies to all types of clients and provides investor protection for clients including retail, professional and institutional clients.

The regulation is similar in scope and requirements, particularly around transparency, to the EU's Markets in Financial Instruments Directive II (MiFID II) and will allow Switzerland, a third-country regime in the EU regulatory framework, to continue to access EU financial markets.

Like MiFID II, FIDLEG is based on a comprehensive set of rules of conduct, including a duty to provide information to clients and ensure services and products offered are suitable for them, and an obligation to ensure best execution. To back up the rules, the regulation includes extensive information, documentation and reporting duties.

Information that financial services providers must disclose includes their identity and regulatory status, the services and financial instruments they offer, how they custody financial instruments, and the risks and costs associated with their services, instruments and custody. They must also ensure that clients have access to the Ombudsman in case of disputes.

Documentation duties require financial services providers to document in writing services they agree to provide and the information they collect on a client, any information and warning they give a client under suitability and appropriateness rules, services provided to a client, the needs of a client, and reasons for any recommendation to acquire or sell a financial instrument. There are also new rules on prospectus content and approval inspired by the EU Prospectus Directive.

Organisational obligations require financial services firms to have appropriate organisation and ensure that their employees and any third parties they instruct have appropriate qualifications, knowledge and experience.

Over and above the rules of conduct, financial services providers must handle client orders in good faith and ensure they provide best execution, taking into account financial terms, speed and qualitative factors. To support best

At a Glance

Regulation: FIDLEG (Financial Services Act)

Regulatory Regime/ Authority: Swiss Government

Target Market Segment: Financial institutions

Core Data Requirement: Data aggregation, distribution, reporting

Significant Milestones

February 18, 2013: Federal Department of Finance publishes proposal on FIDLEG

Q2 2014: Consultation opens

October 15, 2014: Consultation closes

November 4, 2015: Federal Council adopts dispatch on FIDLEG, bill ready for parliamentary deliberation

FIDLEG (cont.)

Diary Dates

Q3/4 2016: Expected adoption in Swiss Parliament

January 2018: Expected effective date

Key Links

Proposal:
http://www.news.admin.ch/NSBSubscriber/message/attachments/31593.pdf

execution, firms are required to implement internal policies on how to execute client orders.

FIDLEG also tackles conflicts of interest, particularly conflicts arising out of distribution fees or any other types of retrocessions, which are dealt with under the regulation's organisational measures and disclosures.

Penalties for non-compliance include criminal provisions for breaches of law in connection with prospectuses and basic information documents, illegal offerings of financial instruments, and breaches of the conduct rules.

Finrep

Description and Data Requirements

Financial Reporting (Finrep) forms part of the European Banking Authority's (EBA) supervisory reporting framework and provides a standardised EU-wide framework for reporting financial accounting data. The framework includes several templates, which set out how firms should report data from income statements and balance sheets, and divides the templates into four groups. The groups cover data that must be reported on a quarterly, quarterly with a threshold, semi-annual or annual basis.

In total, Finrep includes more than 50 templates and 6,500 data fields that must be populated with core and non-core quantitative financial data. The data management challenges for firms that must comply with the regulation include sourcing and processing more granular reporting data than has previously been required for reports mandated by local regulators, and reporting more frequently.

Under the regulation, firms must be able to show the workings that lead to final capital positions. They must also consider the dimensions of data. For example, some credit risk returns need to be divided according to geographic areas, counterparties and the like to provide a clear picture of a firm's activities in Finrep reports. In response to this, firms need to conduct a thorough gap analysis, assessing what data is required and how it can be accessed. They also need systems that can convert the data into the XBRL reporting format required by Finrep, a focus on data governance and the oversight that regulators increasingly demand as part of compliance.

Finrep, like Common Reporting (Corep), was introduced in 2014 as part of the Capital Requirements Directive IV (CRD IV), which aims to harmonise reporting across the EU. Finrep provides financial reporting and Corep capital reporting, although Corep is broader than Finrep covering both entity-by-entity and consolidated reporting, while Finrep applies only at the consolidated group level of credit institutions. Despite this, firms in the scope of the regulation must manage a larger reporting burden than in the past and report more frequently.

At a Glance

Regulation: Financial Reporting (Finrep)

Regulatory Regime/ Authority: EBA

Target Market Segment: European financial institutions

Core Data Requirements: Management of financial accounting data, reporting

Significant Milestones

July 26, 2013: Final draft of requirements published

July 1, 2014: Effective date

Dates for Diary

December 31, 2016: Quarterly reporting date

Key Links

Guidelines: http://www.eba.europa.eu/regulation-and-policy/supervisory-reporting

Taxonomy: http://www.eba.europa.eu/documents/10180/502670/COREP+FINREP+XBRL+Taxonomy+v2.0.0.pdf

FRTB

At a Glance

Regulation: Fundamental Review of the Trading Book (FRTB)

Regulatory Regime/ Authority: BCBS

Target Market Segment: Financial institutions

Core Data Requirements: Market risk and capital requirement calculations, reporting

Significant Milestones

May 2012: First consultation paper

October 2013: Second consultation paper

December 2014: Third consultation paper

January 15, 2016: Final text published

Description and Data Requirements

The Basel Committee on Banking Supervision introduced the Fundamental Review of the Trading Book (FRTB) in a May 2012 consultation paper that set out a revised market risk framework and proposals to improve trading book capital requirements. The final FRTB paper was released on January 15, 2016, replacing existing capital requirements for market risk and suggesting a compliance deadline of 2019.

The regulation is a response to the 2008 financial crisis, which exposed fundamental weaknesses in the overall design of the trading book regime, and focuses on a revised internal models approach to market risk and capital requirements, a revised standardised approach, a shift from value at risk to an expected shortfall measure of risk, incorporation of the risk of market illiquidity, and reduced scope for arbitrage between regulatory banking and trading books.

The revised internal models approach introduces a more rigorous model approval process that enables regulators to remove internal modelling permission from individual trading desks and move them back to the standardised approach. The regulation also requires more consistent identification and capitalisation of material risk factors across banks, and adds more constraints to the capital reducing effects of hedging and diversification. There will also be a separate charge for non-modellable risk factors.

FRTB overhauls the standardised approach that will be used for banks that want a simple and straightforward model and is also the fallback for banks that do not get regulatory approval for internal models. The major change to the standardised approach is that it is based on risk sensitivities across asset classes. This should provide a consistent way to measure risk across geographies and regions, and allow regulators to compare risk and aggregate systemic risk.


Clean.
Consistent.
Complete.
Market data intelligence for pricing and valuations
GoldenSource provides powerful market data management, combining intelligence and consistency across pricing models with complete transparency and data lineage.
Deliver robust regulator-ready pricing data for: Valuations and reporting across all regulations including MiFID II, IFRS, AIFMD and Solvency II.
To find out more, visit
thegoldensource.com/MDS

FRTB (cont.)

