A managed data services solution designed specifically for financial institutions

Designed to enable firms to focus on their core revenue-generating activities by outsourcing data management challenges to a financial data specialist, AC PaSS is a fully comprehensive data platform service that supports the entire data lifecycle. Focused on the needs of the end user, AC PaSS enables firms to enhance the quality of their data and streamline their data operations, while reducing risk and lowering the cost of change.

Put your data in autopilot
www.asset-control.com
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Foreword</td>
<td>6</td>
</tr>
<tr>
<td>AIFMD</td>
<td>8</td>
</tr>
<tr>
<td>AMLD5</td>
<td>11</td>
</tr>
<tr>
<td>AnaCredit</td>
<td>13</td>
</tr>
<tr>
<td>Basel III and IV</td>
<td>15</td>
</tr>
<tr>
<td>BCBS 239</td>
<td>19</td>
</tr>
<tr>
<td>Benchmarks Regulation</td>
<td>22</td>
</tr>
<tr>
<td>CCAR</td>
<td>26</td>
</tr>
<tr>
<td>COREP</td>
<td>30</td>
</tr>
<tr>
<td>CRD IV and V</td>
<td>32</td>
</tr>
<tr>
<td>Dodd-Frank</td>
<td>36</td>
</tr>
<tr>
<td>EMIR and EMIR II</td>
<td>40</td>
</tr>
<tr>
<td>FATCA and GATCA</td>
<td>46</td>
</tr>
<tr>
<td>FIDLEG</td>
<td>49</td>
</tr>
<tr>
<td>FINREP</td>
<td>52</td>
</tr>
<tr>
<td>FRTB</td>
<td>54</td>
</tr>
<tr>
<td>GDPR</td>
<td>58</td>
</tr>
<tr>
<td>IFRS</td>
<td>61</td>
</tr>
<tr>
<td>KYC</td>
<td>63</td>
</tr>
<tr>
<td>MAR and MAD</td>
<td>66</td>
</tr>
<tr>
<td>Margin requirements – BCBS/IOSCO</td>
<td>69</td>
</tr>
<tr>
<td>MiFID II</td>
<td>72</td>
</tr>
<tr>
<td>MiFIR</td>
<td>78</td>
</tr>
<tr>
<td>Money Market Funds</td>
<td>80</td>
</tr>
<tr>
<td>NIS</td>
<td>83</td>
</tr>
<tr>
<td>PRIIPs</td>
<td>85</td>
</tr>
<tr>
<td>SEC CAT</td>
<td>88</td>
</tr>
<tr>
<td>SEC CECL</td>
<td>90</td>
</tr>
<tr>
<td>SEC Forms N-PORT and N-CEN</td>
<td>92</td>
</tr>
<tr>
<td>SEC Form PF</td>
<td>94</td>
</tr>
<tr>
<td>SEC Rules 15c3-1, SEC 15c3-3, SEC 17a-5</td>
<td>96</td>
</tr>
<tr>
<td>SEC Rule 22e-4</td>
<td>97</td>
</tr>
<tr>
<td>SEC Rule 606</td>
<td>99</td>
</tr>
<tr>
<td>Section 871(m)</td>
<td>102</td>
</tr>
<tr>
<td>SFTR</td>
<td>104</td>
</tr>
<tr>
<td>SMCR</td>
<td>107</td>
</tr>
<tr>
<td>Solvency II</td>
<td>109</td>
</tr>
<tr>
<td>UCITS V</td>
<td>112</td>
</tr>
<tr>
<td>Outlook</td>
<td>114</td>
</tr>
<tr>
<td>Glossary</td>
<td>115</td>
</tr>
</tbody>
</table>

---

**A-TEAM GROUP**

**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  
amrew@a-teamgroup.com

Editorial  
Sarah Underwood  
sarah.underwood@a-teamgroup.com  
Lauren McAughtry  
lauran@a-teamgroup.com

Sales - Data Management Insight and RegTech Insight (mid & back office)  
Jo Webb  
jo@a-teamgroup.com

Sales TradingTech Insight and RegTech Insight (front office)  
Phl Ansley  
phil@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

Group Marketing Manager  
Claire Snelling  
claire@a-teamgroup.com

Social Media Manager  
Jamie Icenogle  
jamie@a-teamgroup.com

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

Production Manager  
Sharon Wilbraham  
sharon@a-teamgroup.com

Project & Events Coordinator  
Katie Delaney  
katie@a-teamgroup.com

Design  
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.a-teaminsight.com
DOWNLOAD TODAY

This unique directory provides:

• Detailed overviews of companies and their RegTech solutions

• Listings of solutions by regulation, capability, region, firm type targeted and more

• Statistics of interest such as average funds raised, average size, distribution of solutions by regulation and more

RegTech Suppliers Guide

View our range of guides on various financial data and technology issues, that are available for free download

guides.regtechinsight.com

@regtechinsight
Search: RegTech Insight
www.regtechinsight.com

A-Team Insight
Introduction

An update on the regulatory landscape

Welcome to the seventh edition of A-Team Group’s Regulatory Data Handbook, our most popular and well-read publication among data management and compliance teams in capital markets.

This edition of the handbook adds new regulatory interests including the European Market Infrastructure Regulation (EMIR) Refit, which aims to simplify certain requirements for smaller firms by taking a more proportionate approach. It also addresses issues around compliance costs, transparency issues and insufficient access to clearing for certain counterparties.

SEC Rule 606 is also among this edition’s newcomers. The rule was initially proposed by the Securities and Exchange Commission (SEC) in 2000 to improve public disclosure of order routing practice. It has since gone on to be amended as routing and execution practices have evolved. The latest updates to the rule were made this year and you can read all about them in the handbook.

As well as new entries, we update the details and timelines of the many regulations we have built up in the handbook since our first edition back in 2014.

We have also added information on the data and data management requirements of each regulation, and links to original regulatory texts and other publications that we hope you will find useful.

As you may have seen, we’ve launched a new RegTech Insight channel dedicated to developments in regulatory technology and data for the capital markets. You can become a member for regular updates at www.RegTechInsight.com. It sits alongside our other titles Data Management Insight and TradingTech Insight, all of which can be found at www.a-teaminsight.com.

Be sure to visit to find out more about forthcoming regulations, regulatory change management, the impact of compliance on the business, and the benefits of a holistic data management approach to multiple regulations, whether you prefer to read blogs, listen to webinars, consume white papers, or come and network in person at our Data Management Summits and RegTech Summits.

In the meantime, thanks to all the sponsors of this handbook. We hope you find this guide useful in your work.

Angela Wilbraham
Chief Executive Officer
A-Team Group
Foreword

By Vincent Kilcoyne, EVP Product Management, SmartStream

Regulation continues to be a challenge for capital markets participants, but its impact is changing as the flow of new regulation slows and regulators reiterate existing requirements to improve efficiency. Financial firms are also adapting their approaches to regulation, reviewing how best to manage the proliferation of data emanating from reporting, implementing innovative technologies, preparing for regulatory change, and ensuring they can access, understand and gain value from the data they store and manage.

For most firms, the next major regulatory challenge is the EU’s Securities Financing Transactions Regulation (SFTR), which is designed to increase transparency around activities that are broadly categorised as shadow banking, and comes into force in April 2020. The regulation is extensive, with 150 data fields in its mandatory regulatory reports and including both the kind of transaction reporting practitioners are familiar with, but also a strong reference data requirement.

To ease the pain of implementation, SmartStream has collaborated with A-Team Group to produce a white paper that reviews the requirements of SFTR with a specific focus on its reference data aspects. You can also read about the regulation in this handbook.

Regulatory reiteration has become as demanding as implementing new regulation over the past year or so and will continue to grow, adding to the regulatory burden, but also helping firms clarify their response and improve underlying data management for both internal and external operations.

A case in point is BCBS 248, a follow-on from BCBS 239, which focusses on risk data aggregation and reporting, and has become a foundation for regulatory data management at many firms. BCBS 248 layers a new requirement on BCBS 239 that improves the understanding of risk by superseding BCBS 239 requirements for inter-day liquidity monitoring and requires intra-day monitoring. The outcome is greater resilience.
and robustness in the financial sector, and for firms that implement the requirement well, a better view of cash positions throughout the trading day.

While many firms initially, and often necessarily, took a tactical regulation-by-regulation approach to the tsunami of requirements that followed the 2018 financial crisis, transition is also being made here as firms take a more holistic view of compliance underpinned by data management frameworks that support numerous regulations and deliver both cost reductions and the capability to absorb new or changing requirements.

Data silos, data duplication and friction in data management processes continue to be barriers to streamlined, accurate and timely reporting, and often limit ability to gain business value from data, but these issues are beginning to be addressed, often through the implementation of innovative technologies such as machine learning and other strands of artificial intelligence (AI) that can automate data management across silos or a central data repository. These types of technologies can take reporting to the next level, while ensuring data integrity across the enterprise and delivering benefits beyond compliance. To help firms realise the potential of AI, SmartStream and A-Team Group recently published a white paper on adopting AI for superior reconciliation.

Regulation is changing, as are its challenges. SmartStream solutions and SmartStream Reference Data Utility can help financial institutions not only manage these changes and challenges, but also provide access to contextual data that is vital to better decisions and business growth.
AIFMD

At a Glance

**Regulation:** Alternative Investment Fund Management Directive (AIFMD)

**Regulatory Regime:** EU

**Target Market Segment:** Alternative investment funds

**Core 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
- **2017/18:** European Commission delays review of extension of passport system to non-EU countries as UK negotiates exit from EU under Brexit
- **March 2018:** Proposal for a supplementary AIFM Directive (AIFMD 2)
- **August 2, 2019:** Implementation of AIFMD 2

**Key Links**

- **Full Text:** https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1568976762264&uri=CELEX:32011L0061

**Description and Data Requirements**

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, such as 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, 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 to operate across the EU, giving access to the benefits of the single market. High quality reference data and the ability to accurately evaluate exposure is key to AIFMD. The SmartStream Reference Data Utility is a managed service that delivers accurate and timely data for use in regulatory reporting and risk management operations. A simple and effective source of data that you can rely on.

For financial organisations who need to manage their exposure by the size of their operations, SmartStream has a suite of solutions which can help.

www.smartstream.com
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 was due to be considered by the European Commission before any decisions were made on extending the passport system, but negotiations on the withdrawal of the UK from the EU under Brexit have delayed decisions by the European Commission on ESMA’s advice.


The amended rules aim to harmonise the marketing and pre-marketing position across EU member states to standardise the point at which the fund must be registered with the local regulator. AIFMD 2 applies only to pre-marketing by EU AIFMs, not non-EU AIFMs. However, Recital 12 to AIFMD 2 notes that complying with the new rules should not disadvantage EU AIFMs over non-EU AIFMs, suggesting that regulators are likely to apply the same definition of pre-marketing to non-EU AIFMs.

SWIFTRef’s Entity data helps you correctly identify and assess your existing and future counterparties. Through cross-referenced entity identifiers, legal ownership structure information and key assessment information, SWIFTRef data assists you with ever-increasing regulatory requirements. Our dedicated data teams collect, maintain, map and enrich the entity data on your behalf, ultimately supporting your entity data management, regulatory reporting, risk management, compliance, and due diligence activities.

www.swift.com/swiftref
Description and Data Requirements
The fifth EU Anti-Money Laundering Directive (AMLD5) updates the EU’s fourth AML Directive (AMLD4) and aims to strengthen regulation designed to prevent use of the global financial system for money laundering and counter terrorist financing (CTF).

The European Commission proposed revisions to AMLD4 in July 2016 as part of an action plan against terrorism announced in February 2016 after attacks in Paris and Brussels, and as a reaction to the Panama Papers that were published in April 2016.

AMLD5 was published in the Official Journal of the European Union in June 2018 and entered into force in July 2018. It revises AMLD4, which was released in 2015, and requires member states to transpose the modified regulations into national law by January 20, 2020.

AMLD5 improves transparency of beneficial owners of legal entities, trusts and similar legal arrangements. This is done in various ways, including provision of beneficial ownership registers of legal entities that are publicly accessible for specific types of information gathered on beneficial owners, and making registries of trusts and similar legal arrangements accessible to competent authorities, national Financial Information Units (FIUs), obliged entities in the context of their due diligence measures, and any person who can demonstrate a legitimate interest.

When beneficial ownership registers are in place, Know Your Customer

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 AMLD
July 9, 2018: AMLD5 enters into force
January 20, 2020: AMLD5 must be transposed into national law and applied

Key Links
Full text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
(KYC) processes must consult them before new business relationships are made.

The directive also makes national central registers of banks, payment accounts, and safe deposit box holders accessible to national FIUs and to national competent authorities (NCAs). National registers must be interconnected via a central European platform to promote cooperation between member states.

The directive clarifies politically exposed persons (PEPs) by requiring member states to issue and keep up-to-date a list of the exact functions that qualify as prominent public functions according to their national laws. This is designed to give clarity on who is considered as a PEP in a given member state.

Enhanced customer due diligence measures must be performed in the context of business relationships or financial transactions involving high-risk third countries, and the directive encourages firms within its remit to use eiDAS compliant technology—eiDAS Regulation provides a predictable regulatory environment to enable secure and seamless electronic interactions— for customer due diligence processes.

Strengthening rules around CTF, AMLD5 lowers the thresholds of electronic money and prepaid instruments, and brings into scope virtual currency providers, electronic wallet providers, and persons or intermediaries trading works of art when the value of a transaction or series of linked transactions amounts to €10,000 or more.

Finally, the revised directive extends the rights and competences of national FIUs, as well as cooperation and exchange of information between them.

From a data management perspective, AMLD5 expands demands, particularly around requirements for beneficial ownership information, which will stretch many financial institutions’ current capabilities. Changes to other elements, such as customer due diligence and the definition of PEPs, will require financial institutions to extend and adjust existing data management processes.
AnaCredit

**Description and Data Requirements**
AnaCredit (analytical credit datasets) is a European Central Bank (ECB) regulation set up to build a dataset of detailed information on individual bank loans and deposits in the Euro area and harmonised across all EU Member States. It is designed to make it possible to identify, aggregate and compare credit exposures and to detect associated risks on a loan-by-loan basis. The project was initiated in 2011, early adoption was introduced in December 2017, and full data collection and complete reporting started on September 30, 2018.

