IMF Country Reports 22/108

United Kingdom: Financial Sector Assessment Program -Some Forward Looking Cross-Sectoral Issues

INTERNATIONAL MONETARY FUND

INTERNATIONAL MONETARY FUND

IMF Country Report No. 22/108

UNITED KINGDOM

FINANCIAL SECTOR ASSESSMENT PROGRAM

April 2022

SOME FORWARD LOOKING CROSS-SECTORAL ISSUES

This Financial Sector Assessment Program paper on United Kingdom was prepared by a staff team of the International Monetary Fund. It is based on the information available at the time it was completed on March 18, 2022.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

UNITED KINGDOM

FINANCIAL SECTOR ASSESSMENT PROGRAM

March 18, 2022

TECHNICAL NOTE

SOME FORWARD-LOOKING CROSS-SECTORAL ISSUES

Prepared By
Monetary and Capital Markets Department

This Note was prepared by IMF staff in the context of an IMF Financial Sector Assessment Program (FSAP) in the United Kingdom. The FSAP was led by Mr. Udaibir Das. The note contains technical analysis and detailed information underpinning the FSAP's findings and recommendations. Further information on the FSAP can be found at http://www.imf.org/external/np/fsap/fssa.aspx

CONTENTS

TABLES

APPENDIX

Glossary

AML	Anti-Money Laundering
ARF	Authorities' Response Framework
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BCP	Basel Core Principles
BEIS	Department for Business, Energy, and Industrial Strategy
BIS	Bank for International Settlements
BO	Beneficial Owner
BOE	Bank of England
BOT	British Overseas Territory
CBA	Cost Benefit Analysis
CCG	Cyber Coordination Groups
CCP	Central Counterparties
CD	Crown Dependency
CEG	Cyber Expert Group
CERT	Computer Emergency Response Team
CFT	Combatting the Financing of Terrorism
CIRP	Cyber Incident Response Protocol
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISP	Cybersecurity Information Sharing Partnership
CMORG	Cross Market Operational Resilience Group
CMBCG	Cross-Market Business Continuity Group
CNI	Critical National Infrastructure
COO	Chief Operating Officer
CPMI	Committee on Payments and Market Infrastructure
CQUEST	Cyber Questionnaire
CREST	Council of Registered Ethical Security Testers
CSD	Central Securities Depositories
CSDR	Central Securities Depositories Regulation
CSF	NIST Cyber Security Framework
CTP	Critical Third Party
DAR	Designated Activities Regime
EBA	European Banking Authority
ECP	Economic Crime Plan
EEA	European Economic Area
EMIR	European Market Infrastructure Regulation
ERPC	Executive Regulation and Policy Committee
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCDO	Foreign, Commonwealth & Development Office
FI	Financial Institution

FinECC	Finance Emergency Call Cyber
FMI	Financial Market Infrastructure
FPC	Financial Policy Committee
FRF	Financial Services Future Regulatory Review
FSA	Financial Services Authority
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
FSCCC	Finance Sector Cyber Collaboration Centre
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSMA	Financial Services Markets Act
FSMA 2000	Financial Services and Markets Act 2000
G7	Group of Seven
GFC	Global Financial Crisis
GSIB	Global Systemically Important Banks
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
IBD	Inter-American Development Bank
ICG	Incident communication group
ICO	Information Commissioner's Office
ICP	Insurance Core Principles
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISEWG	Intelligence Sharing Expert Working Group
ISO	International Organization for Standardization
IT	Information Technology
ITAFF	Illicit and Tax Avoidance Related Financial Flow
JMLIT	Joint Money Laundering Intelligence Task Force
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
MiFiD II	Second Markets in Financial Instruments Directive
ML	Money Laundering
MLRs	Money Laundering Regulations
MPR	Mid-Point Reviews
NCA	National Crime Agency
NCCU	National Cyber Crime Unit
NCSC	National Cyber Security Centre
NECC	National Economic Crime Centre
NFIB	National Fraud Intelligence Bureau
NIST	National Institute of Standards and Technology
NRA	National Risk Assessment
OFC	Offshore Financial Center
OFSI	Office of Financial Sanctions Implementation
OPBAS	Office for Professional Body Anti-Money Laundering Supervision
ORF	Operational Risk Framework
ORRD	Operational Risk and Resilience Division

PBS	Professional Body Supervisor
PFMI	CPMI-IOSCO Principles for Financial Market Infrastructures
PRA	Prudential Regulation Authority
PRC	Prudential Regulation Committee
PS	Policy Statement
PSC	People with Significant Control
PSM	Periodic Summary Meeting
SEG	Sector exercising group
SFO	Serious Fraud Office
SM&CR	Senior Management & Certification Regime
SMF	Senior Management Function
SRF	Sector Response Framework
SRPC	Supervision, Risk, and Policy Committee
SRS	Supervisory Risk Specialists
SS	Supervisory Statement
STAR-FS	Simulated Target Attack and Response – Financial Services
SYSC	Systems and Controls Sourcebook
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
TN	Technical Note
TRC	Technology, Resilience and Cyber
TRS	Trust Registration System
TTP	Tactics, Techniques and Procedures
U.K.	United Kingdom
U.S.	United States
UWO	Unexplained Wealth Order

FINANCIAL INTEGRITY, AML/CFT, AND FINANCIAL STABILITY

A. Executive Summary

1. The United Kingdom faces significant money laundering threats from foreign criminal proceeds, owing to its status as a global financial center, but the authorities have a strong understanding of these risks. The authorities estimated the realistic possibility of hundreds of billions of pounds of illicit proceeds being laundered in their jurisdiction. The money laundering risks facing the United Kingdom include illicit proceeds from foreign crimes such as transnational organized crime, overseas corruption, and tax crimes. Financial services, trust, and company service providers (TCSPs), accountancy and legal sectors are high-risk for money laundering, with also significant emerging risks coming from cryptoassets. Some Crown Dependencies (CDs) and British Overseas Territories (BOTs) have featured in U.K. money laundering investigations. Brexit and COVID pandemic have an impact upon the money laundering risks in the United Kingdom. The authorities nevertheless have demonstrated a deep and robust experience in assessing and understanding their ML/TF risks. Leveraging technology tools such as big data and machine learning to analyze cross-border payments may add further dimension to their risk assessments. This technical note (TN) will focus on key aspects of the United Kingdom's anti-money laundering and countering the financing of terrorism (AML/CFT) regime: risk-based AML/CFT supervision, entity transparency and international cooperation.

2. Priority should be given to enhancing the breadth and depth of risk-based supervision of key sectors, especially given the large supervisory population in the United Kingdom. The FCA's tiered supervisory approach (i.e., systematic, proactive, and reactive) are based on the assessment of risks. However, the desk-based and on-site inspections conducted (less than 200 per year) do not appear commensurate to the risks of the 22,000 supervised entities (almost all of which are assessed as either high or medium risks). Broad access to data from supervised entities coupled with robust technological analytical tools as well as leveraging skilled persons will contribute to addressing the challenges of effective risk-based supervision. On cryptoassets, continued assessment of the ML/TF risks of cryptoasset businesses and a robust approach to registration will help ensure that FCA's AML/CFT supervisory approach is effective. This would need to be supported by obligations to have adequate information of parties to a cryptoasset transactions (travel rule). Robust enforcement actions (including effective, dissuasive, and proportionate penalties) over supervised entities will contribute to a strong AML/CFT compliance culture. The Office for Professional Body Anti-Money Laundering Supervision (OPBAS) continues to intensify AML/CFT oversight of the legal and accountancy sectors, with scope to improve the effectiveness of AML/CFT supervision by professional body supervisors (PBSs). To better ensure consistency of supervisory approaches among PBSs, the authorities should consider empowering the OPBAS to directly conduct AML/CFT supervision of legal and accountancy sectors in cases where the PBS has low capacity or high risks.

3. The United Kingdom remains a global leader in promoting entity transparency. The People with Significant Control (PSC) Register is a pioneering effort that allows full, free, and public access to beneficial ownership information of U.K. legal entities. To support the accuracy of the PSC Register, supervised entities are required to report discrepancies between information obtained through customer due diligence and information on the PSC Register. Efforts to further improve the accuracy of the beneficial ownership information should advance, particularly, the requirement on compulsory identify verification and expanding the powers of Companies House over the information. In addition, the Trust Registration System (TRS) collects beneficial ownership information over U.K. express trusts (with or without U.K. tax liabilities), and mechanisms for foreign counterparties to timely access to such information should continue to be available. Priority should also be given to legislative proposals to create the Overseas Entities Bill, which would give public access to beneficial ownership information of foreign entities owning U.K. properties.

4. The United Kingdom also provides a range of timely and constructive international cooperation on economic crimes. The United Kingdom's overseas criminal justice network as well as the strong domestic public and private partnerships are positive features of the U.K. system for exchanging financial intelligence and information. Leveraging the robust confiscation, asset recovery and targeted financial sanctions frameworks (including the unexplained wealth orders and Global Anti-Corruption Sanctions Regime) is critical to addressing the laundering of foreign proceeds of crime, given United Kingdom's status as global financial center and attractive destination for illicit financial flows. Strong and timely information sharing mechanisms between the United Kingdom, CDs and BOTs facilitate complex and cross-border criminal investigations. The U.K. authorities should continue to engage CDs and support BOTs in having robust, effectively calibrated and publicly available beneficial ownership registers, to facilitate foreign criminal investigations.

Table 1. United Kingdom: Main Recommendations		
Recommendation	**Responsible Agency**	**Timeline**
AML/CFT Supervision		
1. **Credit and Financial Institutions**. Further improve breadth and depth of risk-based AML/CFT supervision through enhanced data collection, leveraging technology analytical tools (e.g., big data and machine learning), robust and proportionate enforcement actions, and use of skilled persons.	FCA	NT
2. **Cryptoasset Entities**. Pursue amendments to legal framework for obtaining, holding and transmission of identifying information of all parties to all cryptoasset transactions (travel rule).	HMT	NT
3. **TCSP, Legal and Accountancy Sectors**. Intensify efforts to ensure consistency of supervisory approaches over TCSPs, accountancy and legal sectors, including considering the expansion of the supervisory mandate and powers of OPBAS.	HMRC, FCA, PBS/OPBAS	MT
4. **Augment Assessment of Threats**. Leverage data to enhance the understanding of threats, including in relation to aggregate financial flows and high-risk jurisdictions.	HMT, FCA	MT
5. **Increased Resources**. Move ahead with the proposed Economic Crime Levy to generate critical resources to support AML/CFT reforms (e.g., staffing and technology tools).	HMT	MT
Entity Transparency		
6. **Accuracy of Beneficial Ownership Information**. Amend the legal framework and enhance the powers of Companies House to improve the accuracy of beneficial ownership information in the People with Significant Control Register, including requiring verification of beneficial ownership information and enabling Companies House to access other government databases.	BEIS/ Companies House	NT
7. **Beneficial Ownership of Real Properties**. Pursue proposed Overseas Entities Bill that would require public disclosure of beneficial ownership information of foreign entities owning U.K. real properties.	BEIS	MT
International Cooperation		
8. **Information Sharing**. Continue to strengthen cooperative mechanisms with foreign counterparties for timely sharing of financial intelligence, especially in complex and cross-border economic crime cases.	NCA	NT
9. Support to BOTs and Engagement with CDs. Continue to ensure effective and calibrated support to relevant BOTs and to engage with CDs in accurate and publicly accessible beneficial ownership information of entities created in such jurisdictions.	FCDO	MT
NT = Near Term (now to one year); MT = Medium Term (within 1 to 3 years)		

B. Introduction[1]

5. This Technical Note (TN) provides a targeted review of the U.K. Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) regime in the context of the 2021 Financial Sector Assessment Program (FSAP).[2] It builds upon the 2016 AML/CFT TN that accompanied the previous U.K. FSAP.[3] The targeted review is based on a range of materials, including the 2018 Mutual Evaluation Report (MER) by the Financial Action Task Force (FATF),[4] information provided by the authorities, and publicly available materials. Staff analysis greatly benefitted from discussions in a virtual setting from November 1–12, 2021 with key agencies, particularly, HM Treasury (HMT), Financial Conduct Authority (FCA), HM Revenue and Customs (HMRC), the Prudential Regulation Authority (PRA), Office for Professional Body Anti-Money Laundering Supervision (OPBAS), HMT-Office of Financial Sanctions Implementation (OFSI), Companies House, Foreign, Commonwealth & Development Office (FCDO), Serious Fraud Office (SFO), the Home Office, and National Economic Crime Centre (NECC). The IMF FSAP team deeply appreciates the staff of these agencies for their professionalism, patience, and candor throughout the process.