The replacement of value at risk with an expected shortfall measure of risk is expected to improve the capture of tail risk, essentially the risk of unforeseen events not factored into a bank's model, and understanding of capital adequacy during periods of significant market stress.

The risk of market illiquidity is managed by incorporating varying liquidity horizons in the revised models. These replace the static 10-day horizon assumed for all traded instruments under value at risk in the current market risk framework and are designed to mitigate the risk of a sudden and severe impairment of market liquidity across asset markets.

To reduce arbitrage of regulatory capital between the banking book and the trading book, FRTB imposes a revised boundary between the books. There are also capital disincentives for transfers. Coupled with strict reporting guidelines and regulatory oversight, the regulation should provide a strong framework to govern the boundary between the two books.

While the compliance deadline of FRTB is a few years away, banks need to consider the data management challenges posed by the regulation and begin to review internal systems and controls to ensure they meet the requirements on time.

Dates for Diary

January 2019:
Compliance deadline

Key Links

Text:
https://www.bis.org/bcbs/publ/d352.pdf

GDPR

At a Glance

Regulation: General Data Protection Regulation (GDPR)

Regulatory Regime/ Authority: EU

Target Market Segment: Financial institutions

Core data requirements: Data privacy policies and processes, managing personal data

Significant Milestones

January 25, 2012: European Commission proposes updated data protection regulation

December 15, 2015: European Parliament and Council of the EU agree final text

April 8, 2016: GDPR adopted by Council of the EU

April 14, 2016: GDPR adopted by European Parliament

Description and Data Requirements

General Data Protection Regulation (GDPR) is an EU regulation replacing Data Protection Directive 95/46/EC that was established in 1995. The regulation is designed to harmonise data privacy laws across Europe, protect EU citizens' data privacy and reshape the way organisations across the region approach data privacy.

While GDPR sustains the key principles of data privacy established by the 1995 directive, it extends many of these and clarifies ambiguous territorial applicability set down in the 1995 directive by stating that the regulation applies to all companies processing personal data of data subjects residing in the EU regardless of company location. This means both EU and non-EU based companies processing personal data of data subjects in the EU must comply with the regulation. Organisations located outside the EU must also comply if they offer goods or services to EU data subjects.

The regulation extends data protection requirements to include not only controllers that are within the scope of the 1995 directive and determine the purposes, conditions and means of processing personal data, but also processors that process personal data on behalf of controllers.

GDPR does not make distinctions between industries and sectors, but its extensive demands will have a major impact on the financial services sector and require financial firms to reconsider how they build data management systems and manage personal data. Those that do this well and take a proactive approach to compliance should benefit from improved customer communication, strategic data management and a higher level of trust in the market. For those that breach compliance, the stakes are high – reputational damage and fines of up to 4% of annual turnover or €20 million.

The challenges presented by GDPR include gaining consent to process personal data, building data privacy by design, notifying authorities and individuals of data breaches, ensuring data portability, and giving individuals the right to have data deleted provided there are no legitimate grounds for keeping it. Financial institutions processing large volumes of sensitive data may need to appoint a data protection officer and will have to carry out privacy impact assessments to identify risks, minimise potential data breaches and implement data protection strategy.

GDPR (cont.)

While financial firms subject to the 1995 directive already have data protection policies and practices in place, it is the detail of GDPR that adds complexity and must be addressed to achieve compliance. For example, general contractual terms will no longer be sufficient to provide proof of consent from individuals to process personal data. Instead, consent must be unambiguous, freely given, informed and refer explicitly to each processing purpose. Consent for processing sensitive data held by banks and financial institutions must be explicit. The data management requirement here is to consider how customer data is collected, managed and shared with third parties, and develop appropriate consent management policies.

Financial institutions must also respond to the regulation's enhanced rights for individuals to access, transfer and delete data by amending privacy policies and procedures, and the way in which they manage data access requests. The data privacy by design element requires financial institutions to promote privacy and data protection compliance in new system builds.

GDPR introduces stronger enforcement action if data protection rules are breached, including fines of up to 4% of turnover as mentioned above, and unifies enforcement across the EU with each national supervisory authority authorised to take action. Data breaches at financial institutions that are likely to cause significant damage to customers must be reported to the Data Protection Authority within 72 hours and customers must be notified without undue delay.

GDPR has been some years in the making, but was finally approved by the European Parliament on April 14, 2016. It will take effect in all member states on 25 May 2018, giving financial institutions a window of less than two years to achieve compliance and avoid the heavy fines of non-compliance.

Dates for Diary

May 25, 2018:
Compliance deadline

Key Links

Text:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Summary:
http://www.eugdpr.org/article-summaries.html

FAQs:
http://www.eugdpr.org/gdpr-faqs.html

IFRS

At a Glance

Regulation: International Financial Reporting Standards (IFRS)

Regulatory Regime/ Authority: IASB

Target Market Segment: Global financial institutions

Core Data Requirements: Management of financial statements, reporting

Significant Milestones

January 1, 2013: IFRS 13 takes effect

Description and Data Requirements

The International Financial Reporting Standards (IFRS) are a set of global standards issued by the International Accounting Standards Board (IASB) and designed to support transparency, accountability and efficiency across financial markets.

IFRS comprises 15 published standards, IFRS 1 to IFRS 15, that set out obligations firms must fulfil when issuing financial statements. The obligations cover many aspects of financial reporting including how firms should present cash flows, liabilities, assets, expenses and so on.

The IFRS standards were devised to simplify the reporting process by providing a common set of rules and guidelines for generating reports that can be compared across institutions or with past performance to assess financial strength.

While all IFRS requirements have an impact on the way firms prepare their financial reports, two standards in particular have significant data management implications for financial institutions.

IFRS 9 includes requirements covering the measurement, classification, declassification and hedge accounting of financial assets and liabilities. These requirements can cause a sizeable workload as firms may need to perform impact analysis to identify any changes and adjust accounts accordingly. Using risk data from existing systems can help reduce the burden, as the data can be applied to particular IFRS 9 models, such as the expected loss model for impairment, and support disclosure calculations, saving both time and resources.

IFRS 13 focuses on the definition of 'fair value' and includes guidelines on how firms should conduct valuations, determine fair value and submit corresponding reports. Fair value is defined by IFRS 13 as the exit price, essentially the price that would be received if selling an asset or paid to transfer a liability between market participants on the measurement

IFRS (cont.)

date. Firms need a clear understanding of this market-based measurement to ensure they gather the correct data for accurate reporting and disclosure.