The scope of data collection covers data on credits extended or serviced by EU credit institutions that are not branches of other credit institutions; foreign branches of EU credit institutions, including non-Euro area branches; and foreign branches that are located in the Euro area but are part of a credit institution resident outside the Euro area.

In the first stage, only credit data related to loans of a minimum €25,000 and extended to legal entities that are not natural persons have to be reported. Loans to private households are not covered, although further phases of AnaCredit will follow phase one.

The regulation requires over 100 data points to be reported for each exposure, including 94 data attributes and seven unique identifiers used several times across
various regulatory templates. The ECB expects the information provided to be ‘granular, exact and detailed’. The required information includes data related to the counterparty, such as LEI code, address, balance sheet total; data related to the instrument, type, currency, status, interest rate type, payment frequency; data related to the collateral, type of protection, location, value; and accounting data, such as accumulated impaired amount and source of encumbrance.
Regulatory Data Handbook 2019  15

Basel III and Basel IV

Significant Milestones

December 16, 2010: Basel III 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
December 2017: BCBS publishes reforms for Basel III, referred to as Basel IV
January 1, 2018: Leverage ratio becomes mandatory
January 1, 2018: NSFR ratio introduced
January 14, 2019: BCBS endorses revisions to the market risk framework

Dates for Diary

January 1, 2022: Basel IV starts five-year phase-in
January 1, 2027: Full implementation of Basel IV

Key Links

Full Text: www.bis.org/publ/bcbs189.pdf
Overview: www.bis.org/bcbs/basel3/b3summarytable.pdf
LCR Text: www.bis.org/publ/bcbs238.pdf
NSFR Text: www.bis.org/bcbs/publ/d295.pdf
Basel III Reforms: http://www.bis.org/bcbs/publ/d424_hlsummary.pdf

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

At a Glance

Regulation: Basel III
Regulatory Authority: BCBS and national supervisory authorities
Target Market Segment: Global financial institutions
Core Data Requirements: Disclosure of capital adequacy, risk profile
Basel III and Basel IV

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 outflow 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 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

www.smartstream.com
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 and the full implementation date was subsequently pushed back again to January 1, 2022.

**Basel IV**

In December 2017, BCBS published a package of proposed reforms for the Basel III global regulatory framework, which is frequently referred to as Basel IV. The reforms aim to make the capital framework more robust and improve confidence in the banking system, and include changes to the standardised and internal models approach to credit risk, operational risk, leverage ratio, capital floors and credit valuation adjustment (CVA).

The reforms are being considered by lawmakers in national jurisdictions and at the EU level. As part of this process, national or EU authorities must decide on the use of a limited number of alternative calculations allowed under the BCBS proposal, so called ‘national options and discretions’. An example of such a discretion is operational risk and RWAs which, under the proposed framework, may solely be based on a bank’s revenues or also reflect a bank’s individual loss history. Such national discretions, and other potential modifications, will apply when the framework comes into force in any given jurisdiction.

BCBS proposes a nine-year implementation timetable for Basel IV, which allows considerable time for preparation. A five-year phase-in period is planned to start
from January 1, 2022, with full implementation from January 1, 2027.

In January 2019, the Basel Committee’s oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS), endorsed a set of revisions to the market risk framework and the Committee’s strategic priorities and work programme for 2019. The revisions introduces, among others, a simplified standardised approach for banks with small or non-complex trading portfolios.

Once implemented, the revised framework is estimated to result in a weighted average increase of about 22% in total market risk capital requirements relative to the Basel 2.5 framework. The revised market risk framework will take effect as of January 1, 2022, concurrent with the implementation of the Basel III reforms endorsed by the GHOS in December 2017.

In March 2019, the European Banking Authority published a report into the impact of implementing the final Basel III reforms, showing that European banks’ minimum Tier 1 capital requirement would increase by 19.1% at the full implementation date (2027). In August the EBA published further advice on implementation, revising its conservative assumptions to state that full implementation would increase the minimum capital requirement (MRC) by 24.4% on average.

Asset Control provides market data management solutions – either on-prem or via our managed services AC PaSS - that help banks easily gather and combine external and internal data sources, streamline the preparation of prices and risk factors and distribute them to business users and applications. Our highly scalable solutions provide insight into data sourcing, integration, mastering and distribution and are used to service traded risk and IPV departments.

www.asset-control.com/solutions/regulatory-solutions/
BCBS 239

Significant Milestones
June, 2012: Consultation paper released
January 9, 2013: Regulation published
January 1, 2016: Compliance deadline

Key Links
Full Text: www.bis.org/publ/bcbs239.pdf
Publications: www.bis.org/bcbs/publications.htm
Progress Report 2018: www.bis.org/bcbs/publ/d443.pdf

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.

While BCBS 239 is acknowledged across the financial industry as a base for improved risk data aggregation, data governance and accurate reporting, firms are falling short on compliance. The BCBS 2017 progress report published in June 2018 says banks have found it challenging to comply with the principles of BCBS 239, due mainly to the complexity and interdependence of IT improvement projects. As a result, the expected date of compliance has slipped back for many banks.

The 2017 assessment shows that most banks made, at best, marginal progress in their implementation of the principles and that although the implementation deadline of January 1, 2016 has passed, only three global systemically important banks (G-SIBs) were assessed by their supervisors as achieving full compliance with all principles.

At a Glance
Regulation: BCBS 239
Regulatory Authority: BCBS and national supervisory authorities
Target Market Segment: Global financial institutions
Core Requirements: Risk data aggregation and reporting

SmartStream’s solutions manage transactions from trade inception through to settlement on a single platform. This supports a more efficient automated data aggregation model ensuring the accuracy and integrity of risk reporting. Meanwhile, SmartStream’s TLM SmartRecs facilitates the rapid onboarding of reconciliations to help institutions ensure completeness. The BCBS 239 requires that data is collected and aggregated correctly. SmartStream’s TLM Cash and Liquidity Management supports banks in reconciling all transaction and data types.

www.smartstream.com
While penalties for non-compliance have not yet been issued, and could include increased capital requirements, the report warns that ‘banks should remain committed to their initiatives for implementing the principles and avoid further deadline slippages. Banks should take concrete actions and continue to make progress in the implementation of the principles according to the roadmaps agreed with their supervisors. As the compliance deadline has already passed, further delays should be avoided.’

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 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 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) are 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.

The BCBS augmented BCBS 239 requirements around liquidity in 2016 with the issuance of BCBS 248. This layers a new requirement on BCBS 239 that improves the understanding of risk by superseding BCBS 239 requirements for inter-day liquidity monitoring and requires intra-day monitoring. The outcome is greater resilience and robustness in financial markets.
Benchmarks Regulation

At a Glance
- **Regulation:** Benchmarks Regulation
- **Regulatory Regime:** 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
- **January 1, 2018:** Compliance deadline
- **December 2021:** FCA deadline for Libor transition

**Dates for Diary**
- **January 1, 2020:** EU benchmark administrators providing benchmarks before January 1, 2018 have until January 1, 2020 to apply to their EU national competent authority for authorisation or registration

**Key Links**
- **Register of Benchmarks Administrators:** [https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_bench_entities](https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_bench_entities)

**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 allowed supervisors to make use of certain provisions of the Benchmarks Regulation in advance of its application in January 2018.

The regulation requires benchmark providers to be authorised or registered by their national competent authority (NCA), and defines a benchmark as ‘any index by reference to which the amount payable under a financial instrument or a financial contract, or the value of a financial instrument is determined or an index that is used to measure the performance of an investment fund.

It also sets out three main categories of benchmarks:

**Critical benchmarks**
Benchmarks used for financial instruments, contracts and performance of investment funds having a total value of at least €500 billion, and meeting qualitative criteria such as location of contributors and importance of the benchmark in the country where a majority of contributors is located.

**Significant benchmarks**
Benchmarks used for financial instruments, contracts and performance of investment funds having a total value of at least €50 billion over a period of six months, and meeting qualitative criteria such as the benchmark has no reliable substitute, and its absence would lead to market disorder.

**Non-significant benchmarks**
Benchmarks that do not fulfil the conditions set for critical or significant benchmarks. Euribor was the first benchmark to be included in the list of critical benchmarks. It has since been joined by Libor and the Euro Overnight Index Average (Eonia) with further additions to the list expected to be added by the European Commission in due course. 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 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 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.

**Libor transition**
The Benchmarks Regulation also requires that users of benchmarks must produce and maintain a “robust written plan” outlining the actions they would take in the event that a benchmark materially changed or ceased to be provided, including the nomination of an alternative benchmark where feasible.

This is currently most relevant in the UK, where Libor is due to cease at the end of 2021, requiring firms to transition away from Libor to alternative risk-free rates (such as the Sterling Overnight Index Average, SONIA) for sterling markets. This transition is expected to present substantial data management challenges as firms attempt to upgrade and monitor their systems throughout this process.

In September 2018, ISDA published the ISDA 2018 Benchmarks Supplement, developed primarily to facilitate compliance with the EU Benchmarks Regulation but which can also be used by market participants in connection with their transition away from inter-bank offered rates (such as Libor). On December 10, 2018 ISDA published the Benchmarks Supplement Protocol, a multilateral contractual amendment mechanism enabling adhering parties to incorporate the Supplement into relevant transactions with multiple counterparties on the same platform, rather than having to amend contracts by way of a separate bilateral negotiation with each one.
AC PaSSPort redefines cloud-based data management

AC PaSSPort offers serviced integration to the data sources you require, the controls to transparently manage the data sets you request and inspect the preparation process, and makes data available via APIs and in the formats and frequencies you require.

The advantages of outsourcing data management:
- Maintained integration to Bloomberg, ICE Data Services, IHS Markit, Refinitiv, Six Financial Information, S&P Global or other sources
- Security master in the cloud
- Request management to maintain securities of interest
- Acquisition tool to add/remove instruments
- Access via Operations360, full transparency on the data preparation process and browsing

Put your data in autopilot
www.asset-control.com #StartYourDataJourney
CCAR

At a Glance

Regulation: Comprehensive Capital and Analysis Review (CCAR)

Regulatory Regime: 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
January 30, 2017: Federal Reserve excludes large and non-complex firms from the qualitative assessment of CCAR
2018: Federal Reserve adds six IHCs to the stress test
June 28, 2018: Federal Reserve releases 2018 CCAR results
June 27, 2019: Federal Reserve releases 2019 CCAR results

Dates for Diary

June 2020: CECL integration into CCAR

Key Links

Overview: https://www.federalreserve.gov/supervisionreg/ccar.htm

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 proforma 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. On January 30, 2017, the Federal Reserve Board finalised a rule adjusting its capital plan and stress testing rules, effective for the 2017 cycle. The rule removed large and non-complex firms from the qualitative assessment of CCAR, reducing the burden on these firms and focusing the qualitative review in CCAR on the largest, most complex financial institutions. Large and non-complex firms are defined as BHCs and US intermediate bank holding companies as IHCs. These firms are still required to meet capital requirements under stress as part of CCAR’s quantitative assessment and will be subject to regular supervisory assessments that examine their capital planning processes.

Since 2018, the Federal Reserve has been working towards resetting CCAR and reducing the regulatory burden while increasing transparency. In May 2018 the Economic Growth, Regulatory Relief, and Consumer Protection Act (the Relief Act) was passed, promising a more risk-based approach and exempting institutions with under $100 billion in assets. In October 2018, introduced a new rule defining four categories for firms with assets above $100 billion, replacing the previous “large and complex” and
“large and non-complex” definitions, each subject to different stress-testing requirements.

In February 2019 the Federal Reserve extended further relief to less-complex firms from stress testing requirements and CCAR by effectively moving the firms to an extended stress test cycle for this year, applicable for firms with total consolidated assets between $100-250 billion. These less-complex firms were not subject to a supervisory stress test during the 2019 cycle.

In March 2019, the Federal Reserve also announced that it would limit the use of the “qualitative objection” for CCAR 2019. The changes eliminate the qualitative objection for most firms due to the improvements in capital planning made by the largest firms. However, firms that are newer to the CCAR exercise and as a result may have capital planning capabilities that are less established will remain subject to a possible objection on qualitative grounds. Specifically, a firm must participate in four CCAR exercises and successfully pass the qualitative evaluation in the fourth year to no longer be subject to a potential qualitative objection. For firms still subject to the qualitative objection, their fourth year will generally be the 2020 CCAR cycle.

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. The Federal Reserve continues to widen the scope of CCAR, with the addition of six IHCs to the stress test in 2018. Further changes to supervisory post-stress capital projections were applied as a result of the 2017 Tax Cuts & Jobs Act, including a reduction in the corporate tax rate from 35% to 21%; the elimination of net operating loss
(NOL) carrybacks; and a limitation on NOL carry forwards to 80% of taxable income. These changes could have negative effects on many firms’ post-stress capital ratios, as from a stress testing perspective, banks will no longer be able to offset the stress losses with projected tax refunds.

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.

On June 27, 2019 the Federal Reserve released results for CCAR 2019, with none of the 18 participating banks receiving an objection to their capital plans on either quantitative or qualitative plans, reaffirming the more relaxed, risk-based approach from the regulator. However, some uncertainty remains, including industry concerns around a lack of clarity over trading hedges. In 2020, the new Current Expected Credit Losses (CECL) accounting standard is expected to be integrated into CCAR, which is likely to lead to material increases in provisions (estimated up to 30%). According to a July 2019 McKinsey survey, CECL integration is a top priority for banks for CCAR 2020, although over two thirds of banks surveyed have significant outstanding questions on their methodologies. This integration is likely to throw up substantial upgrade requirements around second and third lines of defence, internal audit functions and compliance, with related data needs around the new models.
COREP

At a Glance
Regulation: Common Reporting (COREP)
Regulatory Regime: 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
January 18, 2017: EBA updates XBRL taxonomy for reporting
September 2018: Publication by EBA of draft Data Point Models (DPM) on proposed changes to LCR reporting
October 26, 2018: Deadline for feedback on proposed revisions to LCR reporting
May 28, 2019: Publication of amendments to supervisory reporting

Dates for Diary
March 31, 2020: First reporting reference date for COREP changes

Key Links

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. The taxonomy was updated by the EBA in January 2017. Reports with reference dates from June 30, 2017 onwards must use the new taxonomy, known as set 2.6.