6. The FATF rated United Kingdom's AML/CFT regime as one of the most effective among its peers (Figure 1). In the 2018 MER, 8 of the 11 Immediate Outcomes (IOs) were rated as satisfactory, with almost half being given the highest ratings (highly effective): IO1 - risk, policy, and coordination; IO9 - terrorist financing (TF) investigations and prosecutions; IO10 - TF preventative measures & financial sanctions; and IO11 - proliferation financing financial sanctions. The FATF however recommended further improvements in three key areas: IO3 - AML/CFT supervision; IO4 - preventive measures; and IO6 - financial intelligence. Key priority actions recommended in the MER included, among others: (i) ensure appropriate intensity of AML/CFT supervision; (ii) improve the quality of beneficial ownership information in relation to legal persons; and (c) continue to work with international partners on information-sharing gateways. The TN will highlight below the key developments and progress made by the authorities to implement these recommendations. It will not cover the full scope of the 11 Immediate Outcomes nor all the priority recommendations in the 2018 MER.

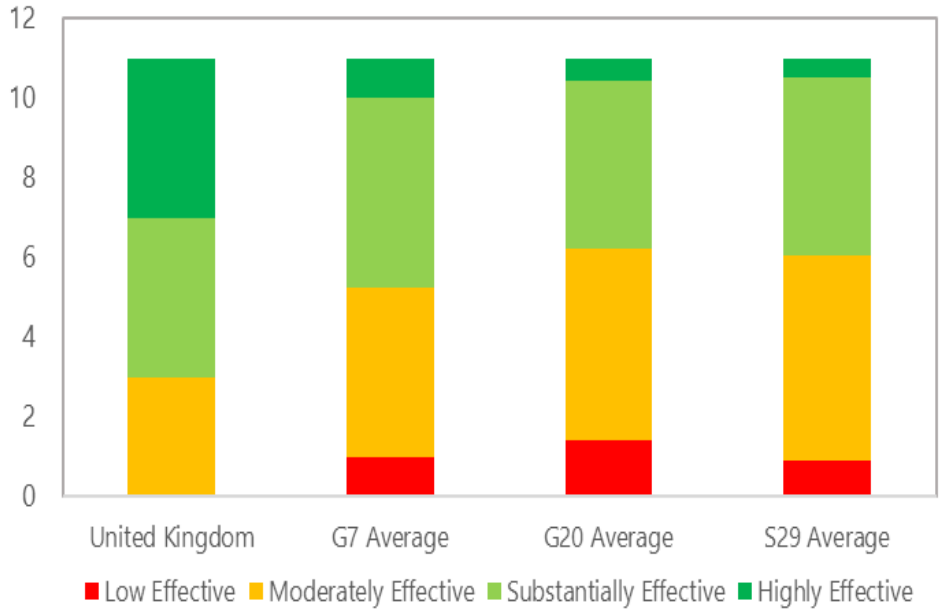
[1] This chapter was prepared by Jonathan Pampolina with analytical support from Maksym Markevych and Alexander Malden, all from the IMF.

[2] Under the IMF's FSAP policy, every FSAP should incorporate timely and accurate input on AML/CFT issues. Where possible, this input should be based on a comprehensive AML/CFT assessment conducted against the prevailing standard. See the Acting Chair's Summing Up—Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism—Executive Board Meeting 14/22, March 12, 2014 (http://www.imf.org/external/np/sec/pr/2014/pr14167.htm).

[3] IMF, United Kingdom (Financial Sector Assessment Program), AML/CFT-TN (June 2016), IMF Country Report No. 16/165 (https://www.imf.org/external/pubs/ft/scr/2016/cr16165.pdf).

[4] FATF, United Kingdom, Mutual Evaluation Report, December 2018 (https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf).

Figure 1. United Kingdom: AML/CFT: Comparison of Mutual Evaluation Report Ratings (as of 2021)



Source: Financial Action Task Force.

7. The 2019–22 Economic Crime Plan (ECP) highlights the authorities' commitment to ensuring that the United Kingdom maintains and enhances its leading role in the global response to illicit finance.[5] The ECP was jointly designed by government agencies and key public and private sector stakeholders to strengthen the "whole-system" response to combatting economic crime. Fifty-two action items with time-bound targets were set and responsible agencies were designated. These action items are grouped into 8 key priority areas, including risk-based supervision and risk management, transparency of ownership, international strategy, and governance and public-private partnership. Based on the authorities' assessment as of February 2021, more than 40 percent of the 52-action items had been completed;[6] by the time of the FSAP virtual meetings in November 2021, the authorities reported completing 50 percent of the ECP.

8. Based on the United Kingdom's risk profile, staff's review for purposes of this FSAP focused on three key areas: (a) AML/CFT supervision; (b) entity transparency; and (c) international cooperation (see Table 1 for summary of main recommendations).

C. Risk Profile

9. The United Kingdom faces significant ML threats from foreign criminal proceeds. As an advanced open economy and global financial center, the United Kingdom is an attractive

[5] HMT and Home Office, 2019-22 ECP (https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version).

[6] ECP: Statement of Progress (July 2019 – February 2021). (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf)

destination or transit location for proceeds of foreign crimes. The risks include foreign proceeds of crime (e.g., transnational organized crime, overseas corruption, tax crimes) flowing to the United Kingdom for integration into the legitimate economy, illicit funds intended for passing through its financial sector, and outflows of domestic proceeds of crime for ML layering. The authorities estimate that there is a realistic possibility that every year hundreds of billions of pounds of illicit proceeds are being laundered in the United Kingdom.[7]

10. The authorities demonstrated a deep and robust experience in assessing national ML/TF risks. Three national risk assessments (NRA) have been published,[8] the latest one in 2020.[9] In September 2021, the first national assessment of proliferation financing risks was also made publicly available.[10] Aside from cash and money service businesses, the financial services sector remains one of the highest risks for ML in the United Kingdom (i.e., retail banking, wholesale banking, wealth management and private banking) (Figure 2). In a joint letter, the PRA and FCA noted the inherent risks of trade finance activities given its complexity, global nature and large volumes of trade flows utilizing multiple currencies.[11] They reiterated their expectations on entities involved in trade finance to take a risk sensitive approach to their control environment and highlighted several significant issues in relation to financial crime controls (e.g., counterparty analysis and transaction approval). Risks from cryptoassets have also risen since the 2017 NRA, recognizing that as an alternative form of value to traditional fiat currency, they have the potential of being abused by criminals and terrorists to move value across the world and obfuscate the source of illicit proceeds.

11. Trust and company service providers (TCSPs), accountancy and legal sectors are high risk for ML. Criminals would often attempt to enlist the enablers in these sectors and leverage their professional qualified status to assist them in giving their illicit proceeds a veneer of authenticity and respectability. Such professional enablers can be used as a means to create and operate corporate structures, invest, and transfer funds to disguise their origins, and lend layers of legitimacy to their operations. For example, complex systems of shell companies and trusts registered abroad are abused to purchase "super prime" properties in the United Kingdom, obscuring the true owners of the property, and obfuscating the sources of funds. Of particular interest, the authorities noted

[7] U.K. NCA, 2020 National Strategic Assessment of Serious and Organized Crime (https://www.nationalcrimeagency.gov.uk/news/nsa2020).

[8] 2015 NRA (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf); and 2017 NRA (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf)

[9] 2020 NRA (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf)

[10] 2021 NRA PF (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020695/National_risk_assessment_of_proliferation_financing.pdf)

[11] PRA-FCA Joint Letter on Trade Finance Activity September 9, 2021. (https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2021/september/trade-finance-activity-letter.pdf?la=en&hash=DFDAD6E357DCDFAF1C4EA5B017509C601C64442B)

"family offices" as increasingly identified as enablers in ML investigations. Family offices provide a range of services (e.g., wealth and property management, legal, accountancy and other services) to high-net-worth individuals and their families and are likely to coordinate the management of companies in charge of a portfolio of investments, adding an extra layer of privacy to further distance the true owners.

Figure 2. United Kingdom: Historical Comparison of ML/TF Risks of Key Sectors

	Money Laundering Risk Score			Terrorist Financing Risk Score		
	2017	2020	*CHANGE*	2017	2020	*CHANGE*
Cash	HIGH	HIGH		HIGH	HIGH	
Money Service Business	HIGH	HIGH		HIGH	HIGH	
Retail Banking	HIGH	HIGH		HIGH	HIGH	
Wholesale Banking	HIGH	HIGH		LOW	LOW	
Wealth Management and Private Banking	HIGH	HIGH		LOW	LOW	
Accountancy Services	HIGH	HIGH		LOW	LOW	
Legal Services	HIGH	HIGH		LOW	LOW	
Company and Partnership	HIGH	HIGH		LOW	LOW	
Trust and Company Service Providers	MEDIUM	HIGH	↑	LOW	LOW	
Property	MEDIUM	HIGH	↑	LOW	LOW	
Art Market Participants	N/A	HIGH		N/A	LOW	
Payment Services and Electronic Money	MEDIUM	MEDIUM		MEDIUM	MEDIUM	
Cryptoasset Risk	LOW	MEDIUM	↑	LOW	MEDIUM	↑
Estate Agency	LOW	MEDIUM	↑	LOW	LOW	
Letting Agency	N/A	MEDIUM		N/A	LOW	
High Value Dealers	LOW	MEDIUM	↑	LOW	LOW	
Trusts	LOW	LOW		LOW	LOW	
Registered Gambling (Casinos)	LOW	LOW		LOW	LOW	
Other Gambling Risks	LOW	LOW		LOW	LOW	

Source: 2017 and 2020 NRA.[1]

[1] Art market participants and letting agencies were subject to the MLRs as of January 1, 2020.

12. Some Crown Dependencies (CDs) and British Overseas Territories (BOTs) continue to feature prominently in U.K. ML investigations and reporting. Criminals seek to exploit the close economic ties between the United Kingdom, CDs, and BOTs by taking advantage of existing channels and strong business connections to disguise illicit assets. For example, U.K. law enforcement agencies (LEAs) noted that the vulnerabilities in one of the BOTs have been exploited for establishing corporate structures that was used to facilitate money laundering.[12] In February 2021, the Cayman Islands (another BOT) was included in the FATF's list of jurisdictions with serious AML/CFT deficiencies, with respect to shortcomings on beneficial ownership information and prosecution of ML cases.[13] This prompted the U.K. authorities to add the Cayman Islands to its own list of high risk jurisdictions.[14] (Box 1).

[12] British Virgin Islands (see 2020 NRA).

[13] FATF, Jurisdictions Under Increased Monitoring (October 2021) (https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html).