With over 140 jurisdictions requiring IFRS to be used by all or most domestic financial institutions and listed companies, most firms are already compliant, but there are some jurisdictions, most significantly the US, that have yet to implement the standards despite regulatory efforts encouraging universal acceptance. The US, which favours the US GAAP reporting standard, is one of only a handful of jurisdictions that do not require or permit the use of IFRS.

Dates for Diary

January 1, 2018:
IFRS 9 takes effect

Key Links

Guide to IFRS Standards:
http://www.ifrs.org/Use-around-the-world/Documents/2016-pocket-guide.pdf

IFRS 9 Summary:
http://www.ifrs.org/current-projects/iasb-projects/financial-instruments-a-replacement-of-ias-39-financial-instruments-recognitio/Pages/financial-instruments-replacement-of-ias-39.aspx

IFRS 13 Summary:
http://www.ifrs.org/IFRSs/Documents/IFRS13en.pdf

KYC

At a Glance

Regulation: Know Your Customer (KYC)

Regulatory Regime/ Authority: Multiple

Target Market Segment: Global financial institutions

Core Data Requirements: Client identification and classification, ongoing customer data due diligence

Significant Milestones

October 26, 2001: US Patriot Act signed into law

Description and Data Requirements

Know Your Customer (KYC) refers to the process companies must go through to identify and understand clients before conducting financial business with them. It also requires the process to be revisited frequently to ensure information is up to date, complete and correct throughout the lifecycle of a client.

From a regulatory perspective, KYC is an essential element of due diligence and financial regulatory legislation such as anti-money laundering (AML) and countering the financing of terrorism. The process is also part of client onboarding and screening client information against sanctions, politically exposed persons (PEPs) lists and other watch lists.

KYC is not a single regulation, but the term used to describe regulatory requirements around client due diligence that are made and enforced in different countries with different legislative regimes. For example, in the US, the Patriot Act has made KYC mandatory for all banks since 2001. In the UK, the AML regime including KYC is set out in the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 and the Terrorism Act 2000.

As financial crime and fraud – particularly identity theft and concern about the financing of terrorism – have escalated over recent years, so too has the need for financial institutions to improve KYC processes and ensure compliance with local AML and counter-terrorism regulation.

KYC (cont.)

Key Links

US Patriot Act:
http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

UK Proceeds of Crime Act:
http://www.legislation.gov.uk/ukpga/2002/29/contents

UK Money Laundering Regulations:
http://www.legislation.gov.uk/uksi/2007/2157/introduction/made

UK Terrorism Act:
http://www.legislation.gov.uk/ukpga/2000/11/contents

A-Team Group Entity Data Handbook:
http://bit/ly/EntityDataHandbook

KYC presents financial institutions with significant data management challenges, but also opportunities such as standardisation of customer information across an organisation, consistency in the quality of client records, improved customer service and the ability to accelerate client onboarding. It can also deliver significant cost savings through data standardisation, the ability to generate and manage one view of a customer across an organisation, and the efficient management of KYC documentation for purposes such as client onboarding.

The data management process requires banks to gather information from clients, often using paper documents, and then identify and correctly classify the clients according to their circumstances, including country of origin, business type, source of assets and income, types and purpose of transactions, and amount of funds. This information needs to be kept up to date and must be submitted to regulators on a frequent basis, meaning banks need to continually reassess their KYC procedures and increase the automation of their processes.

In many cases, due to the complexity of KYC, firms need to do more than keep a central repository of entity data and track audit trails. They may need to link KYC to customer data due diligence, enhanced due diligence and entity hierarchy data to gain an understanding of clients' relationships with other entities and ensure compliance and effective risk management.

In an increasingly hostile environment, client screening is an important part of KYC. It requires client data to be checked against financial sanctions, trade embargoes, PEPs and other watch lists to detect whether an order has been made to prohibit clients from carrying out particular transactions.

KYC also plays a role in client onboarding, a process that was traditionally manual and suboptimal for both clients and banks, but which is now being automated. Regulation is a driver here, along with tough competition to win clients and sustain their loyalty. These factors are leading financial institutions to

KYC (cont.)

readdress their onboarding and offboarding processes, and adopt automated technology solutions that can deliver business benefits as well as compliance.

Considering the extent of KYC and client onboarding, the sheer volume of documentation and data that banks must manage on an ongoing basis is daunting. But solutions are available, including managed services that build and maintain client records on behalf of financial institutions, and shared services, or utilities, that use a one-to-many model to gather, validate and update client data once for the benefit of numerous institutions that are subscribers to the service. Machine learning solutions that automate data collection for onboarding and KYC compliance are emerging.

Beyond compliance requirements, a further consideration is how KYC and client onboarding can be integrated with account and settlement data. If an holistic approach is taken to onboarding a client and managing the client's account and settlement data, firms can move quickly from initiating clients to trade readiness.

While KYC requirements vary between countries depending on specific legislation, regulation and policy, most countries with AML concerns have had KYC rules in place since the early 2000s, although it is only in recent years that regulators have clamped down and issued significant fines for non-compliance, prompting major financial institutions to rethink their KYC processes and get them up to speed.

As well as addressing local AML requirements, improvements in KYC processes can help firms comply with international regulations such as Dodd-Frank and the US Foreign Account Tax Compliance Act (FATCA). KYC compliance is also central to Markets in Financial Instruments Directive II (MiFID II).

MAR and MAD

At a Glance

Regulation: Market Abuse Regulation (MAR) and Directive on Criminal Sanctions for Market Abuse (or MAD)

Regulatory Regime/ Authority: EU

Target Market Segment: Global financial institutions

Core Data Requirements: Data transparency to detect and prevent market abuse

Significant Milestones

July 1, 2005: MAD implemented

December 12, 2012: MAR text approved by European Council

September 10, 2013: MAR endorsed by European Parliament

July 2, 2014: Effective date

July 3, 2016: Compliance deadline

Description and Data Requirements

Market Abuse Regulation (MAR) strengthens EU rules on market integrity and investor protection that were first adopted in the 2003 Market Abuse Directive (MAD).

The regulation aims to challenge insider dealing and market manipulation in Europe's financial markets and is part of an updated EU rulebook that also includes the Directive on Criminal Sanctions for Market Abuse (also known as Market Abuse Directive, or MAD). MAR has been applicable since July 3, 2016.

Many of the provisions in MAR are the same as those in the initial MAD directive, but the regulation extends the scope of previous rules to include new trading platforms and technologies, and commodity and related derivatives markets. It also bans the manipulation of benchmarks and reinforces the investigative and sanctioning powers of regulators.

Where MAD applied to financial instruments admitted to trading on an EU regulated market, MAR includes instruments traded on a multilateral trading facility (MTF) or organised trading facility (OTF). Market manipulation is extended to cover any behaviour, not just transactions and orders to trade, that may give a false or misleading signal, while the regulation also adds attempted market manipulation in the sense of trying to manipulate the market without trading.