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. Regulated organisations in the UK have been required to use COREP to make regular statutory reports since January 1, 2014. In total, the reporting framework has been adopted by 30 European countries.

On August 28, 2018 the EBA launched a consultation to review proposed revisions to Implementing Technical Standards (ITS) for COREP Liquidity Coverage Requirement (LCR) reporting for credit institutions. The proposed revisions reflect an amendment to the Capital Requirements Regulation made in July 2018 regarding the calculation of inflows and outflows in securities financing transactions.

In May 2019 the EBA published amendments to the Implementing Technical Standards (ITS) on supervisory reporting. The updated corresponding Data Point Model (DPM) and XBRL taxonomy include amendments to COREP to reflect the new securitisation framework, as well as amendments with regard to liquidity in response to the LCR Delegated Act, and clarifications and corrections as regards reporting on COREP and additional monitoring metrics for liquidity (technical amendments). The package forms part of the EBA reporting framework version 2.9. The first reporting reference date will be March 31, 2020 for COREP changes, April 30, 2020 for changes regarding liquidity (LCR and ALMM) and December 31, 2019 for resolution planning.
CRD IV and CRD V

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
- **November 23, 2016:** European Commission proposals to amend CRD IV and introduce CRD V
- **May 25, 2018:** Council of the European Union agrees CRD V, a new package of measures aimed to reduce risk in banking
- **May 14, 2019:** European Council adopts CRR II and CRD V reforms.
- **June 7, 2019:** CRR II and CRD V regulations published in the Official Journal of the EU.
- **June 27, 2019:** CRR II and CDR V enter into force.

### Dates for Diary

- **June 28, 2021:** Implementation deadline for the majority of CRR II provisions.

### Key Links


### 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 (CRR), 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 (CRD), 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, extends corporate governance and supervisory requirements, and adds 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).

Firms 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.

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.

Looking forward, the spectre of CRD V appeared in November 2016, when the European Commission outlined proposals to amend the Capital Requirements Regulation and the Capital Requirements Directive.


In April 2019 the European Parliament endorsed an agreement on the banking reform package, with new measures including:

• A leverage ratio requirement for all institutions as well as a leverage ratio buffer for all global systemically important institutions;
• A net stable funding requirement;
• A new market risk framework for reporting purposes;
• A requirement for third-country institutions having significant activities in the EU to have an EU intermediate parent undertaking;
• Revised rules on capital requirements for counterparty credit risk and for exposures to
CRD IV and CRD V

central counterparties;
• A revised Pillar 2 framework;
• An updated macro-prudential toolkit;
• The exclusion of certain banks from the scope of application of the CRR and the CRD;
• A number of measures aimed at reducing the administrative burden related to reporting and disclosure requirements for small non-complex banks, as well as simplified market risk and liquidity rules for those banks;
• A new discount on capital requirements for investments in infrastructure and a more generous discount on capital requirements for exposures to SMEs;
• Targeted amendments to the credit risk framework to facilitate the disposal of non-performing loans and to reflect EU specificities;
• Targeted amendments related to the incorporation of environmental, social and governance aspects into prudential rules;
• Enhanced prudential rules in relation to anti-money laundering;
• A new total loss absorbing capacity (TLAC) requirement for global systemically important institutions;
• Enhanced Minimum Requirement for own funds and Eligible Liabilities (MREL) subordination rules for global systemically important institutions (G-SIls) and other large banks referred to as top-tier banks;
• A new moratorium power for the resolution authority;
• Restrictions to distributions in case of MREL breaches;
• Home-host related measures.


The final CRD V text includes amendments in areas such as the IPU rule, Pillar 2 capital requirements and remuneration. It adopts Basel conditions to determine the modellability of risk factors, but does not include certain Basel IV rules which were agreed in December 2017 – therefore affected firms should ensure that their implementation programmes can tolerate future changes, expected in CRR III, discussions on which should launch mid-2020.
We’re in the exciting planning phase for next year’s events. If you want to make sure you don’t miss out and want us to let you know as soon as we have dates and are taking reservations, pick your event(s) and enter your details at the ‘remind me’ link. We’ll be sure to email you as soon as the details have been firmed up.
**Dodd-Frank**

**At a Glance**

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

**Regulatory Regime:** US Government

**Target Market Segment:** Global financial institutions

**Core Data Requirements:** Identification of issuers, clients and counter parties

---

**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.

Dodd-Frank includes a large number of rules that 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.

---

**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
- **May 22, 2018:** Partial Republican rollback of Dodd-Frank to release SME banks from stress-testing

**Key Links**

- **Full Text:** [https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf)
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 by Dodd-Frank not only for reporting, but also as the basis for systemic risk oversight and improved transparency. Early this year, US president Donald Trump moved to roll back financial regulations brought in after the financial crisis and demanded a review of Dodd-Frank. He said the regulations were too onerous for business and a drag on the economy.

On May 2018, US Congress implemented the first major rollback of the regulation, voting 258-159 to free thousands of small and medium-sized banks (with less than $250bn in assets) from the strict stress tests and leaving fewer than 10 banks subject to full Federal oversight. The rollback was endorsed by original writers Senators Barney Frank and Christopher Dodd, who called it a ‘fairly small change’. Further legislative rollbacks are thought to be unlikely unless Republicans manage to secure a House and two-thirds Senate majority. However, regulators are moving to relax the Dodd-Frank rules under their own scope, with five Federal agencies—including the SEC, CFTC, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency—currently working together to simplify and tailor compliance requirements for the Volcker rule, which generally restricts banking entities from engaging in proprietary trading and from owning or controlling hedge funds or private equity funds. The proposal was released to the public for comments in early June 2018 with comments

A key requirement in the Dodd-Frank Act is the reconciliation of OTC derivatives. In response, SmartStream delivers pre-built Reconciliation solutions and workflow management which manages the trade and its process legs across the lifetime of the trade. TLM Collateral Management supports the evolving requirements arising from Dodd-Frank. All firms can benefit from its portfolio management, reconciliation, dispute workflow, reporting, limit and threshold monitoring, as well as its ability to classify counterparties and product types.

www.smartstream.com
closing on October 17, 2018.

On October 11, 2018 the SEC also re-opened comments on Title VII of the Dodd-Frank regulation, which established a regulatory regime for security-based swap dealers (SBSDs). The SEC also requested additional comment on rulemaking to adopt margin, capital, and collateral segregation requirements applicable to SBSDs. The move represented the first public step towards an SBS statutory regime and compulsory registration, and could impact non-US derivatives traders who will need to consider how to comply with a potentially new US regime.

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.

Each year, the Federal Reserve refines both the substance and process of DFAST, including its development and enhancement of independent supervisory models. For DFAST 2019, the Federal Reserve enhanced the models that project auto loan losses, credit card losses, corporate loan losses, fair value for debt securities, and commercial real estate loan losses. In addition to these model changes, the Federal Reserve made other less material enhancements to simplify the models and account for changes in the historical data used to estimate the models.

Most recently, on August 20, 2019, the Office of the Comptroller of
the Currency and the Board of Directors of the Federal Deposit Insurance Corporation approved an expected rewrite of the regulation on proprietary trading (the Volcker Rule), along with some minor amendments to the provisions governing private equity funds and hedge funds.

The new rule attempts to make it easier and less expensive for banks to comply by changing the way proprietary trading is measured. It adopts a three-tiered approach, under which compliance obligations differ based on the tier in which tier a banking entity finds itself. For non-US banks, only the US operations are considered when determining tier. The system has been hailed as more accurate by removing the previous $50bn threshold.

The revision has been the subject of some controversy, with observers raising concerns around an overly narrow scope for financial instruments subject to the rule. However, the industry has welcomed the changes and urged further reform.
EMIR and EMIR II

**At a Glance**

**Regulation:** European Market Infrastructure Regulation (EMIR)

**Regulatory Regime:** EU

**Target Market Segment:** Global financial institutions

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

**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

**Significant Milestones**

**August 16, 2012:** Effective data

**February 12, 2014:** First reporting deadline

**May 2015:** European Commission launches review of legislation

**June 21, 2016:** First clearing deadline

**September 1, 2016:** First margin requirements deadline

**January 2017:** EMIR 1.5 is adopted

**November 2017:** Compliance with EMIR 1.5

**June 12, 2018:** European Parliament votes to make changes to EMIR that are likely to result in EMIR II

**September 26, 2018:** ESMA issues updated Q&A regarding EMIR implementation


**May 28, 2019:** ESMA issues updated Q&A regarding the EMIR Refit

**June 17, 2019:** EMIR Refit enters into force

**Key Links**


**ESMA EMIR Refit Q&As:** https://www.esma.europa.eu/sites/default/files/library/esma70-1861941480-52_qa_on_emir_implementation.pdf
the entities involved in the trade, is reported to a trade repository. Both OTC and exchange-traded derivatives must be reported, as well as life cycle 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 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

A key requirement for EMIR is the reconciliation of OTC derivatives. In response, SmartStream delivers pre-built Reconciliations solutions and workflow management which manages the trade and the process legs across its lifetime. TLM Collateral Management supports the evolving requirements arising from EMIR. All firms can benefit from its diverse functionality. Reference data for derivatives is critical to the EMIR reporting lifecycle. The SmartStream Reference Data Utility is a simple and cost effective source.

www.smartstream.com
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 eight trade repositories for derivatives processing: DTCC Derivatives Repository, UnaVista, KDPW, Regis-TR, CME TR, ICE Trade Vault Europe, and, most recently, the Bloomberg Trade Repository, and NEX Abide Trade Repository.

In August 2017, ESMA issued final guidelines on data transfer between trade repositories authorised under EMIR, saying data portability is essential for data quality, competition between trade repositories and for risk monitoring by authorities. The guidelines establish a consistent and harmonised approach for the transfer of data between repositories and cover the transfer of data at the request of a repository participant and the transfer of data due to withdrawal of repository registration.

During 2014 and early 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 nine third-country CCPs in South Africa, Canada, Mexico, Switzerland, South Korea, Poland and the US. In 2017, a number of additional third-party CCPs were named, bringing the total to 32.

**EMIR 1.5**

In accordance with Article 85 of EMIR, the European Commission launched a review of the legislation in May 2015. 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

The Commission concluded that, although there was no need for a fundamental change to the nature of the core requirements in EMIR, the legislation imposed disproportionate burdens and overly complex requirements on non-financial counterparties, small financial counterparties and pension funds.

In January 2017, EMIR 1.5 was adopted in a delegated regulation and implementing regulation. Banks and buy-side firms within the scope of EMIR were required to comply with the 1.5 updates from November 2017.

A key change was an extension of the EMIR trade reporting template so that it aligns with Markets in Financial Instruments Directive II (MiFID II) reporting templates. This means EMIR 1.5 covers OTC derivatives trading across all asset classes. In particular, market participants will be required to report complex derivatives contracts composed of a combination of several other derivatives contracts. EMIR 1.5 also brought OTC derivatives contracts derived from credit instruments into scope.

EMIR 2.1/REFITAs a result of the 2015 consultation, EMIR was included within the European Commission’s 2016 Regulatory Fitness and Performance (REFIT) programme.

In May 2017, this resulted in a proposal to amend EMIR based on problems in the regulation identified after four years of observation and two consultations with market participants. The proposal noted the need to make further changes to the regulation to remove unnecessary costs and burdens for certain types of market participants, particularly non-financial counterparties that only trade derivative contracts to reduce risk directly related to their main activities.


The amendments aim to simplify certain requirements for smaller firms, taking a more proportionate approach. They also address issues around compliance costs, transparency issues and insufficient access to clearing for certain counterparties.
**EMIR and EMIR II**

**The EMIR Refit:**

- Amends the definition of “financial counterparty (FC)” to include alternative investment funds (AIFs) and their managers, meaning these entities are now subject to all EMIR obligations.
- Introduces a requirement on clearing members to provide clearing services on fair, reasonable, non-discriminatory and transparent commercial terms – in particular regarding conflicts of interest between trading and clearing units.
- Gives the European Commission the power to suspend the clearing obligation for three month periods, for a maximum aggregate period of 12 months.
- Introduces a new category of “small financial counterparties” which are exempt from the obligation to clear transactions through a central counterparty (CCP), and which have reduced reporting obligations.
- Reduces clearing and reporting obligations for smaller non-financial counterparties, and replaces the 30 day rolling average clearing threshold calculation with an annual calculation based on the aggregate month-end average position for the preceding 12 months.
- Amends reporting requirements, particularly around derivatives.

For OTC derivatives contracts, FCs are solely responsible and legally liable for reporting on behalf of itself and NFCs that are not subject to the clearing obligation. An NFC is also exempt from reporting responsibility if it transacts with a third country entity that would be an FC if established in the EU. Intragroup transactions where at least one counterparty is an NFC are also exempt from the reporting obligation.

- Requires regulators to implement new supervisory procedures to ensure initial and ongoing validation of firms’ risk management procedures for the exchange of collateral.
- Requires CCPs to provide clearing members with an initial margin simulation tool and with information on the initial margin models employed by the CCP.
- Extends the exemption for Pension Scheme Arrangements (PSAs) from the clearing obligation for a further two years.
- Removes the backloading requirement (to report transactions that were no longer outstanding when the EMIR reporting obligation came into effect) is removed.
- Removes the frontloading obligation for clearing, so a contract is required to be cleared where it is entered into or novated.
on or after the date from which the clearing obligation takes effect.

ESMA is in the process of preparing further implementing technical standards (ITS) on the data and format for the information to be reported. These standards are expected to be submitted by June 2020.

In parallel to the Refit, in June 2017 the Commission also proposed a second set of amendments to EMIR to enhance the supervision of third country clearing counterparties (CCPs), to make the supervision of EU CCPs more coherent and to introduce a fee system for CCPs to fund the relevant activities (EMIR 2.2). A political agreement between the European Parliament and member states was reached in March 2019 to upgrade the supervision of EU and third-country CCPs and give greater regulatory powers to the European Central Bank. Further technical work is currently being undertaken before formal adoption.