[14] Regulated businesses in the UK are required to apply enhanced customer due diligence measures and enhanced ongoing monitoring in any business relationship with a person established in a high-risk jurisdiction or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk jurisdiction country

(continued)

13. Despite restrictions from the COVID pandemic that limited the use of cash for ML, organized criminal groups have continued to find alternatives to launder their illicit funds. Lockdown measures have impacted their ability to physically move cash across borders. Nevertheless, the authorities noted the increased use of cryptoassets, mobile banking, and electronic payments, taking advantage of branch closures and facility of remote payments during the pandemic. While international students residing in the United Kingdom may have decreased due to the travel restrictions, other vulnerable individuals (e.g., unemployed) could be coerced by organized criminal groups to open money mule accounts. Distressed businesses were at risk of being targeted by criminals willing to invest their illicit funds as capital. For example, investigations are being pursued against organized criminal groups that may have committed large scale fraud to obtain funds from government loan schemes (e.g., £47 billion loan value of Bounce Back Loan Scheme).[15] The authorities have also noted the potential for trade-based money laundering activities arising from increased demand for certain goods and services during the pandemic, including from new or unfamiliar suppliers. The FCA warned supervised entities not to change their risk appetites to address the operational challenges of the COVID pandemic and to remain vigilant to new types of fraud.[16]

14. Brexit may have medium- and long-term implications to the ML/TF risks faced by the United Kingdom. The National Crime Agency (NCA) assessed that U.K. entities may consider more trade opportunities in other non-European Economic Area (EEA) jurisdictions, which may raise the risks that they may be drawn to corrupt practices in high-risk industries.[17] The creation of freeports and inland clearance hubs may be abused to disguise type and origin of goods and final destination of shipments; however, these freeports will be subject to the same AML/CFT regulatory regime as the rest of the United Kingdom.[18] Heightened risks of smuggling with the opening of new ferry and container services between the United Kingdom and EEA countries (e.g., through Ireland) have also been flagged by the authorities. The authorities, nevertheless, exerted strong efforts to ensure a smooth post-Brexit transition of its AML/CFT legal framework (Box 1).

(https://www.gov.uk/government/publications/money-laundering-advisory-notice-high-risk-third-countries--2/hm-treasury-advisory-notice-high-risk-third-countries).

[15] National Audit Office, The Bounce Back Loan Scheme: An Update (December 3, 2021). https://www.nao.org.uk/wp-content/uploads/2021/12/The-Bounce-Back-Loan-Scheme-an-update.pdf

[16] FCA, Statement on Financial Crime Systems and Controls During Coronavirus Situation (first published on May 6, 2020). https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation

[17] NCA, 2021 National Strategic Assessment of Serious and Organized Crime (https://www.nationalcrimeagency.gov.uk/news/online-is-the-new-frontline-in-fight-against-organised-crime-says-national-crime-agency-on-publication-of-annual-threat-assessment).

[18] HM Government, Freeports: Response to the Consultation (October 2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/924644/FINAL_-_200923_-_OFF_SEN_-_Freeports_Con_Res_-_FINAL.pdf

Box 1. Post-Brexit AML/CFT Legal Framework

The U.K. AML/CFT framework suffered minimal disruption from Brexit and has been strengthened in targeted ways post-Brexit. The United Kingdom's Money Laundering Regulations (MLRs) have broadly remained the same after the post-Brexit transition period. (See EU Exit-related amendments to the MLR.) Given the broad alignment of the AML/CFT frameworks between the United Kingdom and EEA countries with the international AML/CFT standards,[1] there was minimal disruption with respect to compliance by entities with AML/CFT obligations, particularly on assessing risks and implementing AML/CFT controls. Post-Brexit changes to the U.K. AML/CFT framework were aimed at recognizing EEA countries as third-country jurisdictions for the United Kingdom to ensure cross-border ML/TF risks are effectively managed and mitigated (e.g., required information for payers/payees of U.K.-EEA cross-border payments, and enhanced due diligence for U.K.-EEA correspondent banking relationships). In addition, the United Kingdom now issues its own list of high-risk jurisdictions, including EEA jurisdictions (e.g., Malta). Such listing by the United Kingdom triggers a requirement for enhanced due diligence in any business relationship with a person established in a high-risk third country or any transaction where either of the parties to the transaction is established in a high-risk third country. Under the Trade and Cooperation Agreement, both parties committed to cooperating in preventing the use of their financial systems to launder criminal proceeds and exchange relevant information.

Source: IMF Staff analysis.

[1] The United Kingdom is one of the 39 members of the FATF, along with the European Commission as well as other select EEA countries.

15. Since the last FSAP, the direction of financial flows in the United Kingdom has changed with a quarter increase in share of the flows with offshore financial centers (OFCs).[19] IMF staff conducted an analysis of aggregate flows of financial payments to and from the United Kingdom since 2016.[20] The share of cross-border payments with the main counterparties of the United Kingdom (i.e., other G7 countries) remained stable. However, the share of payments with the rest of European countries, except Eastern Europe, have decreased (Figure 3). Both inflows from and outflows to the OFCs have increased, particularly in 2021.[21] The share of Middle Eastern, Commonwealth of Independent States[22], Southern and Western African countries have also increased.

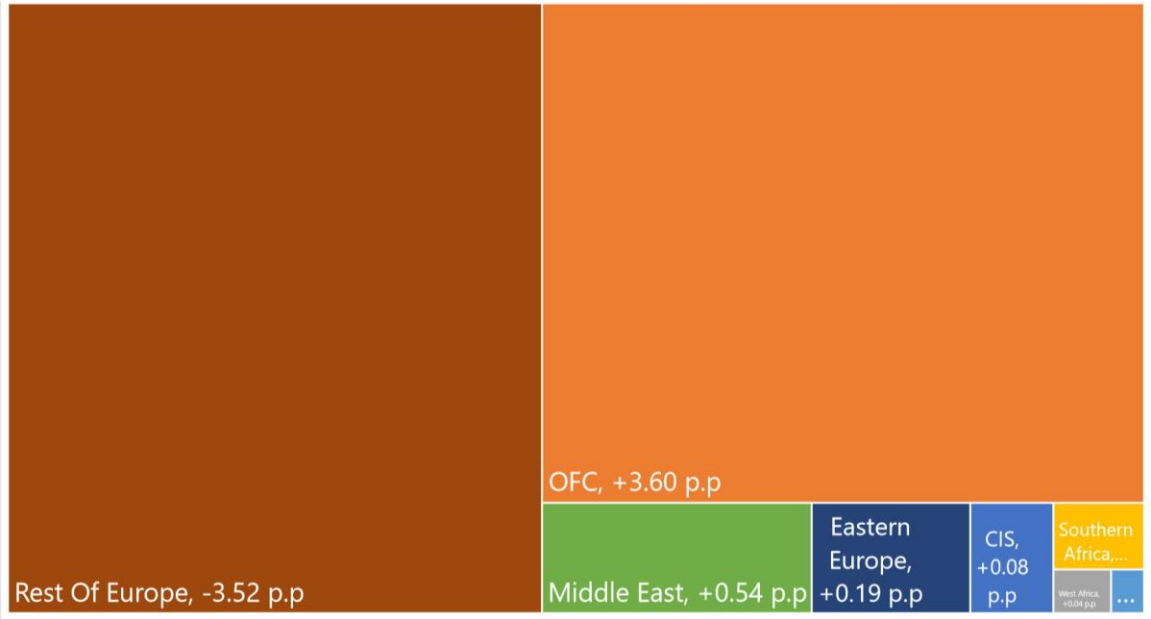
[19] While definitions of OFCs may vary, the operational definition for purpose of this TN refers to jurisdictions where the bulk of financial sector activity is offshore on both sides of the balance sheet, where the transactions are initiated elsewhere, and where majority of the institutions involved are controlled by non-residents. (IMF Background Paper: Offshore Financial Centers (2000).) https://www.imf.org/external/np/mae/oshore/2000/eng/back.htm)

[20] The financial flows analysis presented uses payments between the customers of financial institutions (i.e., SWIFT). The analysis is conducted using aggregate monthly country-level data from July 2016 to October 2021.

[21] The financial flows analysis covers data until October 2021.

[22] Includes founding states of the Commonwealth of Independent States and former member states.

Figure 3. United Kingdom: Aggregate Financial Flows in the United Kingdom to Select Country Groupings (2019–21)
(Percent point share changes from 2015–16)



Source: IMF staff calculations.

16. Financial flows with high-risk jurisdictions have increased, indicating potential elevated threat of cross-border ML/TF. Since 2016, payments to each of the five high risk countries identified in the 2020 NRA[23] have increased, including more than doubling of inflows from two countries and of outflows to three countries in 2021 as compared to 2016. (Figure 4) Both inflows from and outflows to high-risk jurisdictions identified by supervised entities in the latest FCA financial crime survey[24] have also increased, together with the increased average value of transaction-inflow, although average value of transaction-outflow stayed stable. Given the Brexit context, some movement in the cross-border financial flows away from EEA jurisdictions is to be expected. Nevertheless, these increases in financial flows to high-risk jurisdictions demonstrates an ongoing need for the United Kingdom to monitor its ML/TF risks in relation to these jurisdictions.

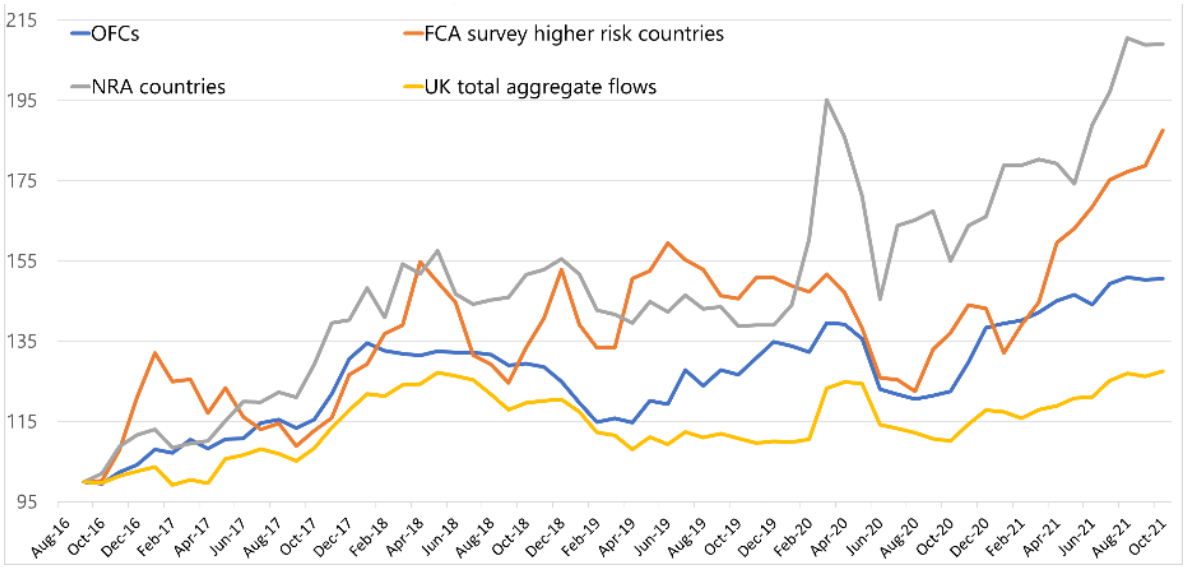
17. Leveraging technological tools to analyze cross-border payments can provide another useful dimension to understanding ML/TF risks. Considering the importance of cross-border transactions to the United Kingdom's AML/CFT risk profile and its leading position in the financial flows globally, analytical tools and approaches could be developed to better monitor cross-border financial flows. The United Kingdom's robust understanding of its ML/TF risks is based on a range of qualitative and quantitative information, which might be complemented by analysis of cross-border payments data. Examining patterns of the United Kingdom's financial flows can provide an

[23] United Kingdom's 2020 NRA assessed China, Hong Kong, Pakistan, Russia, United Arab Emirates as jurisdictions to be particularly relevant to the cross-border money laundering risks faced by the United Kingdom.

[24] Top 25 jurisdictions identified by supervised entities in the FCA's analysis of annual financial crime data return (2017-20) (https://www.fca.org.uk/data/financial-crime-analysis-firms-2017-2020).

additional source of information to identify and assess ML/TF threats, including feeding into the NRA's higher ML/TF risk jurisdiction assessment. Specifically, the authorities should consider analysis of consistency of the level and trends in payments with individual countries with the economic fundamentals, such as bilateral trade and investments, and of the extent the flows are explained by provision of various financial services with scrutiny of associated ML/TF risks. This can usefully complement the authorities' law enforcement and typologies reports analysis, which is based on the detected cases; while it is not clear whether the level of prosecutions and convictions of high-end ML is fully consistent with the United Kingdom's threats and risk profile. Incorporating cross-border payments data would contribute to deepening national analysis of the nature and extent of ML/TF risks, for example as part of the NRA's financial sectors' inherent risk evaluation.