Market manipulation provisions are extended to instruments with values related to traded instruments and to spot commodity contracts related to financial or derivatives markets.

MAR expands the definition of insider dealing, which MAD described as non-public information likely to have a serious impact on an instrument's price, to include information that a reasonable investor is likely to use as the basis for investment decisions.

In terms of extended coverage, MAR includes benchmarks and emission allowances, as well as algorithmic and high frequency trading that is undertaken without an intention to trade, but with an intention to disrupt or delay a trading system.

From a data management perspective, MAR requires firms to review policies and processes to ensure instruments, trading platforms and technologies within its scope are compliant.

MAR and MAD (cont.)

To avoid sanctions for trading on inside information or spreading false rumours in the market, both individual investors and firms need documentation to verify that they are adhering to the regulation and prove that any transgressions are not intentional.

The Directive on Criminal Sanctions for Market Abuse (or MAD) complements MAR by requiring member states to introduce common definitions of criminal offences of insider dealing and market manipulation, and to impose criminal penalties for market abuse offences.

Key Links

Text:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0596

Summary:
http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32014R0596

MAR FAQs:
http://europa.eu/rapid/press-release_MEMO-13-774_en.htm

MAD FAQs:
http://europa.eu/rapid/press-release_MEMO-14-78_en.htm

Margin Requirements – BCBS/IOSCO

At a Glance

Regulation: Margin requirements for non-centrally cleared derivatives

Regulatory Regime/ Authority: BCBS and IOSCO

Target Market Segment: Global financial institutions

Core Data Requirements: Margin calculation

Significant Milestones

September 2, 2013: Initial framework

March 18, 2015: Revised framework

September 1, 2016: Initial and variation margin deadline for large market participants

Description and Data Requirements

The framework for margin requirements for non-centrally cleared derivatives has been developed by the Basel Committee on Banking Supervision (BCBS) and the International Organization of Securities Commissions (IOSCO). The framework sets out international policy on minimum standards for margin requirements for non-centrally cleared derivatives and provides a global benchmark for local regulatory requirements. It was initially released in September 2013 and later revised in March 2015.

The framework is designed to reduce systemic risk related to over-the-counter (OTC) derivatives markets and provide firms with incentives for central clearing, while managing the overall liquidity impact of the margin requirements. Standards within the framework align with collateral requirements for non-centrally cleared derivatives set out in European Market Infrastructure Regulation (EMIR) and require all financial firms and systemically important non-financial entities that engage in non-centrally cleared derivatives transactions to exchange initial and variation margin in line with the counterparty risks arising from the transactions.

The liquidity impact of the margin requirements is addressed through the introduction of a universal initial margin threshold of €50 million, below which a firm has the option of not collecting initial margin. The framework also allows for a broad array of eligible collateral to satisfy initial margin requirements with a view to further reducing the liquidity impact.

From a data management perspective, the requirements go beyond existing market practice on margining and mean firms must make significant changes to infrastructure, systems and processes, particularly in areas that support initial margin calculations, the exchange of collateral and risk management.

Margin Requirements – BCBS/IOSCO (cont.)

The original framework released in September 2013 was the result of two public consultations and a quantitative impact study. It set out a phased four-year implementation of the requirements starting with the collection and posting of initial margin on non-centrally cleared derivatives from December 1, 2015. The March 2015 revision of the framework pushed this deadline forward to September 1, 2016 and added a nine-month delay to the complete four-year phase in.

Dates for Diary

March 1, 2017: Variation margin deadline for market participants that are not large

September 1, 2017 – 2020: Initial margin deadline phased in for all market participants

Key Links

Text: http://www.bis.org/bcbs/publ/d317.pdf

Summary of revisions: http://www.bis.org/bcbs/publ/d317_summarytable.pdf

Consultation document: http://www.bis.org/publ/bcbs242.htm

MiFID II

At a Glance

Regulation: Markets in Financial Instruments Directive II (MiFID II)

Regulatory Regime/ Authority: EU

Target Market Segment: Global financial institutions

Core Data Requirements: Pre- and post-trade data transparency, client and counterparty identification, transaction reporting

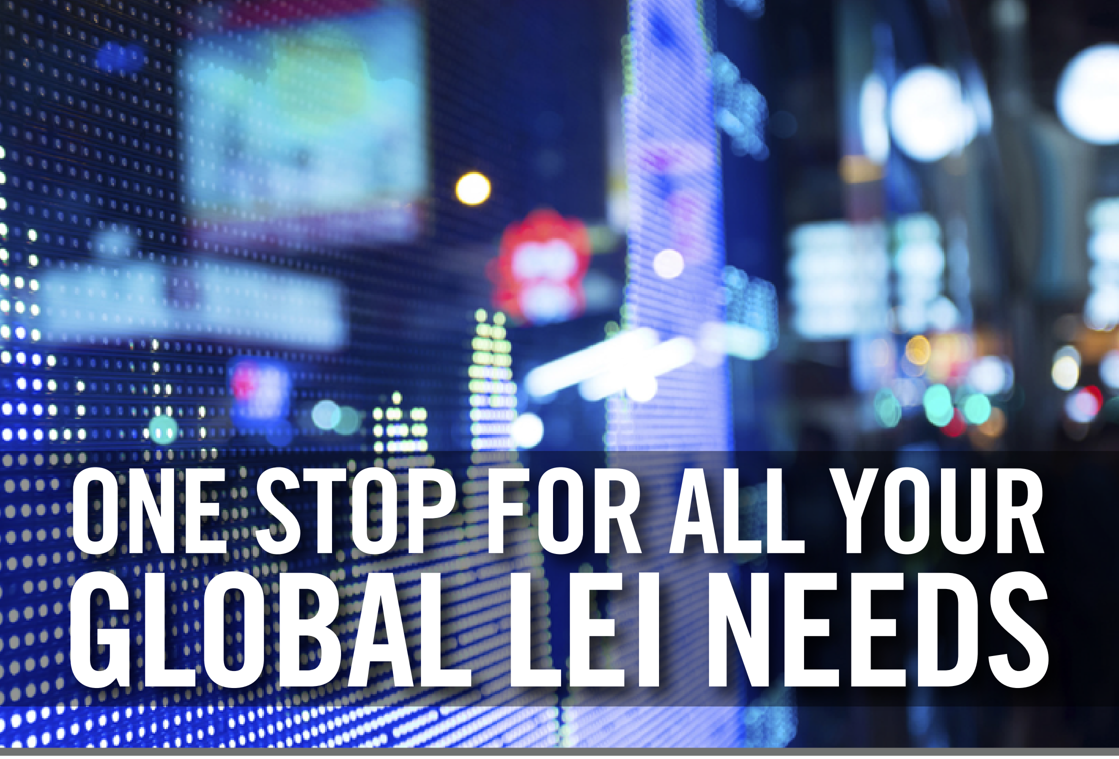
Description and Data Requirements

Markets in Financial Instruments Directive II (MiFID II) is a principles-based directive issued by the EU. It is much broader than MiFID, which was introduced in 2007, and aims to improve the competitiveness of European markets by creating a single market for investment services and activities, and ensuring harmonised protection for investors in financial instruments.