In July 2019 ESMA published responses received to its Consultations on tiering, comparable compliance and fees under EMIR 2.2.
FATCA and GATCA

At a Glance

**Regulation:** Foreign Account Tax Compliance Act (FATCA)

**Regulatory Regime:** US Government

**Target Market Segment:** Global financial institutions

**Core Requirements:** Client identification, data maintenance, reporting

Significant Milestones

- **March 18, 2010:** FATCA is 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
- **January 1, 2019:** 30% withholding tax on sale after December 31, 2018 of property producing US source income
- **March 31, 2019:** Reporting deadline for FFIs in non-IGA jurisdictions and FFIs in Model 2 IGA jurisdictions
- **September 30, 2019:** Reporting deadline for FFIs in Model 1 IGA jurisdictions

Key Links


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 100 Model 1 agreements, which require FFIs to report all FATCA information to their own governmental agencies that then report to the IRS, and 13 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 taxpayers. As the regulation calls for sensitive client data, such as tax, residency, citizenship and account status information, to be 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.

Updates to the FATCA regime were made in July 2018, when the IRS updated the regulation’s registration system to incorporate the certification of pre-existing accounts and a periodic certification process. It also updated its list of

SmartStream’s TLM Corporate Actions facilitates a Financial Institutions reporting tax obligations of global income received from corporate actions by US persons.

www.smartstream.com
FATCA and GATCA

FATCA classifications that entities within the scope of the regulation must review and then update their classifications where necessary.

In September 2019 the European Union published an updated list of accounts to be treated as excepted accounts, and an updated list of entities to be treated as non-reporting financial institutions.

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 1IGA 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 bringing the typical total to 104 countries have signed the convention. Many countries started the exchange of information in 2017 and others have followed over the past year.

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

At a Glance

Regulation: FIDLEG (Financial Services Act)
Regulatory Regime: Swiss Government
Target Market Segment: Financial institution
Core Data Requirement: Data aggregation, distribution, reporting

Significant Milestones

November 4, 2015: Federal Council adopts dispatch on FIDLEG, bill ready for parliamentary deliberation
October 24, 2016: The Commission on Economics and Taxation of the Swiss Council of States proposes amendments to the draft provided by the Federal Council
December 14, 2016: Proposed amendments are debated by the Swiss Council of States
September 2017: Discussion of the bill by the National Council
June 15, 2018: Swiss Parliament adopts FIDLEG

Diary Dates

January 1, 2020: Compliance deadline

Key Links


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, 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 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.

In October 2016, the Commission on Economics and Taxation of the Swiss Council of States proposed the following amendments and changes to the latest draft of FIDLEG provided by the Federal Council:

- Insurance companies should be carved out from FIDLEG; relevant amendments would, instead, be made to the Insurance Supervisory Act (ISA) if deemed necessary in the near future.
- External (independent) asset managers will be regulated by an independent supervisory organisation whereby all public supervisory functions, including enforcement, would remain
with FINMA, the Swiss Financial Market Supervisory Authority.

- New license categories for enterprises active in the FinTech sector should be created, including a sand box area where companies can perform bank-like activities without a license; this should be achieved by amending the Banking Act (BA) and the Banking Ordinance (BO) along with the introduction of FIDLEG.

The proposed amendments were debated by the Swiss Council of States in December 2016, ahead of discussion of the bill by the National Council in September 2017. The Swiss Parliament adopted FIDLEG in June 2018, with the regulation due to go live on January 1, 2020.

The consultation process of the drafts of the related Financial Services Ordinance (FIDLEV), the Financial Institutions Ordinance (FINIV) and the Supervisory Organisation Ordinance (AOV) were also completed in February 2019.
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.

In August 2018, the EBA proposed changes to the Implementing Technical Standards (ITS) of Finrep aimed at amending and adding new reporting of non-performing and forborne exposures, amending the reporting of profit or loss items (in particular on expenses) and reporting on leases. A consultation on the proposed changes closed on December 7, 2018 and in July 2019 the EBA published final amendments to the ITS. The amendments concern the reporting requirements on non-performing exposures (NPE) and forbearance to allow monitoring of reporting institutions’ NPE strategies, the reporting requirements on profit and loss items and the implementation of the new International Financial Reporting Standard on leases (IFRS 16). Notably, only institutions with a NPL ratio equal to or greater than 5% are required to report more granular information on NPE and forbearance. The first reporting reference date is June 30, 2020.
Description and Data Requirements
The Basel Committee on Banking Supervision (BCBS) introduced the Fundamental Review of the Trading Book (FRTB) in a May 2012 consultation paper that set out 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 January 1, 2019. The deadline has since been changed to January 2022.

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 model approach (IMA) to market risk and capital requirements, a revised standardised approach (SA), a shift from value at risk (VaR) 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 IMA 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 (NMRFs).

FRTB overhauls the standardised approach that will be used for banks that want a simple and straightforward model and is also the fall back 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.

The replacement of VaR 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 VaR in the current market risk framework and are designed to mitigate the risk of a sudden and severe impairment of market liquidity across asset classes.

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 has been pushed back

Banks will need to upgrade their market data infrastructure to meet FRTB’s market data, lineage, audit and volume requirements in a cost-effective manner. Asset Control provides deployed and hosted solutions for risk factor preparation including off-the-shelf integration with data providers, business rules to derive risk factors, proxy gaps, cross-reference to internal data and Basel taxonomies and test modellability. Asset Control provides insight-driven data management through highly scalable, NoSQL based, cloud-deployed technology for data exploration and processing.

www.asset-control.com/solutions/regulatory-solutions/
to 2022 and details of some FRTB rules have yet to be finalised by regulators, banks need to consider the data management challenges posed by the regulation now and begin to review internal systems and controls to ensure they meet the requirements on time.

One of the key challenges already identified by firms within the scope of the regulation are NMRFs. Once banks have passed the P&L attribution and back testing requirements associated with using IMA, they need to identify whether their risk factors are either modellable or non-modellable.

If a risk factor does not have at least 24 ‘real’ prices with no more than one month between each observation over a year it is classified as non-modellable. Real prices include executed trades and committed quotes. For OTC markets with little transparency, the process of collecting real price data becomes a significant challenge.

A consultation paper issued by the BCBS on March 22, 2018–Revisions to the Minimum Capital Requirements for Market Risk–aimed to address issues that the Basel Committee identified in the course of monitoring the implementation and impact of the market risk standard issued in January 2016, Minimum Capital Requirements for Market Risk, or FRTB.

The paper does not resolve the problem of real price observations for NMRFs, but does propose changes including:

Changes to the measurement of the SA to enhance its risk sensitivity, including changes to FX risk; recalibration of SA riskweights applicable to general interest rate risk, FX risk and equity risk.

Revisions to the assessment process to determine whether a bank’s internal risk management models appropriately reflect the risks of individual trading desks.

Clarifications on the requirements for identification of risk factors that are eligible for internal modelling.

Clarifications on the scope of exposures that are subject to market risk capital requirements.

Despite the Basel FRTB framework implementation deadline of January 2022, there are some inconsistencies between regional implementation timelines.

In the EU, FRTB was due to come into force under CRR2, which was implemented within the EU Banking
Union Package (CRD V) on June 27, 2019. However, that doesn’t incorporate the full FRTB framework, due to timing constraints. Most of the technical requirements therefore have to be specified via ‘Delegated Acts’. The European Banking Authority (EBA) is expected to publish draft technical standards on the P&L attribution test, liquidity horizons, backtesting, and risk factor eligibility test by March 2020; on reporting standards by June 2020; and on the capitalisation of non-modellable risk factors (NMRFs), and the probability of default/loss given default estimation in the Default Risk Charge (DRC) model, by December 2020.

The CRR II reporting requirement for FRTB’s standardised approach (SA) is expected to be mandated in a delegated act by December 2019, with a start date of December 31, 2020. The start date for internal model approach (IMA) reporting arrives two years later on December 31, 2022 (and could be later) – a full year after the BCBS FRTB implementation deadline of January 1, 2022. Even then, this is only the reporting of a number, in parallel with binding capital requirements, which will continue to be calculated according to current CRR requirements.

The EU is also beginning work on CRR III – which will make FRTB a binding capital requirement. The EBA’s FRTB impact assessment results for CRR III are expected by September 30, 2019. The European Commission is then scheduled to publish its CRR III proposal, and the legislative process for CRR III is expected to kick off in the middle of 2020.
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’ personal information 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 residing 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, which are in 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 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 group 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.

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 are no longer 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 18, 2016. It took effect in all member states on May 25, 2018.

However, take-up appears slow. Research published in September 2019 by software firm Egress suggests that over half (52%) of UK firms are not yet compliant, opening them up to severe penalties should they be found guilty of a data breach. In July 2019 a similar survey by tax consultancy RSM found that 30% of European businesses were not confident that they were compliant, with many saying that GDPR was no longer a key focus and compliance activity had tailed off after the implementation deadline with a “close enough” attitude taking over.

This attitude could be imprudent, especially as signs point to a crackdown by the regulators. In February 2019 the FCA and the Information Commissioner’s Office (ICO, the data protection watchdog) signed a revised MOU to exchange information related to potential failures of systems and controls in relation to data security and related investigations, including GDPR. The ICO’s Regulatory Action Policy 2018 also specifically prioritises “large scale data and cyber security breaches involving financial or sensitive information”, suggesting that 2019 could see greater scrutiny and more coordinated investigations into poor financial information handling practices.

Affected firms will also be interested to see whether the European Data Protection Board’s planned guidelines on the Second Payment Services Directive (PSD2), expected in 2019, provide any further clarity on how PSD2 will operate alongside GDPR.
Significant Milestones

January 1, 2013: IFRS 13 takes effect
January 1, 2018: IFRS 9 takes effect

Key Links


Description and Data Requirement

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 analyses to identify any changes and adjust accounts accordingly.

IFRS 13 focuses on the definition of ‘fair value’ and includes guidelines on how firms should conduct asset 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 date. Firms need a clear understanding of this market-based measurement to ensure they gather the correct data for accurate reporting and disclosure.

At a Glance

Regulation: International Financial Reporting Standards (IFRS)
Regulatory Authority: IASB
Target Market Segment: Financial institutions
Core Requirements: Asset classification, measurement, fair value determination
Delivering business insight to financial technology executives

Become a member and receive weekly content updates, free content downloads and exclusive invites to our webinars and summits at: www.a-teaminsight.com/membership

@ATeamInsight
Search: A-Team Insight
www.a-teaminsight.com
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 EU, the first AML Directive was adopted in 1990 and the legislation has since undergone multiple revisions. In May 2018, the EU Council approved the fifth and latest AML Directive, which is due to come into force on January 10, 2020.

Key Links


At a Glance

**Regulation:** Know Your Customer (KYC)

**Regulatory Regime:** Multiple

**Target Market Segment:** Global financial institutions

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

Know Your Customer and related Anti Money Laundry regulations continue to put a tight grip on businesses. In particular prepaid card issuers and co-brand issuers need to document that the end customer has passed all checks. The same applies for remittance processors, P2P payment/lending platform providers, and effectively any player that ‘touches’ consumer payments and funds transfers. TLM Aurora enables issuers to detect issues as well as to resolve them in an automated, controlled and audited way.

www.smartstream.com
and imposes a number of additional obligations.

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. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 was introduced to ensure the UK’s AML regime complied with the EU’s fourth AML Directive and the Financial Action Task Force’s standards and recommendations, requiring a number of new obligations including a written firm-wide risk assessment and substantially more comprehensive client due diligence including the requirement to identify the beneficial owner of a client.

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 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 on boarding. 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 on boarding.

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.

The Legal Entity Identifier (LEI) and hierarchy data provided by the Global LEI Foundation (GLEIF) are essential here to support an understanding of relationships between entities.

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

Solutions available for KYC include managed services that build and maintain client records on behalf of financial institutions and 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 utility service. Machine learning solutions that automate data collection for onboarding and KYC compliance are emerging.

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).

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

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.

MAR is also closely linked to Markets in Financial Instruments Directive II (MiFID II). Both regulations are designed to strengthen investor protection, maximise market transparency and reduce market abuse, and their requirement overlaps are intentional.

These include the need for surveillance systems and controls to monitor for behaviour that may constitute market abuse and to help monitor for and deliver best execution; record keeping of all trade communications including telephone calls; a review of remuneration policies to phase out remuneration that may cause conflicts of interest; and comprehensive reviews of compliance functions to ensure staff can meet all requirements.
MAR and MAD

An effective regulatory change programme will map requirements across various regulations including MiFID II and MAR.

There is some concern over the requirements for MAR compliance should the UK depart the EU. To pre-empt this, in February 2018 the UK Treasury laid Statutory Instrument 2019 No. 310 (SI) that made the Market Abuse (Amendment) (EU Exit) Regulations (UK MAR). UK MAR retains the same scope of financial instruments admitted to trading or traded on UK and EU trading venues. Requirements on market soundings, insider lists, and the prohibitions on the unlawful disclosure of inside information, insider dealing, and market manipulation remain the same. However, issuers with instruments trading on a UK venue are subject to some additional reporting requirements, must send the FCA notifications of delayed disclosure of inside information, must get FCA consent when delaying disclosure, and must send the FCA manager (PDMAR) transaction reports directly. In February 2019 the FCA clarified that MAR was one area where it would expect firms and other regulated entities to take reasonable steps to comply with the changes to their regulatory obligations by exit day.
**Margin Requirements – BCBS/IOSCO**

**Significant Milestones**
- **September 2, 2013:** Initial framework
- **March 18, 2015:** Revised framework
- **September 1, 2016:** Initial and variation margin deadline for large market participants
- **March 1, 2017:** Variation margin deadline for market participants that are not large
- **March 5, 2019:** Statement on final implementation phases
- **July 23, 2019:** Final implementation extended

**Dates for Diary**
- **September 1, 2017–2021:** Initial margin deadline phased in for all market participants
- **September 2020:** Additional implementation phase
- **September 1, 2021:** Final implementation phase

**Key Links**
- **March 2015 Text:** www.bis.org/bcbs/publ/d317.pdf
- **Summary of Revisions:** www.bis.org/bcbs/publ/d317_summarytable.pdf
- **March 2019 final implementation statement:** https://www.bis.org/press/p190305a.htm
- **July 2019 final implementation extended:** https://www.bis.org/bcbs/publ/d475.pdf

**Description and Data Requirements**
The framework for margin requirements for non-centrally cleared derivatives was 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.