Figure 4. United Kingdom: Aggregate Financial Flows in the United Kingdom for High-Risk Jurisdictions (2016–21)



Source: IMF staff calculations.

18. Monitoring of cross-border payments could complement ML/TF risk understanding in relation to the financial sector. Identification of the ML/TF risk level that individual supervised entities are facing from cross-border ML/TF—one of the main ML/TF risks in the United Kingdom—may be supported by supervisors' understanding of the value, volume, and direction of cross-border payments facilitated by individual entities. The AML/CFT supervisors of key financial institutions and supervised entities (i.e., FCA, HMRC) should consider the incorporation of additional data on cross-border payments in the data collection and analysis to support risk understanding and risk rating of individual entities. Developing supervisory technology (Box 2) could help analyze and cover the entire AML/CFT supervisory population, which in turn will contribute to supervisory decisions on prioritization and selection of entities for inspection (e.g., an entity with a small balance sheet but processing a significant number of cross-border payments).

Box 2. Leveraging Big Data and Data Analytics for Monitoring Cross-Border Flows

Big data and advanced data analytics of cross-border flows can be useful inputs to further advance U.K. authorities' understanding of ML/TF risks. The United Kingdom's large supervisory population, high volume, and number of cross-border payments as well as sophistication of its financial sector create operational challenges for monitoring and analysis. Leveraging big data and advanced data analytics for efficient, effective, and timely detection and assessment of cross-border ML/TF risks can support the United Kingdom's risk-based supervisory approach. The availability of vast amounts of existing data is also a strength. Cross-border payments data can be supplemented with trade, portfolio, direct investments, financial instruments operations, balance of payments, international investment position data to identify unusual payments unexplained by economic activity. Such data analytics can also incorporate various indicators of increased ML/TF risk, using the authorities' risk understanding of various jurisdictions, ML/TF red flags, trends, typologies, open-source data, and structural factors, such as the country's economic crime environment.

Monitoring and analysis of cross-border payments can help identify red flags and patterns that would warrant further oversight by supervisors. Advances in machine learning provide an opportunity for the U.K. authorities to efficiently identify supervised entities exposed to significant cross-border ML/TF risks and unusual payments potentially related to illicit financial flows and receive early warnings about changing payments patterns and corresponding evolving ML/TF risks. IMF staff's outlier detection machine learning algorithm[1] uses global cross-border payments since 2013 and incorporates various indicators of lower and higher ML/TF risks.[2] Based on analysis from this outlier detection algorithm, the United Kingdom attracts the most inflow payments-outliers globally, while not generating many outflows-outliers. Unlike most other countries, inflows-outliers to the United Kingdom are persistent and well-diversified—the outlier activity is detected with most of the world's countries.[3] (See Appendix I.)

Source: IMF Staff analysis.
[1] IMF staff's cross-border payments outlier detection algorithm is based on the isolation forest approach (Fei Tony Liu, Kai Ming Ting and Zhi-Hua Zhou; 2008).
[2] These indicators include bilateral trade, portfolio and direct investments, average transaction value, appearance of new payment corridors, strength of AML/CFT regime, financial secrecy, harmful tax practices, corruption perceptions. The payment amounts are normalized on the ordering country level.
[3] See Appendix I. for information on the data points used and methodological approach for the IMF's outlier detection machine learning algorithm.

19. The authorities' ongoing work to understand the scale of economic crime is welcome. The Economic Crime Research Strategy aims to identify evidence gaps and sets out key areas for further research and analysis. Policy choices and the targeting of resources can be better made with improved capacities for obtaining and analysis of data and evidence.

D. Risk-Based AML/CFT Supervision

20. AML/CFT supervisory authority in the United Kingdom is divided among three statutory supervisors (FCA, HMRC, and the Gambling Commission) and 22 professional body supervisors (PBS) for the legal and accountancy sectors. Credit and financial institutions[25] as well as cryptoasset businesses are supervised by the FCA for AML/CFT purposes.[26] HMRC supervises art market participants, estate and letting agents, and high value dealers as well as other accountants (unless supervised by PBS), money service businesses (unless supervised by FCA), and TCSPs (unless supervised by the FCA or PBS). There are 13 PBSs for the accountancy sector and 9 PBSs for the legal sector, that are covered in the MLRs Schedule.[27] All of these PBSs are subject to oversight by OPBAS (which was established in 2018 within the FCA). OPBAS aims to improve consistency of AML/CFT supervisory approaches among PBSs, but OPBAS itself does not directly supervise accountants or lawyers. Finally, the Gambling Commission is the AML/CFT supervisory authority for land based and remote casinos.[28] All AML/CFT supervisors as well as OPBAS are part of the AML Supervisors Forum, which is a venue to discuss common supervisory issues, share best practices and provide updates on current or future work.

21. The United Kingdom has a large and diverse AML/CFT supervisory population. As of end-2020, there are more than 97,000 entities being supervised for AML/CFT compliance. (Figure 5) The sheer number of entities pose operational challenges to achieving effective risk-based supervision in terms of breadth and depth of monitoring. With respect to credit and financial institutions, the FCA oversees more than 22,000 such entities under the MLRs (90 percent of which are identified as either high or medium risk). In line with the commitments under the ECP, a call for evidence from relevant stakeholders has been launched to assess the United Kingdom's AML/CFT regulatory and supervisory regimes looking at the structure of the supervisory regime, key elements of the current MLRs as well as their overall effectiveness.[29]

AML/CFT Supervision of Credit and Financial Institutions and Cryptoassets

22. The FCA continues to strengthen and recalibrate its tiered-supervisory approach based on risks. As noted in the 2016 FSAP AML/CFT TN and the 2018 MER, the FCA's tiered approach involved the systematic AML program, proactive AML program, risk-assurance reviews, and reactive approaches. The 14 largest financial institutions were subject to a systematic AML program, involving an intensive 4–6-month inspection involving 4–5 staff conducted every four years. Other high risks entities were subject to a less intensive proactive AML program, where 2–3 staff inspect the entity within 2–4 days every four years. Risk assurance reviews were undertaken by the FCA on a

[25] Such as banks, credit unions, building societies, investment managers, and financial advisors.

[26] The FCA's financial crime department has 47 financial crime specialists, who lead on complex AML/CFT issues.

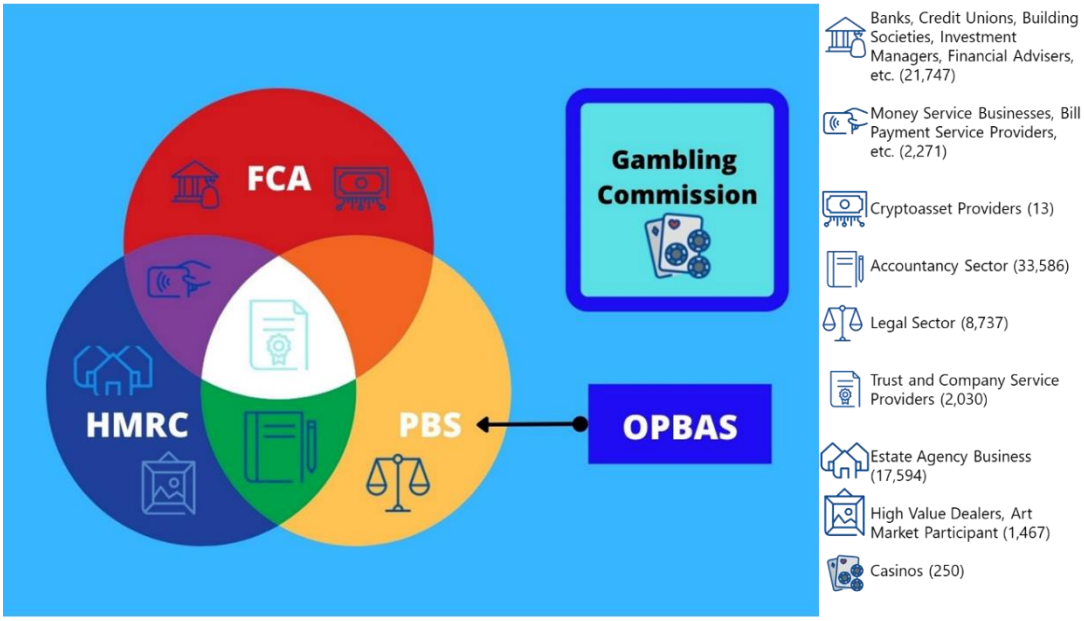
[27] There are an additional three PBSs that have been delegated regulatory functions.

[28] Given the low ML/TF risks of registered gambling (casinos) and other gambling risks as noted above, the TN will not review effectiveness of AML/CFT supervision by the Gambling Commission.

[29] HMT, Call for Evidence Review of the U.K.'s AML/CFT Regulatory and Supervisory Regime (July 2021) (https://www.gov.uk/government/consultations/call-for-evidence-review-of-the-uks-amlctf-regulatory-and-supervisory-regime).

yearly basis, which reviews specific areas across a broader range of selected supervised entities. When the FCA receives actionable information, it also undertakes reactive supervision. This may be entity specific or across a cohort of entities. In the 2018 MER, the FCA was encouraged to consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk. In response to this, the FCA has identified the changes to proactive AML supervisory approach that focuses on key issues or areas among multiple targeted supervised entities across risk profiles and communicating the results to the sector. The changes include the introduction of new *Modular Assessment Proactive Programme* that focuses on reviewing the highest risk areas of the largest and most systematically important entities more frequently; *Proactive AML Programme* that drives supervisory attention on outliers, hotspots and emerging themes as identified through the data/other intelligence sources; and *Focused Supervisory Interventions Programme* that will increase the breadth of the FCA's proactive AML supervision by engaging with entities on specific issues or risk indicators.

Figure 5. United Kingdom: Supervisory Population of Entities with AML/CFT Obligations
(As of end-December 2020)



Sources: U.K. authorities and IMF staff calculations.

23. The breadth and depth of AML/CFT supervision by FCA could be further enhanced. Out of the 22,000 entities, 23 percent are assessed as high risks, and majority (73 percent) are deemed medium risks. However, the annual number of desk-based and onsite inspections (less than 200) in the past three years do not appear commensurate to the assessed risks of the supervised entities (even if these were only confined to the higher risk entities) (Figure 6). Although there is no expectation that all supervised entities are subject to annual onsite inspections, IMF staff express concerns as to the extent to which a substantial portion of supervised entities are effectively monitored for AML/CFT compliance, given the size of the supervisory population, their risk profiles, and number of inspections. While reactive supervision can aim to capture serious ML/TF violations,

this relies on complaints, whistleblowers, or intelligence from law enforcement agencies. The duration and frequency of inspections under the Proactive AML Programme for high risk but non-systematic entities should also be re-calibrated, to better mitigate risks. While supervised entities are required to implement group-wide AML/CFT programs (including for those operations outside the United Kingdom), the extent to which these programs are monitored by the FCA and the effectiveness of coordination with relevant home/host supervisors is outside the scope of this TN.

Figure 6. United Kingdom: FCA On-Site and Desk-Based Inspections

FCA Results of On-Site and Desk Based Inspections			
	2017/18	2018/19	2019/20
Desk-Based Reviews			
Compliant	0	0	90
Partially Compliant	38	20	48
Non-Compliant	0	0	9
TOTAL	**38**	**47***	**147**
Onsite Inspections			
Compliant	0	50	1
Partially Compliant	84	14	14
Non-Compliant	14	0	15
TOTAL	**98**	**64**	**30**
TOTAL ENTITES INSPECTED	**136**	**111**	**177**

Source: IMF staff calculations.
* The FCA's 2018/19 desk-based reviews are comprised of 20 risk assurance reviews and 27 reactive case reviews. Reactive cases were not assigned a compliance rating.
Note: Onsite inspections ceased on March 16, 2020, due to the COVID pandemic restrictions.