The directive was initially scheduled to take effect in January 2017, but in February 2016 the European Commission proposed extending the deadline to January 2018 after being informed by the European Securities and Markets Authority (ESMA) that technical implementation challenges meant neither regulators nor market participants would have systems ready in time to meet the January 2017 deadline. In June, the European Parliament confirmed the extended deadline.

MiFID II amends many existing provisions covering the conduct of business and organisational requirements for providers of investment services, and specifies requirements and organisational rules that must be applied to different types of trading venues. It also makes sweeping changes to the pre- and post-trade transparency of EU financial markets.

Current MiFID rules, which are limited to equities trading on regulated platforms, are extended to cover equity-like and non-equity instruments traded on any trading platform, such as


ONE STOP FOR ALL YOUR
GLOBAL LEI NEEDS

MiFID II (cont.)

Significant Milestones

November 1, 2007: MiFID takes effect

October 20, 2011: European Commission publishes draft proposals for a directive and regulation to revise MiFID

October 26, 2012: European Parliament approves MiFID II

May 13, 2014: EU Council adopts Level 1 text

July 2, 2014: MiFID II enters into force

28 September, 2015: ESMA publishes final report on Regulatory and Implementing Technical Standards

February 10, 2016: European Commission proposes one-year delay

June 7, 2016: European Parliament confirms delay

a multilateral trading facility (MTF) or organised trading facility (OTF), with a view to ensuring that all trading takes place on regulated platforms. Systematic internalisers and other investment firms that trade over the counter will also be subject to expanded pre- and post-trade transparency obligations.

MiFID II details a framework for market data that includes standards, such as ISINs for securities identification and reporting, and will act as a basis for the publication of data to a consolidated tape.

The data management challenges of MiFID II are many and data managers have welcomed the delay in the directive's deadline, although they continue to press on with implementation programmes as the timeframe for completion remains tight.

Changes to improve investor protection and intermediary proposals that seek to reduce instrument complexity raise data issues that firms need to consider when working to achieve compliance. Firms must reach agreement on common data processes and data quality metrics, requirements that reflect the push towards data standards and data consolidation that has been core to the reform process since early drafts of the MiFID II proposal. They must also manage multiple identifiers, including industry standard Market Identifier Codes (MICs) and Legal Entity Identifiers (LEIs).

The directive mandates a move to faster publishing of post-trade transaction data to local competent authorities, reducing the

Financial Instrument Global Identifier (FIGI)

The Only Open Data Standard for Identifying Financial Instruments Across The Globe.

Data Quality. Convergence. Regulatory pressures.

You shouldn't have to worry about instrument symbology, or how and when you use it. FIGI closes the gap in existing symbology systems by providing uniqueness and standardization at multiple levels of granularity, as well as covering instruments that traditional symbology struggles to address. All based upon the core principles of open data – free to use, free to issue, free to redistribute.

Visit **OpenFIGI.com** or contact **support@OpenFIGI.com** with inquiries regarding FIGI integration

OpenFIGI

MiFID II (cont.)

Dates for Diary

July 3, 2017: Deadline for EU countries to implement directive in local legislation

December 2016: ESMA due to deliver four sets of guidelines and recommendations

January 3, 2018: Effective date

Key Links

Text: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0065

Summary: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32014L0065

FAQs: http://europa.eu/rapid/press-release_MEMO-14-305_en.htm

time delay from three minutes to one minute. This move to near real-time reporting is likely to require investment in underlying data architecture and will put pressure on firms' abilities to retrieve supporting reference data from repositories quickly and accurately.

The expansion of MiFID II beyond equity markets extends transparency requirements to sectors such as depository receipts, exchange-traded funds and company certificates. Reporting in non-equity markets will require transaction-based post-trade transparency, with the provision of price, volume, time of trade and reference characteristics of data remaining the primary consideration.

The directive's proposal to introduce a consolidated tape as a means of aggregating data and providing the ability to compare instrument prices across different venues could also be a data management headache and highlight issues around data standardisation, availability, quality and timeliness.

MiFID II introduces controls for algorithmic trading that are designed to provide safeguards and reduce systemic risk, and include regulation of algorithmic traders, including high frequency algorithmic traders, and their market making strategies.

MiFID II has been a long time in the making and the subject of many industry consultations along the way, but firms within its scope now have just over a year to achieve compliance.

MIFIR

Description and Data Requirements

Markets in Financial Instruments Regulation (MiFIR) is an EU regulation associated with the Markets in Financial Instruments Directive II (MiFID II) that aims to harmonise the trading of securities and improve investor protection across Europe. While MiFID II focuses on market infrastructure, MiFIR builds out transaction reporting requirements with a number of new reporting obligations and complements the directive's commitment to trading data transparency.

MiFIR, along with MiFID II, was initially scheduled to take effect in January 2017, but in February 2016 the European Commission proposed extending the deadline to January 2018 after being informed by the European Securities and Markets Authority (ESMA) that technical implementation challenges meant neither regulators nor market participants would have systems ready in time to meet the January 2017 deadline. In June, the European Parliament confirmed the extended deadline.

Under MiFIR, instruments that must be reported include all derivatives admitted to regulated markets, including currently exempt commodity, foreign exchange and interest rate derivatives, all instruments on multilateral trading facilities (MTFs) and organised trading facilities (OTFs), and all instruments that could change the value of instruments trading on any of these venues.

The regulation adds a number of fields to transaction reports, including fields designed to help spot short-selling traders, and trader and algorithm fields designed to identify the individual or program executing a transaction.

The regulation's requirements are likely to have a significant impact on data management processes as they expand the initial reporting requirements of MiFID to a much broader range of instruments. This means firms must ensure access to accurate, timely and verified data associated with the instruments. They must also extend the number of fields required for transaction reporting and use Legal Entity Identifiers (LEIs) to identify issuers or trading venue operators.