**At a Glance**
- **Regulation:** Margin requirements for non-centrally cleared derivatives
- **Regulatory Authorities:** BCBS and IOSCO
- **Target Market Segment:** Global financial institutions
- **Core Requirements:** Margin calculation
Margin Requirements – BCBS/IOSCO

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.

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.

In March 2019, BCBS and IOSCO made a statement on the final implementation phases of the margin requirement to provide clarity and smooth implementation. The statement noted that market participants may need to amend derivatives contracts in response to interest rate benchmark reforms. Amendments to legacy derivative contracts pursued solely for the purpose of addressing interest rate benchmark reforms do not require

TLM Collateral Management has been designed to handle the new business practices arising out of IOSCO Uncleared Margin Rules (UMR) Phase 1-6, such as Central and Client Clearing, Group Thresholds, support for net and gross initial and variation margins, currency-based margining, mismatch haircuts, wrong-way risk and asset concentration management, rehypothecation tracking plus flexible interfaces that can be configured as regulations and best practices evolve.
the application of the margin requirements for the purposes of the BCBS/IOSCO framework, although the position may be different under relevant implementing laws.

In the remaining phases of the framework’s implementation in 2019 and 2020, initial margin requirements will apply to a large number of entities for the first time, potentially involving documentation, custodial and operational arrangements. The statement notes that the framework does not specify documentation, custodial or operational requirements if the bilateral initial margin amount does not exceed the framework’s €50 million initial margin threshold. It is expected, however, that covered entities will act diligently when their exposures approach the threshold.

Most recently, in July 2019, the BCBS and IOSCO revised the framework. Relative to the 2015 framework, the revisions extend by one year the final implementation of the margin requirements. With this extension, the final implementation phase will take place on September 1, 2021. To facilitate this extension, the Basel Committee and IOSCO have also introduced an additional implementation phase that begins on September 1, 2020.
MiFID II

At a Glance

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

**Regulatory Regime:** EU

**Target Market Segment:** Global financial institutions

**Core Requirements:** Data transparency, investor protection, pre-trade pricing, trade and transaction reporting

---

### Significant Milestones

- **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
- **September 28, 2015:** ESMA publishes final report on Regulatory Technical and Implementing Standards
- **February 10, 2016:** European Commission proposes one-year delay
- **June 7, 2016:** European Parliament confirms delay
- **November 10, 2016:** ESMA issues draft Regulatory Technical Standards for package orders
- **July 3, 2017:** Deadline for EU countries to implement directive in local legislation
- **January 3, 2018:** Compliance deadline

---

### Dates for Diary

2019: ESMA expected to review MiFID II if Brexit negotiations fail

---

### Key Links:

- **Text:** eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0065
- **Timeframe:** www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

---

### Description and Data Requirements

Markets in Financial Instruments Directive II (MiFID II) came into force on January 3, 2018, representing one of the biggest changes in regulatory oversight of financial markets for a decade. The regulation extends the remit and scope of its predecessor, the original MiFID that was introduced in 2007, and aims to improve the competitiveness of European markets by creating a single transparent market for investment services and activities, and ensuring harmonised investor protection across Europe.

The regulation amends many previous 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.

MiFID rules that were limited to equities trading on regulated platforms are extended to equity-
like and non-equity instruments traded on any trading platform, including multilateral trading facilities (MTFs) and organised trading facilities (OTFs), with a view to ensuring that all trading takes place on regulated platforms. Systematic internalisers that trade OTC derivatives are subject to expanded transparency obligations.

With transparency a key objective of MiFID II, the regulation makes sweeping changes to the pre- and post-trade transparency of EU financial markets, requiring trading venues to make pre-trade bid and offer prices public, and retaining the requirement for trading venues to make public the price, volume and time of transactions as close to real-time as is technically possible.

In MiFID II, the European Securities and Markets Authority (ESMA) proposes a maximum permissible delay for publication that should ultimately be reduced to one minute in respect of equities and equity-like instruments, and five minutes for non-equities. The regulation also includes exacting best execution rules, requiring firms to prove to regulators that they have achieved best execution for their individual clients.

The regulation includes several new mechanisms, particularly around pre-and post-trade reporting and including the European Securities and Markets Authority’s (ESMA) Financial Instruments Reference Data System (FIRDS), Approved Publication Arrangements (APAs) and Approved Reporting Mechanisms (ARMs).

It also details a framework for market data that includes standards, such as International Securities Identification Numbers (ISINs) to identify securities and, for the first time, OTC derivatives, and Legal Entity Identifiers (LEIs) to identify issuers and counterparties to transactions.

The MiFID II mandate sets aggressive time limits on publishing and reporting pre- and post-trade data. It also introduces controls for algorithmic trading that are designed to provide safeguards and reduce systemic risk, and includes regulation of algorithmic traders, including high frequency algorithmic traders, and their market making strategies.

Another key element is the unbundling of research services provided by sell-side institutions to their buy-side clients and execution fees. This clarifies the cost of research, avoids the offer of research as an inducement to trade with the research provider, and lists
direct costs as line items, thereby improving transparency.

The regulation’s proposal to introduce a consolidated tape that pulls together trade data of financial instruments from regulated markets, MTFs, OTFs and APAs, and consolidates the data into a continuous electronic live data stream providing price and volume data per financial instrument has yet to be realised, although a tape, or maybe two or three tapes, is expected to be created, most probably by a large data vendor. This would increase the transparency of investment markets and mark a step change in how market data is distributed.

Since MiFID II went live on January 3, 2018, it has not all been plain sailing, with many firms reviewing and reworking tactical MiFID II solutions with a view to building cost-efficient and sustainable compliance systems. They have also had to implement elements of the regulation that were not required at go live.

For example, the deadline for best execution reporting kicked in at the end of June 2018, the implementation of Legal Identify Identifiers (LEIs) for counterparties was delayed from January to July 2018, and the formation of a mandatory systematic internaliser regime took place in September 2018. A deferral of requirements around derivatives clearing will not bring the regulator’s concept of open access clearing to market until July 2020.

In April 2019 the European Parliament also adopted a regulation on the prudential requirements and a directive on the prudential supervision of investment firms (IFR/IFD), introducing new prudential requirements depending on activity and asset size. “Systemically relevant” firms now fall under the CRD/CRR regime, while all other investment firms (as defined by MiFID II) come under the new regulation and are no longer subject to CRD/CRR. IFR/IFD also revises the MiFID II/MiFIR third-country regime for investment services: strengthening the requirements for equivalence decisions and the supervision of firms with parent companies in third countries. The changes are due to MiFID II requires firms to keep much more granular execution venue, counterparty and financial instrument information. Asset Control provides a comprehensive data model that tracks data vendor changes and regulatory developments including post-trade reporting requirements. Asset Control’s Managed Services solution AC PaSS delivers proactive and targeted sourcing, integration with data providers and DSB for trade enablement and regulatory reporting. Operational monitoring views are provided to track data quality and delivery against pre-defined KPIs and SLAs.

www.asset-control.com/solutions/regulatory-solutions/
Your trusted data partner. Today and tomorrow.

Outsource the burden of counterparty data

Would you rather run your business on entity data from differing and often unreliable sources, or appoint an expert data provider trusted by the financial industry the world over?

With SWIFTRef, you can be confident you meet regulatory requirements, safe in the knowledge that your data is robust, comprehensive and always up-to-date.

Learn more at swift.com/swiftref.
MiFID II

be transposed into national law by end-2020.

From a data management perspective the challenges of MiFID II implementation have been huge in terms of sourcing and integrating data, managing data quality, accuracy and timeliness, and adjusting to an evolving regulation. Outstanding regulatory problems, such as inefficient operation of the FIRDS database, have added to the data management challenge.

That said, a strategic approach to MiFID II will deliver business and operational benefits overtime. Many firms note early operational gains resulting from IT infrastructure changes required to achieve compliance, as well as new business opportunities from data sources and datasets generated by the regulation, while a better understanding of data and clients will foster improved business processes.

It should be noted that the UK’s FCA stated in its Business Plan for 2019-20 that a priority would be to examine how investment firms were implementing MiFID II and to build on the use of MiFID II transaction reporting data to help combat market abuse. The FCA also plans to consult on a new prudential regime for MiFID investment firms, aligned to the EU Investment Firms Directive and Regulation (IFD/IFR, expected to be in operation for 2020/21, and will publish a consultation paper in the second half of 2019.

MiFID II and MiFIR transparency obligations require access to significant quantities of reference data for each financial product traded in Europe. The SmartStream Reference Data Utility provides all of the reference data needed for pre-trade price transparency, post-trade reporting and transaction reporting.

MiFID II and MiFIR now require greater controls and governance across all instrument types. The new, wider set of mandatory data is just one of the more testing regulations that SmartStream’s Reconciliations solutions can resolve.

www.smartstream.com
Financial institutions are critically dependent on high quality reference data to ensure that they can successfully trade electronically, automate their operations and report accurately to regulators. Large institutions spend millions of dollars to improve data quality, fix data issues and manage the exceptions that occur due to bad data.

The SmartStream Reference Data Utility (RDU) offers a simple solution to satisfy those complex reference data needs, by providing a high quality security master built using industry best practices. The RDU is the product of an initiative developed in close association with demanding global institutions and has been proven to deliver dramatically better quality data.

Transform your business today, contact us on:
info@smartstreamrdu.com
MIFIR

At a Glance

Regulation: Markets in Financial Instruments Regulation (MiFIR)
Regulatory Regime: EU
Target Market Segment: Global financial institutions
Core Requirements: Pre- and post-trade data transparency, transaction reporting

Significant Milestones

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
January 3, 2018: Compliance deadline
September 26, 2018: ESMA updates Q&A on MiFIR reporting
April 9, 2019: ESMA updates Q&A on MiFIR data reporting
July 11, 2019: ESMA updates Q&A on MiFIR and MiFID II investor protection and intermediaries

Key Links:

Background and Timeframe: www.esma.europa.eu/policy-rules/mifid-ii-and-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 the EU.

While MiFID II focuses on market infrastructure, MiFIR builds out transaction reporting requirements by setting out a number of new reporting obligations, and complements the directive’s commitment to trading data transparency.

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 European Securities and Markets Authority (ESMA) has stipulated that transactions must be reported using the ISO 20022 formatting standard. Firms will need to accommodate this standard, which will be used to submit data from all stages of order execution to relevant regulatory authorities.

From a trader’s perspective, MiFIR has extensive implications for disclosure practices. Relevant data to include in a report might involve the bid and offer prices and the extent to which the parties invested in the trade, the volume and time of the trade execution, and any noted systemic issues.

The public and regulatory authorities must be made aware of this information on instruments such as equities, over-the-counter (OTC) and exchange-traded derivatives (ETD) on a continuous basis for transparency purposes. MiFIR does have exemptions relating mainly to the volume of a trade. For example, there are exemptions on regulating block trades and trades exceeding a specific size regarding certain instruments.

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 prices, quotes, execution times and volumes must be published publically. The extension of trade and transaction reporting to additional asset classes means firms must submit more information to regulatory authorities via Approved Publication Arrangements (APAs) and Approved Reporting Mechanisms (ARMs).

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.
At a Glance:

**Regulation:** European Money Market Funds Regulation (MMFR)

**Regulatory Regime:** EU

**Target Market Segment:** Fund managers

**Core Data Requirements:**
- Customer identity
- Bi-annual stress testing
- Daily asset valuation
- Secondary pricing
- Market data

Significant Milestones:

- **September 4, 2013:** Proposal on MMFR presented to European Commission
- **November 14, 2016:** Agreement on draft regulation reached between EU Council and European Parliament
- **April 5, 2017:** EU Parliament approves regulation
- **May 16, 2017:** EU Council formally adopts regulation
- **July 21, 2018:** Regulation comes into force for new funds

Dates for Diary:

- **January 21, 2019:** Regulation comes into force for existing MMF – move into significant milestones
- **October 2019:** Asset managers report to their national competent authority
- **Q1 2020:** MMF managers start quarterly reports of stress testing to national competent authorities

Key Links:

- **Full Text:** eur-lex.europa.eu/eli/reg/2017/1131/oj
- **ESMA Technical Advice and Guidelines:**

Description and Data Requirements:

In 2013, the European Commission proposed legislation to regulate money market funds (MMFs) in response to G20 commitments following the financial crisis. An MMF invests in short-term debt, such as treasury bills, commercial paper and certificates of deposit, and is an important short-term financing instrument for financial institutions and a short-term cash management channel for corporations.

The regulation aims to preserve the integrity and stability of the EU market by making MMFs more resilient, while protecting investors by reducing the disadvantages for late redeemers in stressed market conditions. It expands on the Committee of European
Securities Regulators (CESR) money market fund guidelines of 2010.

European Money Market Funds Regulation (MMFR) came into force on July 21, 2018 for all fund launches. Existing MMFs were given an additional six months to comply with a final implementation deadline of January 21, 2019. On June 11, 2018 Her Majesty’s Treasury published the UK Regulations, which also came into force on July 21, giving the Financial Conduct Authority (FCA) power to investigate and enforce MMFR breaches.

The MMFR applies to all MMFs managed and/or marketed in the EU: including variable net asset value (VNAV) funds, constant net asset value (CNAV) funds, and low volatility net asset value (LVNAV) funds. It requires MMF managers to report information to the authorities on a quarterly basis, which is then made available to the European Securities and Markets Authority (ESMA) for the purposes of creating a central database.

The regulation introduces stringent new liquidity management requirements to ensure that all MMFs maintain sufficient liquid assets to meet any sudden withdrawal of investment. LVNAVs and CNAVs must hold at least 10% of assets that mature within one day and 30% that mature within one week; while VNAVs are required to hold at least 7.5% of assets that mature within one day and 15% within one week.

It also introduces rules on portfolio diversification and valuation of assets. Funds are allowed to invest no more than 5% of assets in money market instruments issued by the same body, no more than 10% of assets in deposits made with the same credit institutions, and no more than 17.5% of assets in other MMFs (to prevent circular investments).

The regulation sets a 15% limit on reverse repurchase agreements with the same counterparty, as well as specific limits on covered bonds and deposits, and it prohibits MMFs from receiving financial assistance from other financial institutions (especially banks).