24. The FCA is utilizing new data driven analytical tools to support risk-based AML/CFT supervision. Tools developed by the FCA analyze data provided by entities to identify outliers, which would then be inputs to identifying entities subject of monitoring. Other analytical tools on sanctions and transaction monitoring are also being developed to test the effectiveness of AML/CFT controls of supervised entities (e.g., using fuzziness tests over names of designated or sanctioned individuals). More than 2,500 of the 22,000 entities (based either on entity type or activity type) are obliged to annually submit financial crime data returns, which provides the FCA key information to assess the nature of inherent financial crimes risks (e.g., exposure to politically exposed persons, sanctions screening controls, jurisdictional risks, suspicious transaction reports, and resources to fight financial crime). As noted above, this regulatory return requires firms to provide details on those jurisdictions it has assessed and considered high-risk.

25. On entities dealing with cryptoassets, the FCA is ramping its efforts to understand their ML/TF risks, monitor registration and ensure effective supervision. The FCA was designated as the AML/CFT supervisor for cryptoasset businesses and have taken a robust approach to their registration. Those wishing to engage in cryptoasset activities first need to be registered and approved by the FCA, including those business that are already registered or authorized by the FCA

for other activities. Those seeking to obtain registration are obliged to identify their beneficial owner/s, detail their AML/CFT controls and risk assessment, ad submit to a fit and proper assessment, among others. As of end-December 2021, the FCA has approved registration for 22 entities,[30] with more than 40 other entities subject of a temporary registration.[31] These registered entities are required to conduct customer due diligence and report suspicious transactions consistent with the MLR. The authorities have noted the increased ML risks from cryptoasset exchanges, cryptoassets automated teller machines and peer-to-peer exchange platforms. The FCA is designing a dedicated supervision function to monitor AML/CFT compliance as the sector evolves. The efforts by HMT to incorporate the FATF's travel rule with respect to cryptoassets[32] are also welcome since it will require registered entities to obtain, hold and transmit identifying information of both parties in any cryptoasset transaction. This will increase information available to relevant LEAs to follow the virtual money trail.

26. Ensuring that the FCA has broad access to data from supervised entities and robust technological tools to analyze information will contribute to addressing the breadth and depth of risk-based AML/CFT supervision. Material data on supervised entities should be accessible and periodically submitted to the FCA, as inputs to its risk-based supervisory plans and strategy. While the number of entities required to file annual financial crime data returns have almost tripled (from 2,500 to 7,000 entities),[33] this remains limited and is not commensurate to the risk profile of the FCA-supervisory population. All supervised entities should be obliged to periodically submit AML/CFT returns that disclose key risk factors including risk classifications of its customer bases (including customers that are politically exposed persons[34]), products or services offered, and geographical risks. To address the expected large volumes of submissions to be received, advanced technological tools should be able to assist in analyzing these massive data points, ensure controls over the quality of the data, and flag key indicators that would further inform the analysis by FCA supervisors. As noted in the earlier section on risk profile, cross-border payments can be useful inputs to identifying unusual transaction flows, which could be flagged using big data and machine learning.

27. Use of third parties may also be considered to broaden FCA's AML/CFT supervisory reach. Currently, the FCA is empowered to appoint and engage "Skilled Persons" as part of its regulatory toolkit.[35] The objective of the FCA when using a Skilled Person is to fact find, obtain

[30] https://register.fca.org.uk/s/search?predefined=CA

[31] https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF

[32] Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022: Consultation Paper (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004603/210720_SI_Consultation_Document_final.pdf).

[33] FCA, Extension of Annual Financial Crime Reporting Obligation: Policy Statement (PS21/4), March 2021 (https://www.fca.org.uk/publication/policy/ps21-4.pdf).

[34] Under the U.K. MLR, a "politically exposed person" or "PEP" means an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official, which aligns with the FATF's definition.

[35] FCA Handbook, SUP5 Reports by Skilled Persons (https://www.handbook.fca.org.uk/handbook/SUP/5/?view=chapter).

expert analysis or recommendations on a firm for either remedial action or whether an investigation is more appropriate. A Skilled Person report can be used to diagnose a niche area or review an entity's wider AML/CFT framework. Each case is determined on a case-by-case basis. The FCA vets and selects Skilled Persons through a procurement process that assesses technical capability and commercial offering (weighted in favor of the former). The FCA may consider further leveraging Skilled Persons to support or complement supervisory activities, particularly for lower risk entities, subject to targeted and transparency guidance and criteria. Resort to such mechanism can be useful or advantageous, considering innovations to financial services (including on financial technology and cryptoassets).

28. In addition to increased government funding, the proposed Economic Crime Levy, will enable additional resources for the authorities' efforts to combat economic crime.[36] AML-regulated entities with annual U.K. revenue over £10.2m will be levied, based on the U.K. revenue size band an entity falls into, either £10,000, £36,000 or £250,000. The levy aims to generate £100m per annum to help fund new and uplifted AML capabilities, including the reform measures under the 2019 ECP. Additional resources to AML/CFT supervisory activities should also be considered, including investments on technological and analytical tools to aid risk identification and oversight (such as monitoring of cross-border payments using big data and machine learning).

29. Enforcement actions against serious AML/CFT violations by supervised entities continue to be pursued. As noted in the 2018 MER, the FCA has a broad range of tools available for enforcement.[37] These include remedial actions (e.g., use of action plans, attestations by firms, early interventions, restricting or suspending an entity's business or license) and sanctions (e.g., banning individuals from an industry, fines and disgorgements, and public censures). Since 2018, there have been more than £665 million of fines imposed by the FCA, including against more than seven large financial institutions.[38] In October 2021, the FCA secured its first criminal prosecution under the 2007 MLR, when a major bank pleaded guilty to serious AML/CFT violations and subsequently sentenced to pay fines of over £264 million. In collaboration and coordination with foreign counterparties, the FCA has also been involved in "global resolutions", where financial penalties have also been imposed against entities for AML/CFT violations. As part of a global resolution agreement (US$475 million) with US and Swiss authorities, the FCA fined a major bank in October 2021 for £147 million for failure to properly manage the risks of bribery with respect to loans related to a foreign government-sponsored project.[39] Finally, the authorities (SFO) have also utilized global deferred prosecution agreements, which allow them to leverage information from competent foreign authorities and extract a share of the penalties.

[36] HMT, Economic Crime (Anti-Money Laundering Levy: Draft Legislation (September 21, 2021) (https://www.gov.uk/government/publications/economic-crime-anti-money-laundering-levy-draft-legislation).

[37] FATF, 2018 MER, Chapter 6 on Supervision.

[38] In December 2021, a large international bank was fined over £63 million owing to deficient transaction monitoring controls and is undertaking a remediation exercise into its AML processes supervised by the FCA.

[39] FCA, Press Release: Credit Suisse fined £147,190,276 (US$200,664,504) and undertakes to the FCA to forgive US$200 million of Mozambican debt (Updated October 22, 2021) (https://www.fca.org.uk/news/press-releases/credit-suisse-fined-ps147190276-us200664504-and-undertakes-fca-forgive-us200-million-mozambican-debt)

30. Continued efforts to pursue enforcement actions will help create a deterrent impact and strengthen AML/CFT compliance by supervised entities. The FCA has several investigations against entities and individuals for AML/CFT violations ongoing, but this number could grow as the breadth and depth of supervisory activities expands. Full resort should be made to the application of the broad range of enforcement tools (particularly criminal penalties against corporations and senior managing officials) commensurate to the scale of the AML/CFT violations. With respect to corporate criminal liability, the identification principle (i.e., identifying the senior person with controlling will and mind and making their acts attributable to the supervised entity) provides for a high bar for prosecuting corporate criminal liability for economic crimes. Enhancing the legal framework on corporate criminal liability can contribute to ensuring strong AML/CFT compliance in large entities by holding senior management accountable for failure to prevent economic crimes. In this regard, the Law Commission is studying options for corporate criminal liability, including for serious violations of AML/CFT obligations by supervised entities.[40]

AML/CFT Supervision of TCSP, Legal and Accountancy Sectors

31. AML/CFT supervision of some sectors is overlapping. In particular, TCSPs can either be subject to AML/CFT supervision by the FCA, HMRC or PBSs. The 9 PBSs are responsible for supervising for AML/CFT compliance most of the accountancy sector; but HMRC also supervises other accountants, often sole practitioners working part-time with a small number of clients, where more than 95 percent are classified as low risk. Meanwhile, the legal sector is supervised by 13 PBS, where nearly two-thirds are under the Law Society/Solicitors Regulation Authority. Supervised entities can also be multi-service businesses, whereby they provide TCSP, accountancy and legal services as ancillary to their main business line (e.g., family offices).

32. OPBAS continues to intensify AML/CFT oversight of the legal and accountancy sectors by supporting deeper risk understanding by the PBSs and consistency of their supervisory approaches. Since its establishment in 2018, OPBAS has published three reports on its assessment of supervisory practices of the PBSs.[41] PBSs have made progress and are generally assessed by the OPBAS to be in technical compliance with the AML/CFT legal framework. OPBAS, however, observed variance in the level of effectiveness of implementation. For example, some of the larger PBSs (e.g., Solicitors Regulation Authority) have issued their own assessment of ML/TF risks to guide their members. However, a vast majority of the PBSs have not implemented an effective risk-based approach to AML/CFT supervision, and two thirds did not demonstrate an effective enforcement framework. OPBAS continue to guide PBSs and ensure the consistency of supervisory approaches and prevent regulatory arbitrage. Robust oversight by PBSs (including use of effective, dissuasive, and proportional sanctions) should also contribute to promoting a strong compliance culture among TCSPs, accountants and lawyers.

[40] Law Commission, Corporate Criminal Liability: A Discussion Paper (June 9, 2021). https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/06/Corporate-Criminal-Liability-Discussion-Paper.pdf

[41] OPBAS Reports of March 2019, March 2020, and September 2021.

33. Efforts by OPBAS to inform and raise awareness of key ML/TF risks in the accountancy and legal sector are positive developments. In conjunction with the NECC, OPBAS established two Intelligence Sharing Expert Working Groups (ISEWGs), each for the accountancy and legal sectors. ISEWGs are aimed at facilitating the increase of information sharing between the PBS, LEAs, AML/CFT supervisors and other relevant agencies. This includes both strategic intelligence sharing (developing common understanding of emerging or existing ML/TF threats) and tactical intelligence sharing (developing high quality live intelligence sharing with LEAs). ISEWGs provided support and inputs to the 2020 NRA exercise, which helped identify additional key factors contributing to the high ML/TF risks in the accountancy and legal sectors. Through typology reports, alerts, and anonymized case studies, the ISEWGs create a virtuous feedback loop, ensure consistency, and build trust between public and private stakeholders (e.g., supervisors and LEAs can gain operational perspective on transactions and flows; while supervised entities are informed of trends to better calibrate their AML/CFT controls). Such information sharing platforms should continue and help foster deeper understanding and awareness of risks in these two high risk sectors.