Like MiFID II, MiFIR mandates data transparency. Most of its transparency requirements are around post-trade data processes, but it does cover some pre-trade transparency requirements, such as equal access to trading opportunities data. The regulation's post-trade transparency requirements call for alterations to the trading environment as data such as

At a Glance

Regulation: Markets in Financial Instruments Regulation (MiFIR)

Regulatory Regime/ Authority: EU

Target Market Segment: Global financial institutions

Core Data Requirements: Pre- and post-trade data transparency, transaction reporting

Significant Milestones

December 2010 – February 2011: Public consultation on MiFID review

October 20, 2011: European Commission publishes draft proposals for a directive and regulation to revise MiFID

October 26, 2012: European Parliament approves MiFID II/MiFIR

May 13, 2014: Council of the EU adopts Level 1 text

July 2, 2014: MiFIR enters into force

MIFIR (cont.)

Dates for Diary

January 3, 2018:
Effective date

Key Links

Text:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN

prices, quotes, execution times and volumes must be published publicly. The extension of transaction reporting to additional asset classes means firms must submit more information to regulatory authorities.

Provisions in MiFIR aimed at reducing disruptive trading, speculative activity and systemic risk mean firms need to be aware of rules covering these issues that are in place in the markets in which they operate, not least because of the powers given to regulators and venue managers to interfere should rules be violated.

Commodity derivatives, in particular, face significant scrutiny under MiFIR and are subject to new position limits, transparency requirements and measures to reduce price volatility. These requirements are designed to give regulators greater oversight and authority in the market.

NIS

Description and Data Requirements

The Network and Information Security (NIS) Directive is the first piece of consolidated European legislation on cybersecurity. Its provisions aim to make the online environment more trustworthy and better able to support the smooth functioning of the EU Digital Single Market.

The directive is based on proposals that were put forward by the European Commission in 2013 and designed to ensure a high, common level of network and information security across the EU. In 2015, the European Parliament and Council agreed measures to boost the overall level of cybersecurity in the EU. The European Parliament adopted the NIS Directive on July 6, 2016 and it took effect in August 2016. Member states have 21 months from August 2016 to transpose the directive into national law.

The rules of the directive aim to improve cybersecurity capabilities in member states and improve member states' cooperation on cybersecurity. To facilitate an improvement in national cybersecurity capabilities, the directive requires a minimum level of NIS capabilities based on member states adopting a national NIS strategy that defines strategic objectives, appropriate policy and regulatory measures relating to cybersecurity.

Member states are also required to designate a national competent authority for the implementation and enforcement of the directive, as well as Computer Security Incident Response Teams (CSIRTs) that are responsible for handling incidents and risks.

To improve cooperation on cybersecurity, the directive creates a cooperation group between member states that is designed to facilitate strategic cooperation, exchange of information and development of trust and confidence. The group also networks national CSIRTs to promote swift and effective operational cooperation on specific cybersecurity incidents and to share information on risks.

The directive covers operators of essential services in the banking, financial market infrastructure, energy, transport, healthcare and digital infrastructure sectors, as well as providers of key digital services, such as cloud computing, search engines and online marketplaces. It requires them to take appropriate security measures and report serious incidents to relevant national authorities.

At a Glance

Regulation: Network and Information Security (NIS) Directive

Regulatory Regime/ Authority: EU

Target Market Sector: Global financial institutions

Core Data Requirements: Security, reporting

Significant Milestones

February 7, 2013: Initial European Commission proposal on cybersecurity

December 7, 2015: European Parliament and Council agree proposal

July 6, 2016: European Parliament adopts directive

August 2016: Enters into force

Dates for Diary

June 2018: Compliance deadline

Key Links

Text: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Press release: http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm

PRIIPs

At a Glance

Regulation: Packaged Retail and Insurance-based Investment Products (PRIIPs)

Regulatory Regime/ Authority: EU

Target Market Segment: Providers of retail investment and insurance products

Core Data Requirement: Data aggregation, maintenance, distribution

Significant Milestones

July 3, 2012: European Commission proposes legislation

November 26, 2014: European Council publishes regulation

November 11, 2015: Consultation paper on draft RTS

March 31, 2016: Final RTS published

June 30, 2016: RTS adopted by European Commission

September, 2016: RTS rejected by European Parliament

Description and Data Requirements

Packaged Retail and Insurance-based Investment Products (PRIIPs) is an EU regulation designed to avoid the sale of unsuitable investment and insurance products to consumers and, instead, provide them with clear product information they can use to understand and compare products before they invest. This information is contained in a Key Information Document (KID) that must be provided by PRIIP manufacturers for all products within the scope of the regulation.

The regulation covers firms manufacturing PRIIPs, which include investment funds, insurance investment products and structured products such as deposits and securities, but not general insurance and protection-based life insurance policies, deposits exposed only to an interest rate and other products that carry no investment risk, directly held shares and bonds, and pensions.

Although Undertakings for Collective Investment in Transferable Securities (UCITS) meet the definition of PRIIPs, the existing UCITS Directive contains a requirement for Key Investor Information Documents that are similar to KIDs. On this basis, the regulation gives UCITS providers a transitional period up to December 31, 2019, during which they will be exempt from PRIIPs.

The KID must be created before the PRIIP is made available to retail investors and must be published on the product manufacturer's website and provided on paper in face-to-face PRIIP sales. The document is limited in length to three A4 pages, must be presented in a way that is fair, clear and not misleading, and must contain only information needed by investors. It must promote comparability of products, explain the purpose of the KID, detail the product manufacturer and its regulator, and include mandatory sections such as 'What is the product?', 'What are the risks and what could I get in return', 'What are the costs?', and 'How long should I hold it and can I take money out early?'.

For PRIIPs manufacturers that must produce a KID for every product they promote, the data management requirement is considerable, leading some firms to review their range of products and many to consider working with third-party service providers to support the production and distribution of KIDs. Penalties for non-compliance include liability for damages if investors lose money.

PRIIPs (cont.)

While PRIIPs is due to take effect on December 31, 2016, the compliance deadline could be delayed following the rejection of Level 2 Regulatory Technical Standards (RTS) by the Economic and Monetary Affairs (ECON) Committee of the European Parliament on September 1, 2016, and a further rejection by the European Parliament a couple of weeks later.

The European Parliament has called on the European Commission to consider postponing the application date of the Level 1 regulation so that is does not enter into force without the RTS. What the Commission will do next is not yet clear. It could adopt new RTS taking into account the objections of the European Parliament and take these to a further parliamentary vote in October 2016.

Alternatively, it could propose to postpone the Level 1 regulation, or it could do nothing. The latter is unlikely, but would lead to no change to the December 31, 2016 deadline as the European Parliament alone cannot initiate a formal delay of the regulation or force the European Commission to postpone the date.