Investment requirements limit eligible assets and prohibit the use of techniques such as short-selling, securities lending and borrowing, while new valuation rules limit the use of amortised cost methods. Risk management requirements impose biannual stress testing and internal assessment procedures to determine credit quality, while MMF managers are required to implement Know Your Customer (KYC) policies and supply surveillance information to the authorities.
In March 2018, ESMA released draft guidelines for MMF stress testing, which are to be updated on an annual basis. On September 28, 2018 ESMA launched a public consultation on internal stress testing for European MMFs, closing on December 1, 2018, with new guidelines expected in Q1 2019.

Guidelines resulting from this consultation were issued on July 19, 2019. There are two sets of guidelines regarding the stress testing of MMFs and reporting on MMFs to national competent authorities. The guidelines on stress testing establish common reference parameters of the stress test scenarios MMFs or managers of MMFs should include in their stress scenarios. The guidelines on reporting provide guidance on how to fill in the reporting template on MMFs that managers of MMFs must transmit to competent authorities as of Q1 2020.
Significant Milestones

February 7, 2013: Initial European Commission proposal on cybersecurity
July 6, 2016: European Parliament adopts directive
August 2016: Enters into force
May 9, 2018: Deadline for directive to be transposed into national legislation
June 2018: Compliance deadline
November 9, 2018: Deadline to identify operators of essential services

Key Links


Description and 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 must transpose the directive into national legislation by May 9, 2018 and identify operators of essential services by November 9, 2018. These include 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. The directive requires them to take appropriate security measures and report serious incidents to national authorities.

As cybersecurity threats are evolving fast, the European Commission is encouraging swift implementation of the directive and in September 2017 adopted a communication that aims at supporting member

At a Glance

Regulation: Network and Information Security (NIS) Directive
Regulatory Regime: EU
Target Market Sector: Global financial institutions
Core Requirements: Security, reporting
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.

Since it was established under the NIS directive, the cooperation group has published five working documents, which result from its first biennial work programme running from 2018 to 2020. The first focuses on security measures for operators of essential services and the second on incident notification for operators of essential services. The other three documents include a reference document on the identification of operators of essential services, a compendium on cybersecurity of election technology, and a cybersecurity incident taxonomy.
### 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  
**November 16, 2016:** European Commission postpones compliance deadline  
**March 8, 2017:** Revised RTS is published  
**April 3/4, 2017:** European Council and Parliament approve revised RTS  
**January 1, 2018:** Compliance deadline  
**November 8, 2018:** ESMA and EBA consultation on amendments to PRIIPs KID  
**February 8, 2019:** ESAs publish final recommendations following consultation

### Dates for Diary

**December 31, 2019:** UCITS regulated by PRIIPs

### Key Links

- **Text:** eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R1286  
- **Summary:** eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32014R1286  
- **Consultation paper on PRIIPs KID:** https://eiopa.europa.eu/Publications/Consultations/Consultations/Joint%20Consultation%20Paper%20on%20targeted%20amendments.pdf  
- **ESAs publish final recommendations:** https://eiopa.europa.eu/Publications/Reports/2019-02-08%20Final_Report_PRIIPs_KID_targeted_amendments%20%28JC%202019%20%26%29.pdf

### 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.
PRIIPs

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) meets 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.

The PRIIPs compliance deadline was initially slated for December 31, 2016, but in November 2016, the European Commission postponed the deadline by a year, moving it to January 1, 2018 and aligning compliance with that of Markets in Financial Instruments Directive II (MiFID II).

The Commission’s decision to postpone PRIIPs, and the creation of associated KIDS, was driven by a European Parliament vote in September 2016 against the Level 2 Regulatory Technical Standards (RTS) on the KIDS element of the regulation. The Economic and Monetary Affairs (ECON) Committee of the European Parliament rejected the RTS ahead of the European Parliament vote.
After a review of the RTS, the Commission published a final iteration in March 2017. The European Council approved the revised version on 3 April 2017, along with the European Parliament, ensuring the January 1, 2018 PRIIPs compliance deadline.

Since then, in November 2018, the European Supervisory Authorities (ESAs) published a consultation paper on targeted amendments to the PRIIPs KID. A final report based on the consultation was published in February 2019.

The report notes that feedback to the consultation paper did not support the proposed targeted amendments. On this basis, the ESAs decided it was not appropriate to propose substantive amendments to PRIIPs. Instead, they initiated work to provide input to a review of PRIIPs during 2019, which is ongoing.
At a Glance

Regulation: Consolidated Audit Trail (CAT)
Regulatory Regime: SEC
Target Market Sector: National securities exchanges, broker-dealers
Core Requirements: Securities reporting

Significant Milestones

July 11, 2012: SEC adopts Rule 631
February 26, 2013: SEC issues RFP for the CAT
November 15, 2016: SEC approves NMS CAT plan
January 2017: Thesys Technologies selected as CAT plan processor
November 15, 2018: SROs expected to report to the CAT
February 1, 2019: Thesys Technologies to be replaced
Early March 2019: CAT NMS selects FINRA as plan processor

Dates for Diary

December 16, 2019: Testing environments open for equities and options
April 2020: First phase of reporting goes live
July 2022: All phases of reporting live

Key Links

SEC adopts CAT: www.sec.gov/divisions/marketreg/rule613-info.htm
CAT NMS plan: www.catnmsplan.com/home/about-cat/cat-nms-plan/

Description and Data Requirements

The US consolidated audit trail (CAT) results from the SEC’s July 2012 adoption of Rule 613 of Regulation National Market System (NMS). The rule required self-regulatory organisations (SROs) to jointly submit a plan – the NMS plan – to create, implement and maintain a CAT.

The rule mandated that the NMS plan should require national securities exchanges and the Financial Industry Regulatory Authority (FINRA) to provide detailed information to a central repository – the CAT – covering each quote and order in an NMS security, and each reportable event with respect to each quote and order, such as origination, modification, cancellation, routing and execution.

The rule allows the SROs to determine the specifics of how market participants report data to the repository and to select a plan processor to create and operate the CAT. The SEC posted a request for proposal (RFP) for the
CAT in February 2013. In January 2017, the SROs selected Thesys Technologies to build the CAT, despite expectations that FINRA, operator of the predecessor to the CAT, the Order Audit Trail System (OATS), would win the bid.

The Thesys build did not make good progress and in a statement on February 1, 2019, the CAT NMS noted that the project would transition to a new plan processor. Early in March 2019, the CAT NMS selected FINRA as plan processor for the CAT and released updated industry member technology specifications and industry member technical specifications scenarios.

The task of reporting to the CAT is huge, with about 58 billion data points being collected every day when the system is in full operation. Data management challenges include the requirement for broker-dealers and national securities exchanges to report data to the CAT repository by 8 am Eastern Time the following trading day for analysis by regulators. SROs and their members must synchronise clocks to record the date and time of reportable events and timestamp the events. Data quality and the use of personal customer information are also at issue.

While first phase reporting to the CAT – covering SROs – was initially due to begin on November 15, 2017, the late development of the solution and replacement of the plan processor pushed reporting deadlines back.

Plans now show testing environments for file submission and data integrity validation opening for equities and options on December 16, 2019. Reporting will be phased in from April 2020, depending on asset class, size of firm and data type, and should be complete by July 2022, when the production environment for customer and account information is due to go live.

Section 31 is a fee assessed by the SEC to SROs and national securities exchanges to recover the costs of supervising and regulating markets and securities professionals. SmartStream has fully implemented support for the automated calculation, accounting, billing and collection, and payment for Fees and Expense Management platforms.

www.smartstream.com
At a Glance

**Regulation:** Current Expected Credit Loss (CECL)

**Regulatory Regime:** SEC

**Target Market Sector:** Financial institutions

**Core Data Requirements:** Accounting data including past events, current conditions, reasonable and supportable forecasts

Significant Milestones

- **June 2016:** FASB introduces CECL model
- **July 17, 2019:** FASB proposes to extend implementation date for all firms except large SEC filers to January 2023

Dates for Diary

- **January 2020:** Effective data for public businesses entities that are SEC registered
- **January 2021:** Current effective data for public business entities that are not SEC registered, could move to 2023
- **January 2022:** Current effective data for non-public business entities, could move to 2023

Key Links


Description and Data Requirements

The Current Expected Credit Loss model (CECL) is an accounting model the Financial Accounting Standards Board (FASB) issued for the recognition and measurement of credit losses for loans and debt securities. It is designed to help investors understand managers’ estimates of expected credit losses and should result in financial reporting that better reflects managers’ expectations and institutions’ credit risk info.

The standard is planned to take effect for Securities and Exchange Commission (SEC) registrants’ 2020 financial statements and for firms that are not SEC registrants in 2021, although FASB proposals made suggest moving all reporting except for large SEC files out to 2023.

CECL is expected to have far-reaching implications and play a role in supporting business decisions. Its anticipated impact is driving financial institutions to consider replacing traditional spreadsheets and legacy systems with a more responsive, configurable platform with enabling tools and credit model options to sustain a CECL framework.

The FASB change replaces the ‘incurred loss’ accounting model with the CECL ‘expected loss’
model, and requires banks to record amounts they do not expect to collect in the allowance for loan and lease losses (ALLL) and in an allowance for credit losses on held-to-maturity debt securities.

Banking regulators have referred to CECL as ‘the biggest change ever to bank accounting’, as the standard is expected to have a huge impact on the costs to prepare and audit the ALLL, how investors analyse the ALLL, and how banks manage their capital.

The standard is likely to affect a financial institution’s technology needs, approaches and investments, and require design and development of a new platform. It also requires significant changes to the data a bank maintains and analyses, including more granular data and new performance metrics.
SEC Forms N-PORT and N-CEN

At a Glance
- **Regulation:** Forms N-PORT and N-CEN
- **Regulatory Regime:** SEC
- **Target Market Sector:** Registered investment companies
- **Core Requirements:** Risk metrics, exchange-traded funds and securities lending data

**Significant Milestones**
- **October 13, 2016:** SEC adopts new rules and forms
- **June 1, 2018:** N-PORT compliance for larger funds groups with net assets of $1 billion or more
- **June 1, 2018:** N-CEN compliance
- **April 30, 2019:** N-PORT reporting for larger funds groups
- **April 30, 2020:** N-PORT reporting smaller funds groups

**Key Links**
- **SEC reporting modernisation:** www.sec.gov/rules/final/2016/33-10231.pdf
- **SEC proposed rules:** www.sec.gov/rules/proposed/2015/33-9776.pdf

**Description and Data Requirements**
The Securities and Exchange Commission (SEC) Forms N-PORT (portfolio) and N-CEN (census) are designed to modernise the reporting and disclosure of information by registered investment companies. Form N-PORT requires certain registered investment companies to report information about their monthly portfolio holdings to the SEC in a structured data format. Form N-CEN requires registered investment companies, other than face-amount certificate companies, to report annually certain census-type information to the SEC in a structured data format.

The forms came into effect in January 2017 and were accompanied by amendments to Regulation S-X, which requires standardised, enhanced disclosure about derivatives in investment company financial statements; amendments to Forms N-1A, N-3 and N-CSR to require certain disclosures regarding securities lending activities; and the recision of Forms N-Q and N-SAR.

Collectively, the new forms and amendments are part of the SEC’s modernisation plan and designed to improve the information the SEC receives from investment companies and help it to better fulfil its mission of protecting investors, maintaining fair, orderly and efficient markets, and facilitating capital formation.

From a data perspective, Form N-PORT requires more portfolio level information than its predecessor Form N-Q. The additional reporting data is expected to improve risk analyses and other oversight by the SEC. It includes certain risk metric...
calculations that measure a fund’s exposure and sensitivity to changing market conditions, such as changes in asset prices, interest rates, or credit spreads. Reporting of a fund’s complete portfolio holdings on a position-by-position basis must be made on a trade date plus one day (T+1) basis.

Form N-CEN replaces the form previously used to report fund census information, Form N-SAR. Funds report at the registrant level and reports must be filed annually within 75 days of the end of a fund’s fiscal year, rather than semi-annually as required by Form N-SAR. Form N-CEN includes many of the same data elements as Form N-SAR, but to improve the quality and usability of information reported, replaces outdated items with items the SEC believes to be of greater relevance today.

Form N-CEN also streamlines and updates information reported to the SEC to reflect current information needs, such as requiring more information on exchange-traded funds and securities lending. Where possible, Form N-CEN eliminates items that are reported on other SEC forms, or are available elsewhere.

Funds must report portfolio and census information on Forms N-PORT and N-CEN using an XML structured data format, which improves the ability of the SEC and the public to aggregate and analyse information across all funds and to link reported information with information from other sources.
At a Glance

**Regulation:** Form Private Fund (Form PF)

**Regulatory Regime:** SEC

**Target Market Segment:** Private funds

**Core Requirements:** Fund assets, 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

---

**Key Links**

- **FAQs:** [www.sec.gov/divisions/investment/pfrd/pfrdfaq.shtml](http://www.sec.gov/divisions/investment/pfrd/pfrdfaq.shtml)

---

**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.

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.

The SEC cracked down on fund advisers that failed to submit Form PF for the first time in 2018, reporting in June 2018 that it had made settlements with 13 registered investment advisers that repeatedly failed to provide required information that the SEC uses to monitor risk. Without admitting or denying the findings, the advisers agreed to be censured, cease and desist, and each pay a $75,000 civil penalty.
SEC Rules 15c3-1, 15c3-3 and 17a-5

At a Glance

Regulation: Rules 15c3-1, 15c3-3 and 17a-5
Regulatory Regime: SEC
Target Market Sector: Broker-dealers
Core Requirements: Net capital calculations

Description and Data Requirements
SEC Rules 15c3-1, 15c3-3, 17a-5 are integral to the Commission’s Customer Protection Rule that seeks to avoid, in the event of a broker-dealer failure, a delay in returning customer securities or a shortfall in which customers are not made whole. This is done by requiring broker-dealers to safeguard both the cash and securities of their customers, and eliminating the use of customer funds and securities to finance broker-dealers’ overheads and certain other activities.

Rule 15c3-1 sets capital requirements for brokers and dealers. Under the rule, a broker or dealer must have sufficient liquidity to cover its most pressing obligations. This is defined as having a certain amount of liquidity as a percentage of the broker-dealer’s total obligations.