34. Given the high risk of the TCSP, accountancy and legal sectors, the U.K. authorities should further explore mechanisms that ensure consistency of AML/CFT supervisory approaches. For low capacity or high-risk PBSs, the OPBAS could be given discretionary power to directly conduct AML/CFT supervision to maximize efficiencies and better harmonize supervisory approaches. While some PBSs can manage and effectively perform their AML/CFT supervisory responsibilities, opening the possibility of direct AML/CFT supervision could be an alternative approach for other PBS that may not have the same degree of resources or capacities. Such an expansion of OPBAS's powers would require legal amendments and entail additional resources. Notably, the issue of extending OPBAS's remit and powers is one of the questions in the HMT's call for evidence on the AML/CFT regulatory and supervisory regime, in addition to the broader question of the overall supervisory model (i.e., whether to seek a degree of consolidation of the supervisory regime towards a model with fewer, very few, or even a single supervisor).[42]

E. Entity Transparency

35. The United Kingdom remains a global leader in promoting entity transparency. The 2018 MER recognized that the United Kingdom's system for entity transparency goes beyond the FATF technical standards in some respects (particularly open and public access to beneficial ownership information). In the ECP, the U.K. authorities recognized that identifying the person who owns and ultimately controls a corporate entity is vital to exposing wrongdoing and disrupting economic crimes. Thus, the authorities committed to improving their system for transparency of ownership of legal entities and legal arrangements as one of their strategic priorities under the ECP. Established in 2016, the People with Significant Control (PSC) Register is a pioneering effort that

[42] HMT, Call for Evidence Review of the U.K.'s AML/CFT Regulatory and Supervisory Regime (July 2021) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004602/210720_MLRs_Review_Call_for_Evidence_final.pdf).

allows full and free public access to beneficial ownership information[43] of U.K. legal entities (including Scottish limited partnership as of 2017). Such legal entities are required to submit annual statements confirming the beneficial ownership information and notifying the Companies House of any changes to beneficial ownership information within 28 days. Finally, legislative proposals on public procurement are also being developed that would mandatorily exclude bidders from competing for public contracts if they do not disclose their beneficial owner/s.[44]

36. Discrepancy reporting obligations are contributing to ensuring accuracy of the beneficial ownership information in the PSC Register. A 2019 review revealed that most stakeholders (e.g., law enforcement agencies, civil society organizations) found a positive impact of the PSC register to their work, but suggested validation and verification processes to improve the quality of the beneficial ownership information.[45] In line with the ECP (Action Item No. 43), requirements were introduced that obliged entities with AML/CFT obligations to submit and report any discrepancies in the PSC register in the course of their own customer due diligence activities. A discrepancy exists when the supervised entity has information that clearly indicates that the PSC information recorded by Companies House is inaccurate (i.e., clear factual errors, not typing mistakes). Since the implementation of the discrepancy reporting obligations in January 2020, there have been more than 42,000 discrepancy reports filed with Companies House.[46] Financial institutions make up almost all originators of discrepancy reports (more than 93 percent of all submissions); with less than 5 percent coming from TCSPs, accountancy, legal and real estate sectors. Most of the discrepancy reports are either the beneficial owner is missing or further information on the beneficial owner is lacking (e.g., date of birth).

37. The authorities continue to advance in improving the quality and accuracy of the beneficial ownership information in the PSC register. The quality of beneficial ownership information contained in the PSC Register is generally reliant on self-reporting by U.K. legal entities. Enforcement actions against non-submission or false information is thus critical to incentivizing truthful disclosures and enhancing accuracy of the beneficial ownership information. Legislation is being proposed to introduce compulsory identity verification for all directors and beneficial owners of U.K. registered companies and require compulsory identity verification for those that file beneficial ownership information in the PSC register.[47] Increased efforts by supervised entities

[43] Under the U.K. Companies Act (Schedule 1A), the PSC (or beneficial owner) of a legal entity is any natural person who generally complies with any of the following conditions holds more than 25 percent of shares or voting rights in the legal entity, can appoint or remove most of the legal entity's board of directors, or has the right to exercise significant influence or control over the company or trust.

[44] Cabinet Office, Green Paper: Transforming Public Procurement (December 15, 2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/943946/Transforming_public_procurement.pdf

[45] BEIS, Review of the Implementation of the PSC Register (2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822823/review-implementation-psc-register.pdf

[46] As of November 2021, the total number of discrepancy reports received by Companies House is at 58,147.

[47] BEIS, Corporate Transparency and Register Reform (September 18, 2020).

(particularly TCSPs, accountants and lawyers) to monitor and report discrepancies should also be encouraged.

38. The powers of Companies House over the information in the PSC register should be strengthened. As the custodian of the company formation regime, Companies House has limitations in querying information presented to them (i.e., it generally cannot verify the accuracy of what it receives).[48] To ensure that information submitted is accurate, Companies House should be able to verify the beneficial ownership information submitted to it (including the individuals filing the information) and unilaterally remove information from the PSC Register, if it is found to be inaccurate. Access to other database will allow Companies House to cross-reference relevant data that will contribute to efforts to verify the accuracy of the beneficial ownership submitted to the PSC Register. Enhanced resources and analytical capabilities should strengthen Companies House's capacity to identify red flags and facilitate information sharing with AML/CFT supervisors, LEAs, and other competent authorities.

39. Beneficial ownership information of trusts is being collected and made accessible to competent authorities. Under HMRC, the Trust Registration System (TRS) covers and makes available to competent authorities the beneficial ownership information of more than 170,000 U.K. express trusts[49] (with and without U.K. tax liabilities).[50] The majority of trusts on the register, including all trusts required to register for the purpose of combatting ML/TF, are required to report any changes to their beneficial ownership information within 90 days. All relevant U.K. express trusts are currently required to register by September 1, 2022, and thereafter new trusts are required to register within 90 days of their formation. Given the criticality of the ownership information contained in the TRS, the authorities should continue to ensure that mechanisms are available to foreign counterparties to timely access such information, especially in cases where the registered trust has a link to the foreign jurisdiction (e.g., a U.K. trust owning foreign assets located outside of the United Kingdom).

40. Given the ML risks from the real property sector, efforts to boost transparency of beneficial ownership of real properties held by foreign entities should be prioritized. U.K. property purchases have been identified in the 2017 and 2020 U.K. NRAs as an attractive means of laundering large amounts of illicit funds, especially when made by corporate structures or trusts created in high risk or secrecy jurisdictions.[51] The proposed Overseas Entities Bill is a step in the right direction to address this since it would ensure public access to beneficial ownership information of foreign entities owning U.K. properties.[52] This would complement existing legal

[48] BEIS, Review of the Implementation of the PSC Register (BEIS Research Paper Number 2019/005).

[49] "An express trust is a trust created deliberately by a settlor, usually in the form of a document such as a written deed or declaration of trust." (HMRC, Trust Registration Service Manual, TRSM21030)

[50] The 2020 amendments to the MLRs expanded the scope of TRS to also include UK express trusts without UK tax liabilities.

[51] In addition, a Stamp Duty Land Tax surcharge is to be imposed beginning April 1, 2021, for non-resident buyers of residential property in the UK, including against non-resident legal persons (e.g., corporations) and legal arrangements (e.g., trusts).

[52] BEIS, Draft Registration of Overseas Entities Bill (July 2018). See also ECP, Action Item No. 44.

requirements for real estate agents and lawyers to conduct customer due diligence on property transactions. Greater ownership transparency will help prevent real properties from being abused for ML purposes (e.g., corrupt foreign officials laundering their illicit wealth in London luxury apartments). Similarly, mechanisms to verify the accuracy of the information would need to be incorporated (e.g., identity verification, discrepancy reporting, enforcement mechanisms for non-submission or false information).

F. International Cooperation

41. The 2018 MER recognized the broad range of timely and constructive international cooperation that the U.K. authorities provide. The United Kingdom received a substantial effectiveness rating for international cooperation (IO2). The MER identified three central authorities with respect to mutual legal assistance: (i) the U.K. Central Authority in the Home Office for requests relating to England, Northern Ireland, or Wales; (ii) the International Mutual Assistance Team in HMRC for requests relating to tax matters; and (iii) the International Co-operation Unit of the Scottish Crown Office and Procurator Fiscal Service for requests relating to Scotland.[53] The United Kingdom was assessed to provide high-quality, constructive and timely mutual legal assistance and a wide range of assistance. An extensive overseas criminal justice network of U.K. law enforcement officers (investigators and prosecutors) acting as liaisons covering over 160 jurisdictions also facilitates formal and informal cooperation. Established in 2018, the multi-agency National Economic Crime Centre leads the United Kingdom's response to domestic and foreign economic crimes, and harnesses intelligence from public and private sectors.[54] The FATF recommended that the authorities continue to improve coordination on MLA requests and the collection and maintenance of consistent, national statistics on international cooperation.

42. Another strong feature of United Kingdom's international cooperation system is the leveraging of strong domestic public and private partnerships. The Economic Crime Strategic Board was created in January 2019 to set priorities for addressing economic crime, which includes the Home Secretary, Chancellor as well as senior representatives from the private financial sector. The Joint Money Laundering Intelligence Taskforce (JMLIT) is a public-private partnership that aims to implement a "whole of system" approach to exchanging analysis and information relating to economic crime threats and risks. Through the NCA, foreign counterparts can submit cases to the JMLIT, to generate financial intelligence, which also utilizes information and data from supervised entities, aside from LEAs.

43. The U.K. authorities noted little difference in post-Brexit cooperation and financial intelligence sharing with EEA authorities. Information sharing with EEA countries was previously facilitated by a wide range of regional cooperation tools and information sharing gateways. In the last four years (2018–2021), most of the United Kingdom's international cooperation activities

[53] The UKCA handles a significant portions of incoming mutual legal assistance requests. (2018 MER, paragraph 465.)

[54] NECC include representatives from NCA, SFO, FCA, HMRC, City of London Police, Crown Prosecution Service, Cabinet Office, Home Office, and Foreign, Commonwealth and Development Office.

(incoming exchange of information and mutual legal assistance requests) was with EEA countries. Sustained efforts in keeping the existing strong channels for information sharing are encouraged.

44. The robust frameworks for confiscation, asset recovery and targeted financial sanctions provide the authorities valuable tools that can be leveraged, given the United Kingdom's status as a global financial center and attractive destination for illicit foreign financial flows. There are a broad range of seizure and confiscation tools that can be utilized by LEAs against assets in the United Kingdom that are involved in criminal activities. Unexplained Wealth Orders (UWOs) is a civil power and investigation tool that places the burden on the respondent to provide justification as to the sources of funds used to purchase U.K. assets.[55] Such tools are not only useful for seizing and confiscating illicit assets in the United Kingdom; they can further build evidence or unearth further intelligence that could be beneficial to foreign criminal investigations. In 2021, the Global Anti-Corruption Sanctions Regulations were established which allows the designation of persons involved in serious corruption and the freezing of their U.K. assets.

45. The U.K. authorities should maintain strong information sharing mechanisms with CDs and BOTs, given the ML risks involving entities created in these jurisdictions. In 2016, the United Kingdom had bilateral agreements (Exchange of Notes) that would allow timely sharing of beneficial ownership information for legal entities and legal arrangements registered in CDs and BOTs. Law enforcement and tax authorities in the United Kingdom, CDs and BOTs are to be provided by their counterparties with the requested beneficial ownership information within 24 hours, or if the request is urgent, within one hour. Such timely access has been useful to U.K. LEAs in investigating complex and cross-border criminal cases, adding significant value in providing time sensitive information.[56] However, efforts need to continue to ensure that the registers in the CDs and BOTs are complete and the accuracy of the information are effectively verified.

46. The U.K. authorities should continue to support BOTs and engage CDs in having robust beneficial ownership registers that are effective and well-calibrated. Under the Sanctions and AML Act of 2018 (Section 51), the Secretary of State is tasked to provide all reasonable assistance to BOTs to enable them to establish a publicly accessible register of the beneficial ownership of companies registered in each government's jurisdiction. Given the lessons learned from the operations of the PSC Register, the U.K. authorities are well placed to provide technical, legal, financial, and other relevant support to high-risk or low-capacity BOTs (including on public access and discrepancy reporting). The FCDO's draft Order in Council outlines expected key features of the register, including public accessibility and information of the beneficial owner that is deemed relevant and required to be kept.[57] A network of publicly available and accurate beneficial

[55] U.K. Proceeds of Crime Act 2002 (Sections 362A-362I).