Dates for Diary

December 31, 2016:
Effective date

December 31, 2019:
UCITS regulated by PRIIPs

Key Links

Text:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R1286

Summary:
http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32014R1286

FAQs:
http://europa.eu/rapid/press-release_MEMO-14-299_en.htm

SEC Form PF

At a Glance

Regulation: Form Private Fund (Form PF)

Regulatory Regime/ Authority: SEC

Target Market Segment: Private funds

Core Data Requirements: Classification, stress testing, reporting

Significant Milestones

March 31, 2012: Full implementation

June 15, 2012: Compliance for firms with more than $5 billion AUM

December 31, 2012: Compliance for all firms with more than $150 million AUM

Description and Data Requirements

Form Private Fund (Form PF) is a US Securities and Exchange Commission (SEC) rule that details reporting standards for private funds and is designed to provide a view of the risk exposure of the assets in the funds.

Under Form PF, fund advisers are required to report regulatory assets under management to the Financial Stability Oversight Council, an organisation created under the Dodd-Frank Wall Street Reform and Consumer Protection Act to assess risk in financial markets.

SEC registered investment advisers, commodity pool operators and commodity trading advisers with $150 million or more under management are subject to the rule and must regularly submit a Form PF. Further requirements depend on the size and type of fund. Large private fund advisers are classified as those with more than $1.5 billion of assets under management (AUM), advisers with more than $2 billion in private equity funds, and liquidity fund advisers with more than $1 billion in combined assets. Anything smaller is classified as a small private fund adviser.

Small fund advisers must submit an annual Form PF including basic information. Large fund advisers must report more information, with private equity funds filing annually and hedge and liquidity funds filing on a quarterly basis.

Form PF requires a significant data management effort, including gathering, identifying, verifying and storing data that is essential to filling out the form correctly. Firms need to focus on reliable and easy access to the data, whether it is held internally or by external service providers, and they must understand the definitions and classifications of Form PF. Form PF also includes a number of stress tests that must be reported and requires firms to prove that reported data is accurate and consistent with other regulatory filings.

SEC Form PF (cont.)

Institutional investors may request access to Form PF information in order to assess their investment decisions, risk profiles and due diligence efforts, meaning firms must determine how they gather and present information for both investors and regulators.

Form PF came into effect on June 15, 2012, with the largest funds (more than $5 billion AUM) having to meet compliance immediately. Smaller funds (with more than $150 million AUM) had until December 31, 2012 to comply.

Dates for Diary

November 29, 2016, March 1, 2017: Next filing dates for large fund adviser

December 31, 2016: Next filing date for all other advisers

Key Links

Full Text:
http://www.sec.gov/rules/final/2011/ia-3308-formpf.pdf

FAQs:
http://www.sec.gov/divisions/investment/pfrd/pfrdfaq.shtml

Section 871(m)

At a Glance

Regulation: Section 871(m) of the Internal Revenue Code

Regulatory Regime/ Authority: US Internal Revenue Service

Target Market Sector: Global financial institutions

Core Data Requirements: Identifying dividend equivalents, tax withholding, reporting

Significant Milestones

2012: IRS issues temporary and proposed regulations

September 17, 2015: IRS issues final regulations

Description and Data Requirements

Section 871(m) of the Internal Revenue Code is a set of regulations drawn up by the US Treasury Department and Internal Revenue Service (IRS). It governs withholding on certain notional principal contracts, derivatives and other equity-linked instruments (ELIs) with payments that reference (or are deemed to reference) dividends on US equity securities.

The regulations, which generally apply to transactions issued on or after January 1, 2017, impose up to 30% withholding tax on certain amounts arising in derivative transactions over US equities when those amounts are paid to non-US persons.

The regulations are a response to concerns about non-US persons dodging withholding tax on US securities' dividend payouts by using carefully timed swaps and other equity derivatives. These result in a dividend equivalent.

A dividend equivalent is defined in the regulations as: any substitute dividend made pursuant to a securities lending or a sale-repurchase transaction that directly or indirectly is contingent upon, or determined by reference to, the payment of a dividend from sources within the US; any payment made pursuant to a specified notional principal contract (specified NPC) that directly or indirectly is contingent upon, or determined by reference to, the payment of a dividend from sources within the US; and any other payment determined by the IRS to be substantially similar.

A specified NPC is defined to include any NPC if: in connection with entering into such contract, any long party to the contract transfers the underlying security to any short party to the contract; in connection with the termination of such contract, any short party to the contract transfers the underlying security to any long party to the contract; the underlying security is not readily tradable on an established securities market; in connection with entering into such contract, the underlying security is posted as collateral by any short party to the contract with any long party to the contract; or such contract is identified by the IRS as a specified NPC.

The IRS issued temporary 871(m) regulations in 2012, provided amended proposed regulations in 2013 and issued final regulations on September 17, 2015.

Equity-linked investments (ELIs) that fall within the scope of the regulations include swaps, options, futures, convertible

Section 871(m) (cont.)

debt, structured notes and other customised derivative products. Amending previous proposals, the final regulations make ELIs subject to tax withholding if the delta, or ratio of change to the fair market value, is 0.80 or greater, with delta calculated when the equity derivative is issued.

Dates for Diary

January 1, 2017:
Regulations take effect for transactions entered into on or after January 1, 2017. Regulations also apply to any payment of a dividend equivalent made on or after January 1, 2018 as a result of transactions entered into on or after January 1, 2016 and before January 1, 2017

Key Links

Final regulations:
https://www.irs.gov/irb/2015-41_IRB/ar07.html

SFTR

At a Glance

Regulation: Securities Financing Transactions Regulation (SFTR)

Regulatory Regime/ Authority: EU

Target Market Segment: Investment fund managers

Core data requirements: Client, counterparty and trade identification, reporting

Significant Milestones

September 2013: EU action plan on shadow banking

January 2014: European Commission proposes SFT regulation

January 12, 2016: Effective date

Dates for Diary

January 12, 2017: ESMA to publish Level 2 RTS

Q1 2018: SFT reporting starts

Key Links

Text:
http://ec.europa.eu/internal_market/finances/docs/shadow-banking/140129_proposal_en.pdf

FAQs:
http://europa.eu/rapid/press-release_MEMO-15-5931_en.htm

Description and Data Requirements

Securities Financing Transactions Regulation (SFTR) is an EU regulation and part of a drive by the EU to increase transparency of activities that are broadly categorised as shadow banking. The regulation is designed to highlight transactions that could pose a significant level of systemic risk and specifically sets out requirements to improve market transparency of securities financing transactions (SFTs).

SFTs are typically transactions that use securities to borrow cash, or vice versa. They include securities and commodities lending, margin lending and repurchase agreements. Total return swaps are also covered by some of the regulation's disclosure requirements.

To achieve improved transparency, SFTR requires all SFTs and associated collateral to be reported to an EU registered trade repository, making the transactions visible to relevant EU regulators.