For customer cash, Rule 15c3-3 requires a broker-dealer to maintain a reserve of funds or qualified securities in an account at a bank that is at least equal in value to the net cash owed to customers. The rule also requires a broker-dealer to maintain physical possession or control over customers’ fully paid and excess margin securities.

Rule 17a-5 requires broker-dealers to file monthly Financial and Operational Combined Uniform Single (FOCUS) reports concerning customer reserve account requirements and the proper segregation of customer securities. It also requires broker-dealers to file compliance reports annually that contain a description of each material weakness in the internal control over compliance of the broker-dealers, and to notify the SEC when it learns of a material weakness that could result in a violation of Rule 15c3-3.

Broker-dealers must provide accurate information to the SEC on their compliance with the Customer Protection Rule, and must self-report certain failures to comply, or material weaknesses in controls that hinder compliance efforts.

Significant Milestones

July 30, 2013: SEC finalises amendments to broker-dealer financial responsibility requirements and financial reporting rules

Key Links

Regulatory Data Handbook 2019  97
SEC Rule 22e-4

Significant Milestones

**September 22, 2015:** SEC proposes reform of liquidity risk management  
**October 13, 2016:** SEC issues final rule  
**January 17, 2017:** Effective data  
**February 2, 2018:** SEC pushes out compliance deadline by six months  
**June 28, 2018:** SEC adopts a final rule on risk management programmes  
**June 1, 2019:** Compliance deadline for larger entities to implement a liquidity risk management programme

Dates for Diary

**December 1, 2019:** Compliance deadline for smaller entities to implement a liquidity risk management programme

Key Links


Description and Data Requirements

The Securities and Exchange Commission (SEC) voted to propose reforms that would enhance liquidity risk management at open-end funds, including mutual funds and exchange-traded funds (ETFs), in September 2015.

The resultant rule, Rule 22e-4, creates a regulatory framework to help funds design robust liquidity risk management programmes. The SEC’s goal is to reduce the risk of a fund being unable to meet its redemption obligations and to minimise dilution of shareholder interests by promoting stronger and more effective liquidity risk management across open-end funds. Put simply, the rule aims to ensure investors can redeem shares and receive assets in a timely manner.

After an industry comment period, the SEC adopted a final Rule 22e-4 in October 2016. The rule emphasises the need for mutual funds and ETFs to implement liquidity risk management programmes and details disclosure regarding fund liquidity and redemption practices.

Mutual funds and ETFs must classify their portfolios as highly liquid,
SEC Rule 22e-4

moderately liquid, less liquid or illiquid, and only 15% of a fund’s assets are permitted to be classified as illiquid.

This is a potential challenge, particularly in fixed income markets where only a small minority of securities trade regularly, but also an opportunity for mutual funds to improve operational procedures, reduce trading costs, and better understand their portfolios by elevating liquidity to a risk factor.

The initial Rule 22e-4 timeline, required all registered open-end investment companies, including open-end ETFs but not smaller entities, to adopt the rule and implement a written liquidity risk management programme, approved by a fund’s board of directors, by December 1, 2018.

Smaller entities, defined as funds with less than $1 billion in net assets, would follow six months later and implement liquidity risk management programmes by June 1, 2019. Money market funds are exempt from all the requirements of the rule and ‘in-kind ETFs’ are exempt from some requirements.

On February 22, 2018 the SEC adopted an interim final rule that revised the compliance date of rule 22e-4 by six months and provided further guidance for firms within the scope of the rule. The revised compliance date requires larger entities to be compliant on June 1, 2019, and smaller entities on December 1, 2019.

In addition to pushing forward Rule 22e-4 compliance, on June 28, 2018, the SEC adopted a final rule that requires funds to disclose information about their liquidity risk management programme in reports to shareholders. The SEC also amended Form N-PORT to enhance the liquidity information reported to the Commission.
Significant Milestones

**November 17, 2000:** SEC adopts Rules 605 & 606

**November 2, 2018:** SEC adopts amendments to Rule 606, with a deadline of May 2019

**April 30, 2019:** SEC extends the compliance date for Rule 606 amendments to begin September 30, 2019

**August 2019:** SEC issues new guidance on amendments to Rule 606

**September 4, 2019:** SEC grants delay to compliance reporting deadline

At a Glance

**Regulation:** Rule 606 (a) and (b) of the Regulation National Market System (NMS)

**Regulatory Regime:** US

**Target Market Segment:** Broker-dealers

**Core Requirements:** Data transparency, data consolidation, data lineage, trade and transaction reporting

Dates for Diary

**January 1, 2020:** Compliance deadline for Rule 606(a) for all broker-dealers

**January 1, 2020:** Compliance deadline for Rule 606(b) for broker-dealers engaging in self-routing activity

**April 1, 2020:** Compliance deadline for broker-dealers that outsource routing activity

Key Links


**Guidance:** https://www.sec.gov/tm/faq-rule-606-regulation-nms


Description and Data Requirements

In November 2000, the Securities and Exchange Commission (SEC) adopted two rules to standardise and improve public disclosure of execution and routing practices, as part of the Regulation National Market System (Regulation NMS), a set of rules designed to improve the US exchanges through improved fairness in price execution. Rule 605 required that all “market centres” trading NMS securities make available standardised, monthly reports containing statistical information about “covered order” executions. Rule 606 required broker-dealers routing customer orders in equities and option securities to publish quarterly reports providing a general overview of their routing practices.

In November 2018 the SEC adopted a set of amendments to Rule 606, requiring broker-dealers to provide enhanced disclosure of their routing practices – in part to encourage effective and competitive order
SEC Rule 606

handling and routing services, and in part (from a regulatory perspective) to better investigate the relationship between exchange and trading venue rebates and routing decisions.

The amendment separates orders into “held” (which must be executed immediately) and “not held” (which give the broker some level of time and price discretion) with different disclosure obligations for each. Upon customer request, the new Rule 606(b)3 requires broker-dealers to provide specific disclosures, within seven days, for the past six months regarding not held orders. This includes information such as fill rates, spread sizes, liquidity changes, net fees or rebates paid to and received from trading venues, and more.

Rule 606(a)(1) for held orders requires less detail, but enhances the order routing disclosures that broker-dealers must make publicly available on a quarterly basis – including:

- Splitting limit order information into marketable and non-marketable categories;
- More detailed disclosure of payments received from or paid to certain trading centres;
- Describing terms of payment for order flow arrangements and profit-sharing relationships; and
- Publishing the order routing reports on a website that is free and accessible to the public for a minimum of three years.

Firms must now publish both 606(a) and new 606(b)3 reports on a bi-annual and quarterly basis, respectively, in place of the lengthy legacy 606 report. And unlike the previous incarnation, which was accepted in almost any format, the SEC will only accept the new reports in XML or PDF.

Originally due for implementation May 2019 along with the rest of the amendments to Reg NMS, the SEC in April delayed the compliance deadline until September 30, 2019 in response to a request from the Financial Information Forum (FIF) for further clarification. In August, the SEC released new guidance, clarifying issues such as the definition of “discretion” and the definition of “venues”.

However, on August 2, 2019, prior to the release of the SEC guidance, FIF and the Security Traders Association (STA) filed a joint letter with the SEC requesting a further delay in implementation, and particularly warning that a lack of clarity around the process of reporting “look-through data” (data that indicates where the destinations are routing
flow and the fees/rebates paid to those destinations) was preventing stakeholders from moving forward with the implementation of Rule 606 in a manner that would “provide end-customers with consistent and accurate data.”

On September 4, 2019 the SEC acquiesced, extending the compliance deadline to January 1, 2020 for all broker-dealers for Rule 606(a) and for self-routing broker-dealers for Rule 606(b), and to April 1, 2020 for broker-dealers who outsource routing activity.

The onus of Rule 606 compliance falls heavily on the sell-side, and the delays to implementation have primarily been due to concerns over data availability. The SEC indicated in its initial 2018 amendment that much of this data was already available, but in fact the wider breadth of data combined with a lack of clarity on certain key issues has made compliance a serious concern for sell-side firms, who have complained that some of the requested data (such as fee and rebate information and look-through data) is simply not currently available.

With a further extension granted, firms must now focus on coordinating with their vendors and/or executing brokers to effectively consolidate all the required order execution data into a format that is effectively transferable into the new 606(a) and (b) formats, and into the completely new 606(b)3 report that is now required.
Section 871(m)

At a Glance

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

**Regulatory Authority:** US Internal Revenue Service

**Target Market Sector:** Global financial institutions

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

---

### Significant Milestones

- **2012:** IRS issues temporary and proposed regulations
- **September 17, 2015:** IRS issues final regulations
- **December 2, 2016:** IRS notice on guidance and clarification
- **January 1, 2017:** IRS sets effective dates for the regulations within Section 871(m)
- **September 21, 2018:** IRS defers the effective dates of several aspects of 871(m)

---

### Key Links


---

### 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
The IRS issued temporary 871(m) regulations in 2012, provided amended proposed regulations in 2013 and issued final regulations on September 17, 2015. In December 2016, the IRS issued Notice 2016-76, aiming to provide taxpayers with guidance and additional clarifications on the administration of, and compliance with, section 871(m) regulations.

The latest amendment to Section 871(m) was made on September 21, 2018, when the US Department of the Treasury and the IRS issued a notice announcing their intention to defer the effective dates of several aspects of the section 871(m) regulations, and extend certain related phase-in periods and transition rules.

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.

Equity-linked investments (ELIs) that fall within the scope of the regulations include swaps, options, futures, convertible debt, structured notes and other customised derivative products.
SFTR

**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 approved trade repository.

**Significant Milestones**
- **September 2013**: EU action plan on shadow banking
- **January 2014**: European Commission proposes SFT regulation
- **January 12, 2016**: Effective date
- **March 31, 2017**: Final ESMA report on implementing SFTR
- **July 24, 2018**: European Commission notifies ESMA of proposed amendments of RTS on reporting under SFTR
- **September 5, 2018**: ESMA publishes opinion rejecting amendments
- **March 22, 2019**: SFTR legally binding

**Dates for Diary**
- **April 14, 2020**: Reporting go-live for banks and investment firms
- **July 13, 2020**: Reporting go-live for CSDs and CCPs
- **October 12, 2020**: Reporting go-live for all other financial counterparties
- **January 11, 2021**: Reporting go-live for all non-financial counterparties

**Key Links**
- **Text**: [eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2365](eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2365)
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.

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.

The European Securities and Markets Authority (ESMA) issued its final Regulatory Technical Standards (RTS) on implementing SFTR in March 2017, detailing the rules for reporting SFTs to approved trade repositories. Broadly, the details of the report remain consistent with previous drafts, but there are changes in the final standards covering elements of the regulation including the generation of Unique Trade Identifiers (UTIs), collateral reporting timing, margin lending, use of the Legal Entity Identifier (LEI) and reportable fields.

Following publication, ESMA sent the final standards to the European Commission for endorsement.

A year later, in the summer of 2018, the Commission informed ESMA of its intention to endorse the RTS published in March 2017 but only if ESMA would make certain changes. In early September, ESMA declined to do this, pushing the decision on the adoption of SFTR back to the Commission.

The Commission is now expected to move forward with formal adoption.

SFTR includes 153 fields in post-trade reporting; topping EMIR’s 129 and MiFID II’s 65. It requires in-depth reporting on securities financing transactions. Asset Control provides a comprehensive data model that tracks data vendor changes and regulatory developments including post-trade reporting. Our Managed Services solution AC PaSS delivers proactive and targeted sourcing and integration with data providers to get the instrument data right for regulatory reporting. Operational monitoring views provide complete transparency to track data quality and delivery against pre-defined KPIs and SLAs.
of the rules and reporting could start in late 2019 or early 2020.

A year later, in the summer of 2018, the Commission informed ESMA of its intention to endorse the RTS published in March 2017 but only if ESMA would make certain changes. In early September, ESMA declined to do this, pushing the decision on the adoption of SFTR back to the Commission.

After the Commission and ESMA agreed the RTS, the seven delegated regulations and three implementing regulations comprising SFTR legislation were published in the Official Journal of the EU on March 22, 2019, making the regime legally binding. The reporting obligations were also set: April 14, 2020, reporting go-live for banks and investment firms; July 13, 2020, reporting obligation for CSDs and CCPs; October 12, 2020, reporting obligation for all other financial counterparties; January 11, 2021, reporting obligation for all non-financial counterparties.

Most recently, in May 2019, ESMA opened a public consultation on draft guidelines on how to report SFTs. The consultation paper seeks stakeholders’ views on key elements of future ESMA guidelines on reporting under SFTR. These guidelines will complement the SFTR technical standards and ensure consistent implementation of the SFTR rules. The consultation paper was accompanied by an open hearing on SFTR reporting on July 15, 2019.

ESMA is expected to consider feedback it receives from the consultation in the third quarter and publish a final report on the guidelines for reporting under SFTR in the fourth quarter of 2019.

The European Union (EU) Securities Financing Transaction Regulation (SFTR) aims to bring transparency to the securities financing markets by requiring both parties to an SFT to report new, modified or terminated SFTs to a registered trade repository. Each SFT trade report must include specific details about the security being traded and The SmartStream Reference Data Utility simplifies the sourcing of the essential security reference data required to enrich each SFT report.
Significant Milestones

**December 2013:** UK parliament legislates application of SMCR to banking sector

**October 2015:** UK Government announces all regulated firms will be subject to SMCR from 2018

**March 7, 2016:** SMCR takes effect

**March 7, 2017:** Banks complete certification

**July 2018:** FCA publishes proposals to extend SMCR to all FCA authorised firms

**December 9, 2019:** All FCA authorised firms must be compliant with SMCR

Dates for Diary

**December 2013:** UK parliament legislates application of SMCR to banking sector

**October 2015:** UK Government announces all regulated firms will be subject to SMCR from 2018

**March 7, 2016:** SMCR takes effect

**March 7, 2017:** Banks complete certification

**July 2018:** FCA publishes proposals to extend SMCR to all FCA authorised firms

**December 9, 2019:** All FCA authorised firms must be compliant with SMCR

Key Links


**FCA Policy Statement on Extension of SMCR to FCA Firms:** [www.fca.org.uk/firms/senior-managers-certification-regime](http://www.fca.org.uk/firms/senior-managers-certification-regime)

Description

The Senior Managers and Certification Regime (SMCR) was established uniquely in the UK in response to the 2008 banking crisis and significant conduct failings in the banking sector, such as the manipulation of Libor.