[56] U.K. Statutory Review of the Implementation of the Exchange of Notes on Beneficial Ownership Between the United Kingdom, Crown Dependences and Overseas Territories (June 27, 2019). https://www.gov.uk/government/publications/statutory-review-of-the-exchange-of-notes-arrangements/statutory-review-of-the-implementation-of-the-exchange-of-notes-on-beneficial-ownership-between-the-united-kingdom-crown-dependencies-and-overseas-te

[57] FCDO, Overseas Territories (Publicly Accessible Registers of Beneficial Ownership of Companies). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/943307/SAMLA_s51_Draft_Order_in_Council.pdf

ownership registers in these jurisdictions will be an invaluable resource for foreign criminal investigations, as demonstrated by the immense utility derived from the United Kingdom's own PSC register. Similarly, considering public commitments made by CDs to establish public access to beneficial ownership data of companies held in a central register.[58] the U.K. authorities are encouraged to engage CDs in dialogue on experience with the PSC Register and good practices.

STRENGTHENING THE OVERSIGHT OF RISKS OF CYBER THREAT

A. Executive Summary

47. Safeguards against the growing exposure to cyber risks has become a top financial stability concern of the U.K. authorities and has an important bearing on the findings of the FSAP. In June 2017, the Financial Policy Committee (FPC) set out a regulatory strategy aimed at strengthening the U.K. financial system's ability to withstand, and recover from, cyber incidents. The strategy is supported by a fast developing institutional and regulatory framework, innovative supervisory approaches, extensive testing practices, and communication policy.

48. This focus is vital for the United Kingdom. Materialization of cyber risks at systemically important banks, insurers and financial market infrastructures carries important ramifications for the wider financial system and its potential cross border spillovers. A cyber incident at a critical third-party service provider could impact a series of financial institutions and result in a systemic event. Indeed, the United Kingdom recognizes that significant incidents with near systemic consequences have already occurred globally. Single-firm incidents like a disruption or an integrity compromise of a critical service could also have an adverse impact on the financial system, if the firm's size, non-substitutability, and interconnectedness exceeded certain thresholds. In addition, because of the global importance of the U.K. financial system, cyber shocks could be transmitted well beyond its national borders through interconnectedness and financial contagion.

49. The U.K. authorities have been developing a principles-based and outcome-focused regulatory framework to address cyber risk. General risk management expectations are implicit in the PRA threshold conditions and FCA principles of business, which are complemented with an operational resilience framework and a series of specific policies that address well-known, as well as emerging topics, including cyber resilience, business continuity and contingency planning, governance, and third-party risk management. The regulatory framework is consistent with and builds on international good practices, guidelines, and cross-sectoral cybersecurity standards.

50. In an appropriate response, the U.K. authorities oversee cyber resilience by regulating and supervising both the sector (macro-prudential) and single firms as single entities (micro-prudential) and collaborating and coordinating the sector. The CBEST penetration testing

[58] Joint Commitment by Guernsey, Jersey, and the Isle of Man: Registers of Beneficial Ownership Companies (June 2019). https://www.gov.gg/CHttpHandler.ashx?id=119716&p=0

program, aimed at realistically assessing the effectiveness of cyber defenses with simulated attacks, forms the cornerstone of the testing strategy. Supervisory dialogue is used to gain deeper insight into the cyber resilience strategies and capabilities of regulated firms (non-regulated financial firms are not yet being covered). Severe, but plausible scenarios are played out in various simulation exercises organized in public-private partnerships, e.g., under the auspices of the Cross Market Operational Resilience Group (CMORG). Industry information sharing and response is coordinated through the Finance Sector Cyber Collaboration Centre (FSCCC) and Finance Emergency Call Cyber (FinECC).

51. Given the 'nuts and bolts' and the evolving nature of cyber risk management, focus on the following issues is highly desirable to further strengthen the current effectiveness of cyber risk management:

a. **Changes to the operational resilience framework need to be conveyed in a timely and consistent manner.** Regulated financial institutions started implementing the operational resilience framework and outsourcing and third-party risk management requirements in 2021, with the first industry results expected in 2022. The principle-based and outcome-focused approach allows for multiple interpretations and could result in diverging implementations. Supervisory authorities are advised to clearly communicate expectations and provide guidance on identified implementation challenges.

b. **Complement existing supervisory practices with on-site activities to verify the operational effectiveness of firms' cybersecurity controls.** These on-site examination activities would add value in at least three areas: providing a higher level of assurance over the operational effectiveness of cybersecurity controls; encouraging candor by senior management; and developing a deeper understanding on the way supervised firms are organized and operated, including the corporate culture.

c. **Formalization as well as an alignment of the reporting requirements, processes and tools is recommended.** The general notification requirements do not provide firms with specific guidance and criteria for cyber incident reporting, which could result in inconsistencies and underreporting.

d. **Improve the already effective penetration testing program.** In addition to the new implementation guideline, templates, and reporting guidelines, authorities could consider opportunities for leveraging internal threat intelligence and/or testing capabilities of firms, subject to meeting CBEST accreditation criteria. Allowing firms to use their internal capabilities — subject to the same stringent requirements as external providers — could stimulate the adoption of tests like STAR-FS. Additional learning opportunities for CBEST participants could be created through grey box testing and purple teaming.[59] A generic threat intelligence report for smaller

[59] Grey box testing is an approach in which testers are given some information on the target environment, for example of a such nature and extent that a persistent and well-resourced attacker can reasonably obtain. Purple teaming means that the testers and the defenders regularly meet and exchange information during the test to maximize the benefits of the exercise.

firms could assist in further broadening access to cyber threat intelligence led testing in the U.K. financial system.

52. Finally, the U.K. authorities are encouraged to:

a. *Seek additional statutory powers to directly assess the resilience (including cyber resilience) of any critical services that third party service providers.* Systemic firms' growing reliance on critical third parties for the provisioning of vital services could increase financial stability risks, especially in the absence of greater direct regulatory oversight. BOE, PRA, FCA and HMT, under impulse of the FPC, should further their thinking on specifying resilience standards for these providers as well as their inclusion in resilience testing. It should be noted however that there are limits to the extent to which financial regulators alone can effectively mitigate the risks of critical third parties (including cloud outsourcing) absent an appropriate cross-sectoral regulatory framework and cross-border cooperation.

b. *Continue meeting regulatory and supervisory demands for internal cyber expertise*, which is expected to further increase.

c. *Increase the supervisory attention on thousands of other U.K. regulated financial services firms that are facing important cyber risks*. Cyber incidents at non-systemically important firms are not likely to result in systemic events but could impact other objectives like customer protection.

See Table 2 for summarized recommendations.

B. Introduction[60]

Further the Resilience Against Cyber Risk

53. Constantly evolving cyber threats require vigilance from the financial institutions, regulators, and supervisory authorities alike. Malicious cyber actors with varying level of sophistication continue to evolve and innovate their tactics, techniques, and procedures (TTPs). The first half of 2021 has been characterized by the exploitation of a series of critical zero-day vulnerabilities[61] (e.g., in F5 Big-IP, MS Exchange, and Pulse Secure), supply chain attacks, and distributed denial-of-service attacks. Additionally, non-malicious incidents like accidental data disclosures and configuration, implementation or processing errors continue to be an important source of cyber risk.[62]

[60] This chapter was prepared by Tamas Gaidosch (IMF) and Filip Caron (IMF Expert).

[61] Zero-day vulnerabilities are weaknesses in a system not known to security researchers, developers, and operators. If cyber threat actors discover these first, exceptional opportunities to hack high-value targets may occur.

[62] While the UK authorities' definition of cyber risk does not include risk stemming from non-malicious intent, these are covered in the wider strategy.

Table 2. United Kingdom: Main Recommendations	
Recommendation	**Timing[1]**
Institutional and regulatory framework	
1. Regulators should continue reviewing cyber risk, and more broadly, technology risk management expectations with the aim to publish more specific guidance and/or industry best practice.	ST
2. The Bank/PRA and FCA should seek additional statutory powers to assess the resilience (including cyber resilience) of any critical services that third party service providers provide to regulated financial institutions, as recently suggested by the Bank of England Financial Policy Committee (FPC).	ST
3. The Senior Managers and Certification Regime should be extended to BOE supervised FMIs as currently being consulted on by HMT.	ST
4. Cyber risk reporting processes, including for cyber incidents and material outsourcing arrangements, should be aligned across the different regulators based on specific criteria and templates.	ST
Supervisory practices	
1. Supervisors should conduct additional cybersecurity control verification activities to complement desk-based analytical work, supervisory engagement, and CBEST testing.	ST
2. Regulators should further strengthen their operational and cyber resilience supervisory teams.	ST
3. The CQUEST cybersecurity questionnaire could be usefully augmented with requiring that firms provide evidence to support the self-assessment.	ST
4. Prioritize developing the proposed cyber resilience maturity assessment framework of the core assurance framework to gain better insight in the cyber resilience posture of the supervised FMIs, and to communicate the supervisory expectations according to defined maturity levels.	ST
5. Regulators should consider additional opportunities to strengthen the penetration testing framework.	MT
6. The usefulness of cyber stress testing could be greatly improved with quantifying the impact on liquidity and capital buffers. It would be beneficial to assess the impact of severe but plausible cyber incidents on liquidity and capital buffers. [2]	MT
7. Broad international representation and key functions in standard setting bodies could be further leveraged to promote internationally better aligned supervisory expectations and tools.	MT

[1] I Immediate (within 1 year); ST Short term (within 1–2 years); MT Medium Term (within 3–5 years)
[2] The PRA has started incorporating cyber scenarios in their financial resilience testing

54. The shifts in business operating practices and use of technology in response to COVID-19 pandemic are increasing the vulnerability to cyber risk threats. In general, financial institutions' existing business continuity plans and home working arrangements have been successfully leveraged to maintain operational resilience. But malicious cyber actors have been exploiting the COVID-19 pandemic theme, for example in phishing campaigns, and certain cybersecurity controls needed to be relaxed all the while the attack surface grew due to the increased use of potentially vulnerable services and personal devices. Furthermore, pandemic response measures often impacted financial institutions' ability to respond to additional operational stress.

55. The U.K. authorities have identified cyber risk as a top financial stability concern within the broader operational resilience agenda. A cyber incident impacting the confidentiality, integrity or availability of a financial institutions' critical activities may have the potential to destabilize that institution. U.K. supervisory authorities focus on outcome-based assessments and the supervisees' cybersecurity controls' design adequacy.

56. The materialization of a cyber risk may have ramifications for the wider financial system, both domestic and international. While not every cyber incident at a systemically important financial institution threatens the financial stability of the jurisdiction, systemic impact resulting from a cyber incident is conceivable under certain conditions. For a single-firm incident to impact the wider financial system a series of size, non-substitutability and interconnectedness threshold criteria would need to be exceeded. Category 1 supervised institutions and BOE supervised FMIs generally meet these criteria.[63]

57. Critical third parties are increasingly identified as a potential source of a systemic cyber events. Compromising widely adopted technology solutions could be an effective manner of impacting a series of financial institutions at the same time. Due to economies-of-scale and network effects, plus the potential for improvements in the resilience of individual institutions, technological diversity between institutions is decreasing. Financial institutions are adopting common software solutions, acquiring highly similar hardware components, and migrating to a select set of global Cloud Service Providers (CSPs). A cyber incident in the supply chain could be propagated via confidence and financial contagion channels.

58. Continuous enhancement of operational and cyber resilience is becoming the norm as cyber incidents are bound to happen. Although not necessarily destabilizing events, most financial institutions report having faced cyber incidents over the last year. Strong capabilities to timely detect anomalies and compromises, as well as to respond and recover are critical in the current cyber threat landscape.

[63] The CPMI-IOSCO guidance on cyber resilience for financial market infrastructures refers to the need for an orderly settlement by the end of the day to avoid systemic events.

Review Scope: Systemic Banks and Financial Market Infrastructures

59. The note reviews key elements of the cybersecurity regulatory and supervisory approach for the financial sector in the United Kingdom. This includes the role and practices of the U.K. authorities[64] in the development and maintenance of the cybersecurity regulatory framework, cyber threat intelligence gathering, cyber risk related information sharing, on-site and off-site supervisory processes, cybersecurity testing and operational resilience.