The regulation permits collateral reuse, but only when the collateral provider has given explicit consent in writing. It also mandates fund managers to disclose policies on the use of SFTs and total return swaps to their investors in both pre-investment documents and ongoing periodical reports.

SFTR came into effect on January 12, 2016, although transaction reporting is not expected to start until 2018. The regulation's scope is broad, covering SFTs made by firms established in the EU, SFTs made by EU branches of non-EU firms, and SFTs where securities used are issued by an EU issuer or by an EU branch of a firm.

The regulation explicitly identifies Undertakings for Collective Investment in Transferable Securities (UCITS) funds and Alternative Investment Fund Management (AIFM) funds as being within its scope, but its reach means any firm engaging in SFTs will have to review workflows and upgrade data management systems to fulfil the transaction reporting obligation.

Final details of reporting have not yet been published, but they are due to be provided by the European Securities and Markets Authority (ESMA) to the European Commission in Level 2 draft Regulatory Technical Standards (RTS) by January 12, 2017. Reporting is expected to follow existing European Market Infrastructure Regulation (EMIR) derivatives reporting and will require the use of Legal Entity Identifiers (LEIs) to identify counterparties and beneficial owners of parties using LEIs. Electronic platform providers must issue unique transaction identifiers to identify SFTs.

Solvency II

Description and Data Requirements

Solvency II is an EU directive that aims to harmonise European insurance regulation and create a unified and stable industry driven by risk and solvency requirements. It is designed to protect consumers, improve regulatory supervision and increase the competitiveness of European insurers in international markets.

The regulation is principles based, complex and broad in scope, covering not only insurers and reinsurers, but also asset managers and asset servicers. It is broken down into three pillars covering: capital requirements, including a solvency capital requirement based on an internal or standard model and a minimum capital requirement; governance and supervision, including effective risk management and an internal Own Risk and Solvency Assessment; and public disclosure and regulatory reporting on a quarterly and annual basis.

While insurers bear the greatest burden of data management under Solvency II and must manage both existing and new data, such as the Complementary Identification Code (CIC) for asset classification, Nomenclature Statistique des Activités Economiques dans la Communauoté Européenne (NACE) for industry classification, and the Legal Entity Identifier (LEI) for entity identification, the burden carried by asset managers and asset servicers is not insignificant.

Under the regulation's 'look through' component, asset managers and servicers must provide transparency on the investments they hold on behalf of insurance company clients in accordance with technical standards outlined by the European Insurance and Occupational Pensions Authority (EIOPA). The standards, which cover both asset data and risk data, include quality requirements of complete, timely, accurate and appropriate data.

Asset managers and servicers must also provide granular information on entities issuing securities and the component

At a Glance

Regulation: Solvency II

Regulatory Regime/ Authority: EU and EIOPA

Target Market Segment: Insurance companies and their service providers

Core Data Requirements: solvency capital calculation, risk management, governance, reporting

Key Links

Text: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02009L0138-20140523

Timeline: https://eiopa.europa.eu/regulation-supervision/insurance/solvency-ii

FAQs: http://europa.eu/rapid/press-release_MEMO-15-3120_en.htm

Dates for Diary

October 2016: next quarterly reports

January 2017: Next annual reports

Solvency II (cont.)

Significant Milestones

November 10, 2009: Adoption by European Council

March 14, 2014: Omnibus II vote revises the Solvency II directive

January 18, 2015: Enters into force

January 31, 2015: Deadline for transposing Solvency II rules into national law

June 2015: Preparatory phase annual reporting

November 2015: Preparatory phase quarterly reporting

January 1, 2016: Effective date

April 2016: First reporting

elements of derivative instruments. It is expected that some asset managers will divest asset classes that do not have the underlying performance data required for Solvency II compliance and instruments that create a large capital charge and are perceived by insurers as disadvantageous in terms of solvency capital requirements.

With data management requirements running through the principles and pillars of Solvency II, insurers are likely to source data for compliance purposes from both internal and external sources, often consolidating data from a number of data vendors to generate required data sets and always seeking to input consistent data across the three pillars of the regulation.

Easing the burden of 'look through' data flow between insurers and asset managers is a tripartite template, developed by the Investment Association in the UK, BVI in Germany and Club Ampere in France, and providing a common template to support the exchange of data.

The compliance deadline for Solvency II was January 1, 2016, but many firms are still using some manual workarounds and most have yet to complete automated solutions.Overcoming the challenges of the regulation can deliver not only compliance, but also opportunities of reduced capital requirements, improved risk management, a clearer link between capital and risk to support business decisions and a sturdy compliance platform.

UCITS

At a Glance

Regulation: UCITS V

Regulatory Regime/ Authority: EU

Target Market Segment: European fund managers and depositories

Core Data Requirements: Asset management, reporting

Significant Milestones

1985: First UCITS Directive

July 1, 2011: UCITS IV takes effect

September 17, 2014: UCITS V implemented

March 18, 2016: UCITS V takes effect

Key Links

Text: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0091

FAQs: http://europa.eu/rapid/press-release_MEMO-14-298_en.htm?locale=en

Description and Data Requirements

Undertakings for Collective Investment in Transferable Securities (UCITS) are investment funds regulated at EU level on the basis of regulations issued by the European Commission. UCITS V is the most recent UCITS directive and aims to increase the level of protection already offered to investors in UCITS and to improve investor confidence in them. It plans to do this by enhancing the rules covering the responsibilities of depositaries and by introducing remuneration policy requirements for UCITS fund managers.

The first UCITS directive was implemented in 1985 and has since been improved incrementally as well as by a major overhaul in 2009 that created UCITS IV, which came into effect in July 2011. The UCITS V directive was implemented in September 2014 and took effect in March 2016.

The changes made in UCITS V include a requirement to appoint a single depositary for each UCITS, publication of a list of entities eligible to act as depositaries, harmonisation of the duties of a depositary to keep the assets of the UCITS safe, monitoring cash movements to and from the fund, and overseeing the fund manager's performance of its key functions. The directive also specifies safe-keeping requirements that a depositary needs to comply with in respect of financial instruments.

To avoid financial loss, the directive requires member states to ensure that assets held in custody by a depositary are protected in the event of the depositary becoming insolvent. Similarly, the depositary is liable for the avoidable loss of a financial instrument held in custody.

A further requirement is the need for UCITS management companies to have transparent remuneration policies covering key staff. The directive also aims to harmonise different approaches to sanctioning across the EU by introducing a range of sanctions, including minimum and maximum penalties, that can be imposed by EU regulators for breaches of the directive.

In terms of data management, UCITS V tightens the rules issued in previous directives and calls on depositories to improve their understanding and visibility of asset data, and ensure oversight of fund managers' performance. Data must also be managed for annual reports and must be accessible to regulators investigating infringements of the directive.