The government set up the Parliamentary Commission for Banking Standards (PCBS) to recommend how to improve standards in early 2013, and in turn, the PCBS recommended a new accountability framework focused on senior management. It also recommended that firms take more responsibility for employees being fit and proper, and that there be better standards of conduct at all levels in banking firms.

Based on these recommendations, Parliament passed legislation in December 2013, leading to the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) applying SMCR to the banking sector.

SMCR replaces the discredited Approved Persons Regime (APR) set down in the Financial Services and Markets Act (FSMA) and initially applied to UK banks, building
societies, credit unions, branches of foreign banks operating in the UK and the largest investment firms regulated by the FCA and PRA. An extension of the SMCR regime was made in 2015 to cover all firms authorised under FSMA.

Key features of SMCR include: an approval regime focused on senior management, with requirements on firms to submit robust documentation on the scope of these individuals’ responsibilities; a statutory requirement for senior managers to take reasonable steps to prevent regulatory breaches in their areas of responsibility, with the burden of proving misconduct carried by regulators; a requirement for firms to certify as fit and proper any individual who performs a function that could cause significant harm to the firm or its customers; and a power for regulators to apply enforceable Rules of Conduct to any individual who can impact their respective statutory duties.

SMCR became operational for banks, building societies, credit unions and PRA-regulated investment firms in March 2016. Banks were given until March 2017 to complete the certification of staff. The extension of the regime to cover all firms authorised under FSMA came into operation in 2018.

In the summer of 2018, the FCA published its long-awaited proposals for the extension of SMCR to all FCA authorised firms. These firms must be compliant by December 2019. The extension of SMCR aims to foster a culture of greater individual accountability. It will increase individual responsibility at the most senior levels and ultimately seeks to continue to help restore confidence in the financial services industry.

With only two months to go until the regulatory commencement date of the extension, firms should be working on implementation programmes and being careful not to underestimate the amount of work, internal training, and communication required to ensure compliance with the regime.
Solvency II

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

**January 1, 2016:** Effective date

**April 2016:** First reporting

**March 2019:** European Commission adopts new rules

**Dates for Diary**

**2020:** European Commission plans to review Solvency II

**Key Links**


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

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


**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.

**At a Glance**

**Regulation:** Solvency II

**Regulatory Regime:** EU and EIOPA

**Target Market Segment:** Insurance companies and their service providers

**Core Requirements:** solvency capital calculation, risk management, governance, reporting
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 Communauté 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 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 datasets.

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. Firms with successful implementations of the regulation can not only deliver compliance, but also gain opportunities to reduce capital requirements, improve risk

Asset Control provides market data management solutions – either on-prem or via our managed services AC PaSS - that help firms integrate and combine external and internal data sources, streamline the preparation of prices and risk factors, infer links between different instruments to satisfy lookthrough requirements and distribute validated data to business users and reporting applications. Our highly scalable solutions provide insight into data sourcing, integration, mastering and distribution and easy access to data.
management and achieve a clearer link between capital and risk to support better business decisions.

Since 2016, EIOPA has been collecting evidence and experiences of the application of Solvency II and submitted two sets of technical advice in response to calls from the European Commission.

The first set of advice focused on the solvency capital requirements standard formula by putting forward evidence based changes. The aim is to reduce the complexity of the standard formula where needed while retaining a proportionate, technically robust, risk-sensitive and consistent supervisory regime for the insurance sector. Essentially, the advice covers proposals regarding simplified calculations requiring less data input.

The second set of advice addressed remaining technical issues including risk margin, catastrophe risks, non-life and life underwriting risks, non-proportional reinsurance covers, unrated debt and unlisted equity and own funds.

On the basis of this advice, on March 8, 2019, the European Commission adopted new rules that take the form of a delegated act and aim to improve the balance between burden and risk and ensure that Solvency II remains up-to-date.

The act lowers the capital requirements for insurers’ investments in equity and private debt, aligning with rules applicable to banks and insurers. Other amendments to Solvency II include: new simplifications in the calculation of capital requirements; improved alignment between the insurance and banking prudential legislations; and updated principles and standard parameters to better reflect developments in risk management.

These amendments were due to be scrutinised by the European Parliament and Council for three months, and will be part of a scheduled review of the implementing rules of Solvency II, ahead of a more fundamental review of the regulation in 2020. On this basis, the Commission asked EIOPA for further technical advice in February 2019 with delivery of the advice due by June 30, 2020.

The ability to accurately evaluate exposure to asset types is key to Solvency II. The SmartStream Reference Data Utility is a managed service that delivers accurate and timely reference data for use in critical regulatory reporting and risk management operations. Solvency II requires firms providing insurance to prove the quality and accuracy of the data being used by their internal models. SmartStream’s Data Management Services provide high quality and fully audited data to assist firms in preparing correctly.

www.smartstream.com
**At a Glance**

**Regulation:** UCITS V  
**Regulatory Regime:** EU  
**Target Market Segment:** European fund managers and depositaries  
**Core Requirements:**  
Asset management, reporting

**Significant Milestones**

1985: First UCITS Directive  
July 1, 2011: UCITS IV takes effect  
July 2012: European Commission consultation on UCITS V  
September 17, 2014: UCITS V implemented  
March 18, 2016: UCITS V takes effect  
April 30, 2019: ESMA publishes final report on integrating sustainability risks in UCITS  
June 4, 2019: ESMA publishes latest Q&A on application of the UCITS Directive

**Key Links**

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

In July 2012, the European Commission ran a consultation on a potential UCITS VI. The consultation made recommendations for changes to UCITS V, but UCITS VI has yet to materialise.

The changes made in – CHANGE TO to 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.

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 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 depositaries to improve their understanding and visibility of asset data, and ensure oversight of fund managers’ performance. Data must also be managed for annual reports.

While UCITS VI has not yet materialised, and maybe never will, ESMA has continued to revise UCITS V, updating Q&As and recently, in December 2018, issuing a consultation paper on its technical advice to the European Commission on integrating sustainability risks and factors in the UCITS Directive (and AIFMD).

A final report published in April 2019 reviews responses to the consultation and covers topics on which the Commission requested ESMA to provide technical advice, namely organisational requirements, and operating conditions and risk management provisions set out in the UCITS (and AIFMD) Level 2 frameworks. ESMA is working with the Commission to transform the technical advice into formal delegated acts.
Since the financial crisis of 2008, financial institutions have been hit by wave after wave of regulation. The journey to compliance has been difficult, to say the least, and it is not over yet, but many factors are coming into play that will help firms more easily meet regulatory obligations and begin to benefit from their implementation.

There is no doubt that a slowdown in the issuance of regulations is helping firms review previous, and often tactical, approaches to compliance. Many are centralising data to support reporting across a number of regulations, or adding a layer on top of data silos to gather required data more efficiently, while others are building frameworks to meet data and data management requirements.

Technology is also key to the compliance journey, with cloud, data matching, natural language processing, text analytics, machine learning and other strands of artificial intelligence easing the burden and helping firms to not only be compliant, but also extract value from the huge volumes of data they store and manage.

Data standards are making slow progress, but they are increasingly acknowledged by the financial services sector as a means to improve regulation from both a firm and regulatory perspective. Simplification of regulation is also beginning to kick in.

Looking over the horizon, technology will have a huge impact on automating regulatory reporting, and coupled to a strategic approach to compliance, will deliver the business benefits that are so often promised yet rarely claimed. As volumes of data and data costs continue to rise unabated, the concept of shared regulatory data is beginning to attract interest among market participants. This could be the final stretch of the compliance journey, at least for the next few years.
<table>
<thead>
<tr>
<th>Glossary Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIFMD</td>
<td>Alternative Investment Fund Management Directive</td>
</tr>
<tr>
<td>AMLD</td>
<td>Anti-Money Laundering Directive</td>
</tr>
<tr>
<td>APA</td>
<td>Approved Publishing Arrangement, an organisation offering publication of order data on a commercial basis</td>
</tr>
<tr>
<td>ARM</td>
<td>Approved Reporting Mechanism, an organisation to which firms must submit transaction reporting</td>
</tr>
<tr>
<td>AUM</td>
<td>Assets under management</td>
</tr>
<tr>
<td>BCBS</td>
<td>Basel Committee on Banking Supervision</td>
</tr>
<tr>
<td>BHC</td>
<td>Bank holding company</td>
</tr>
<tr>
<td>CAT</td>
<td>US consolidated audit trail</td>
</tr>
<tr>
<td>CCAR</td>
<td>Comprehensive Capital Analysis and Review</td>
</tr>
<tr>
<td>CECL</td>
<td>Current Expected Credit Loss</td>
</tr>
<tr>
<td>CFI</td>
<td>Classification of Financial Instruments</td>
</tr>
<tr>
<td>CIC</td>
<td>Complementary Identification Code</td>
</tr>
<tr>
<td>Corep</td>
<td>Common Reporting</td>
</tr>
<tr>
<td>CRD</td>
<td>Capital Requirements Directive</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CTF</td>
<td>Counter terrorist financing</td>
</tr>
<tr>
<td>CVA</td>
<td>Credit value adjustment</td>
</tr>
<tr>
<td>D-FAST</td>
<td>Dodd-Frank Act stress testing</td>
</tr>
<tr>
<td>D-SIB</td>
<td>Domestic systemically important bank</td>
</tr>
<tr>
<td>EBA</td>
<td>European Banking Authority</td>
</tr>
<tr>
<td>ECB</td>
<td>European Central Bank</td>
</tr>
<tr>
<td>EIOPA</td>
<td>European Insurance and Occupational Pensions Authority</td>
</tr>
<tr>
<td>ELI</td>
<td>Equity-linked investments</td>
</tr>
<tr>
<td>EMIR</td>
<td>European Market Infrastructure Regulation</td>
</tr>
<tr>
<td>ESMA</td>
<td>European Securities and Markets Authority</td>
</tr>
<tr>
<td>ETD</td>
<td>Exchange-traded derivatives</td>
</tr>
<tr>
<td>Euribor</td>
<td>Euro Interbank Offered Rate</td>
</tr>
<tr>
<td>FASB</td>
<td>Financial Accounting Standards Board</td>
</tr>
<tr>
<td>FCA</td>
<td>Financial Conduct Authority</td>
</tr>
<tr>
<td>FINRA</td>
<td>Financial Industry Regulatory Authority</td>
</tr>
<tr>
<td>FIRDS</td>
<td>Financial Instruments Reference Data System</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Information Unit</td>
</tr>
<tr>
<td>Form PF</td>
<td>Form Private Fund</td>
</tr>
<tr>
<td>FRTB</td>
<td>Fundamental Review of the Trading Book</td>
</tr>
<tr>
<td>FSB</td>
<td>Financial Stability Board</td>
</tr>
<tr>
<td>FSMA</td>
<td>Financial Services and Markets Act</td>
</tr>
<tr>
<td>G-SIB</td>
<td>Global systemically important bank</td>
</tr>
<tr>
<td>IFRS</td>
<td>International Financial Reporting Standards</td>
</tr>
<tr>
<td>IHC</td>
<td>Intermediate bank holding company</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organisation of Securities Commissions</td>
</tr>
<tr>
<td>ITS</td>
<td>Implementing Technical Standards</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organisation for Standardisation</td>
</tr>
<tr>
<td>KID</td>
<td>Key Information Document</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>LCR</td>
<td>Liquidity coverage ratio</td>
</tr>
<tr>
<td>LEI</td>
<td>Legal Entity Identifier</td>
</tr>
<tr>
<td>Libor</td>
<td>London Interbank Offered Rate</td>
</tr>
<tr>
<td>MAR</td>
<td>Market Abuse Regulation</td>
</tr>
<tr>
<td>MiFID II</td>
<td>Markets in Financial Instruments Directive II</td>
</tr>
<tr>
<td>MiFIR</td>
<td>Markets in Financial Instruments Regulation</td>
</tr>
<tr>
<td>MIC</td>
<td>Market Identifier Code</td>
</tr>
<tr>
<td>MMFR</td>
<td>Money Market Funds Regulation</td>
</tr>
<tr>
<td>MTF</td>
<td>Multilateral trading facility</td>
</tr>
<tr>
<td>NCA</td>
<td>National Competent Authority</td>
</tr>
<tr>
<td>NSFR</td>
<td>Net stable funding ratio</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security Directive</td>
</tr>
<tr>
<td>OTC</td>
<td>Over-the-counter</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically exposed person</td>
</tr>
<tr>
<td>PRA</td>
<td>Prudentially regulated person</td>
</tr>
<tr>
<td>PRIIPS</td>
<td>Prudential Regulation Authority</td>
</tr>
<tr>
<td>RTS</td>
<td>Regulatory Technical Standards</td>
</tr>
<tr>
<td>RWA</td>
<td>Risk weighted asset</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SFTR</td>
<td>Securities Financing Transactions Regulation</td>
</tr>
<tr>
<td>SI</td>
<td>Systematic internaliser</td>
</tr>
<tr>
<td>SMCR</td>
<td>Senior Managers and Certification Regime</td>
</tr>
<tr>
<td>SRO</td>
<td>Self-regulatory organisations</td>
</tr>
<tr>
<td>UCITS</td>
<td>Undertakings for Collective Investment in Transferable Securities</td>
</tr>
<tr>
<td>UPI</td>
<td>Unique Product Identifier</td>
</tr>
<tr>
<td>UTI</td>
<td>Unique Transaction Identifier</td>
</tr>
</tbody>
</table>
Our customers tell us that they need to use transformative digital strategies to remain relevant in today’s challenging financial landscape. Strategies that will allow them to improve operational control, reduce costs, build new revenue streams, mitigate risk and comply accurately with regulation.

To help you make the journey towards digital transformation, we provide a range of solutions for the transaction lifecycle. AI and Blockchain technologies are now embedded in all of our solutions, which are also available in a variety of deployment models.

Digital transformation. Reaching the summit just got a little easier.

info@smartstream-stp.com
smartstream-stp.com