60. This review is limited to the framework for systemically important banks, insurers, and financial market infrastructures. Supervisory practices for non-systemic financial institutions in the United Kingdom were out of scope for this review.[65] Single-firm cyber incidents with the potential to become systemic events are typically limited to the institutions in scope. However, cyber incidents at other institutions might also threaten regulators' objectives, for example, financial stability in case of a coordinated multi-firm attack. The designation of critical national infrastructure in the financial sector, as well as additional expectations and arrangements[66] regarding their cybersecurity posture and resilience, were also out of scope.

61. The mission collected information from several sources. These include questionnaire answers provided by the BOE, PRA, FCA and HMT, interviews with both authorities and supervised institutions, the study of relevant national laws and reports published by the authorities, as well as documentation of their work.

62. Conclusions and recommendations of the review are aligned with international regulatory and supervisory good practices. As there are no binding international regulatory standards on cybersecurity risk management, the mission team used internationally recognized regulatory good practice as the basis of this report. The following documents were used as a benchmark in the assessment: the FSB Stock take of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices; the BCBS Cyber-resilience: Range of practices; the IMF Departmental Paper on Cybersecurity Risk Supervision and the G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector. The basis of the review in the case of FMIs was the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.

C. Institutional and Regulatory Framework

Legal Basis

63. The BOE, PRA and FCA objectives and responsibilities in mitigating cyber risks and strengthen resilience of the United Kingdom's financial sector stem from their broad statutory objectives and responsibilities. Cyber risk regulation and supervision of systemically

[64] The term "U.K. authorities" refers to the Bank of England (BOE), the Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA) and HM Treasury (HMT). References to UK regulators indicate involvement of the BOE, PRA and FCA.

[65] The PRA supervises around 1,500 institutions and the FCA supervises about 49,000, while the number of systemically important institutions is 29 (i.e., 15 banks, 10 FMIs and four insurers).

[66] Relative to expectations and arrangements by the financial supervisory authorities.

important banks and insurers is conducted jointly by the PRA and FCA, focusing respectively on cyber risks which could affect the safety and soundness of regulated firms, and which could cause detriment to consumers or the integrity of the market. The BOE plays an important role in mitigating cyber risks that could affect the financial stability of the system. In addition to FMIs, the BOE also regulates firms that provide critical services to recognized payment systems, by virtue of the statutory power of HMT to bring them in the BOE remit.

64. Authorities' statutory powers are defined in the Financial Services and Markets Act of 2000 (FSMA 2000) and the Banking Act of 2009 and are fully applicable in cyber risk and resilience matters. The regulators have broad statutory powers to set the rules related to the mitigation of cyber risks, as well as to supervise and enforce these rules. Furthermore, they have powers regarding information-gathering and dealing with failing financial institutions. HMT has statutory powers to respond to disruption, including those induced by cyber incidents. HMT can also propose legislation that changes the statutory powers of the regulators to Parliament.

65. The FSMA 2000 provides the PRA and FCA with the statutory power to request "skilled person reports", which is a highly effective but not regularly used supervisory tool. A skilled person report (Section 166 of the FSMA 2000) can be commissioned for the following purposes: to identify, measure and address risks; to monitor the development of identified risks; to limit or reduce the impact or likelihood of identified risks; and to define and implement adequate responses for materialized risks. However, this tool has been used very sparingly. For example, in the last three years the supervisor authorities, together, commissioned six skilled person reports in the field of Technology and Information Management (Lot J).

66. The Banking Act 2009 allows HMT to include specified service providers to recognized payment systems in the recognition order of payment system operators. Based on Section 206A, HMT can bring the specified service provider within the regulatory remit of the BOE. So far, there is only one such firm in the United Kingdom.[67] Part five of the Banking Act 2009 gives statutory powers including information-gathering, reviewing proposed appointments, directions and enforcement, and special administration regime.

67. The cybersecurity framework for the financial sector is principles-based and outcome-focused. The different components of the cybersecurity regulatory framework provide a series of high-level expectations grounded in current internationally recognized best practices. In general, advanced financial systems with mature risk management practices benefit more from a principles-based approach. A focus on outcomes rather than prescriptive rules allows for more proportionality and risk-based supervision. At the same time, it could lead to variance in interpretation, challenges regarding consistency across firms and potentially debatable findings. Strong regulatory engagement and soft power is needed to address these challenges.[68]

[67] This is Vocalink, a technology service provider for some payment systems and ATM switching platforms.

[68] Firm specific guidance offered by the NCSC to critical national infrastructure was out of scope for this review.

68. While not financial sector regulators themselves, HMT, and the National Cyber Security Centre (NCSC) work closely with the U.K. regulators and financial institutions on cybersecurity matters. HMT focuses on mitigating cyber risks with the potential to cause economic or societal harm or harms to public finances. As the United Kingdom's National Technical Authority for cyber security, the NCSC provides technical cyber security advice to both regulators and financial institutions.

Regulators' Governance Structure

69. Cyber risk forms an integral part of the discussion in different PRA and FCA risk and policy committees, resulting in it being integrated in the holistic risk view for the financial sector. There are five key Bank of England/PRA committees that deal with cyber risk and resilience: (i) the Financial Policy Committee (FPC) considers the financial stability and systemic aspects of cybersecurity and resilience; the Prudential Regulation Committee (PRC) is the highest decision-making committee for the PRA and has responsibility for key micro-prudential decisions, including issuing new rules; (iii) the PRA's Supervision, Risk, and Policy Committee (SRPC) oversees the risk portfolio, discusses thematic findings, reviews the appropriateness of the cyber risk supervisory tools and processes, and approves their updates; (iv) the FMI Board is the highest decision-making committee of the BOE in its capacity as supervisor of FMIs and critical service providers to recognized payment system operators within the BOE's regulatory remit and (v) the Executive Committee is involved and consulted on the PRA cyber macro and microprudential strategy, cyber threat landscape, and the FPC cyber agenda. The FCA committees that are involved in cyber risk matters are: (i) the Executive Committee, which issues general guidance as defined by law and oversees crisis management arrangements including operational continuity; and the (ii) Executive Regulation and Policy Committee (ERPC), which oversees regulatory issues and is responsible for executive decision making.

70. The supervisory authorities have adopted a center-of-excellence model, which allows more flexible and risk-based assignment of deep technical expertise. Within the Bank, the Operational Risk and Resilience Division (ORRD) within the Supervisory Risk Specialists (SRS) directorate provides deep technical cyber risk expertise in support of PRA supervision and working with risk specialists within FMID, FMID supervision. Specifically, the ORRD informs and shapes regulation, and supports line supervisors and supervisory judgments based on specialist expertise, data analytics, and modeling. Each PRA supervision directorate has operational resilience hubs that are more focused on the market segment of the directorate, i.e., U.K. deposit takers, international banks, and insurance companies. Hubs therefore work more closely with line supervision and combine business understanding and cyber expertise. With the support of the ORRD cyber specialist team (and, where appropriate the Legal Directorate and Prudential Policy Directorate) this results in an effective organizational setup. Similarly, the FCA's Technology, Resilience and Cyber (TRC) department provides technical expertise to supervisors and firms so that they become more resilient to both cyberattacks and other disruption.

Macroprudential Framework

71. Discharging BOE's responsibility to mitigate systemic cyber risk, the Financial Policy Committee (FPC) is the key governance body that develops the macro-prudential cyber risk mitigation and resilience framework. The FPC had formally recognized cyber threat as a risk to financial stability in 2013 and recommended establishing a work program to improve and test cyber resilience. Shortly thereafter, in 2014, the regulators launched the CBEST penetration testing program, globally the first of its kind. (See section on Testing) Leveraging the experience gained the FPC then evolved its recommendation to make CBEST a component for regular testing of the cyber resilience of the U.K. financial system. Then, in 2017 it set out a more specific framework driven by the FPC priorities that focuses on cyber resilience and testing with four key elements: (i) clear and proportional baseline resilience expectations; (ii) regular resilience testing by both firms and supervisors; (iii) identification of important firms outside of the regulatory perimeter; and (iv) clear and tested cyber incident response arrangements.

72. Besides discharging their micro-prudential supervisory responsibilities, the PRA's, FCA's and FMID's work operationalize the FPC's priorities in the cyber context. Examples include the recent operational resilience framework and expectations on outsourcing and third-party risk management (see section on Outsourcing and Third-Party Risk); the strengthening of the CBEST security testing program; and the cyber stress test program.

Microprudential Expectations and Additional Guidance for Cybersecurity

73. Cyber risk management expectations are implicitly included in the threshold conditions and fundamental rules that establish general expectations on risk management. The PRA Fundamental Rules and the FCA Principles for Business set out general risk management expectations, that are applicable to the identification and management of cyber risks and outsourcing risks, as well as business continuity and contingency planning. These rules are sufficiently broad to cover all aspects of cyber risk management practices at supervised financial institutions, however they do not have any technology or cyber risk specific provisions.

74. Supervisory expectations from U.K. regulators for financial institutions are further detailed in a series of supervisory statements and guidance. Figure 7 provides a schematic overview of the cybersecurity regulatory framework for systemic banks in the United Kingdom. The regulatory framework is informed by international good practice captured in frameworks like the NIST Cyber Security Framework, and cross-sectoral cybersecurity standards.

Figure 7. United Kingdom: United Kingdom's Regulatory Framework for Cybersecurity at a Microprudential Level

Source: Bank of England.

75. International principles and guidance form the basis for cyber risk and resilience reviews at the FMIs. The supervision of FMIs is conducted against the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) and the Guidance on Cyber Resilience for Financial Market Infrastructures. Principles cover cyber governance, identification, protection, detection, response, and recovery (including a two-hour recovery time objective), testing, situational awareness, and learning and evolving. This guidance stays principle-based and mostly non-prescriptive, which allows for a degree of flexibility in their implementation.

76. The recently adopted operational resilience framework (ORF) provides a holistic strategic framework that brings together the different areas of financial regulation relevant to operational (including cyber) incidents, i.e., operational risk management, business continuity and contingency planning, data security, outsourcing and third-party risk management. In addition, the ORF leverages the U.K. regulators' requirements and expectations on corporate governance and individual accountability, the Senior Managers and Certification Regime (SM&CR). In addition to the abovementioned detailed requirements and expectations [69], the regulators published in March 2021 their ORF (i.e., PRA PS6/21 and FCA PS21/3). This requires supervised financial institutions to:

- identify their important business services that if disrupted could cause harm to consumers or market integrity, threaten the viability of firms or cause instability in the financial system.

[69] As established by the general organizational requirements of the PRA Rulebook and SYSC4 and SYSC13 of the FCA Handbook.

- set impact tolerances for each important business service, which quantify the maximum acceptable level of disruption they would tolerate.
- identify and document the people, processes, technology, facilities, and information that support their important business services; and
- take action to remain within their impact tolerances through a range of severe but plausible disruption scenarios.

77. Dually supervised financial institutions must comply with both PRA and FCA expectations on impact tolerances. This is due to differences in statutory objectives and supervisory priorities. Generally, FCA requirements result in tighter tolerances, because in a cyber incident consumer harm usually occurs earlier than material impact on the safety and soundness of the firm.[70] However, the PRA and FCA developed their respective policies simultaneously and in close coordination and consider them to be aligned. Complying with the PRA's and FCA's respective expectations is not perceived as a major difficulty by the industry as the highest resilience expectation will implicitly set the bar and firms may concentrate their efforts in ensuring they can remain within the more stringent tolerance.

78. The European Banking Authority's Guidelines on Information and Communications Technology and Security Risk Management have been onshored. These guidelines (EBA/GL/2019/04) define good practices for the mitigation and management of information and communication technology risks. Credit institutions, investment firms and payment service providers are required to:

- Establish sound internal governance and internal control frameworks.
- Manage and mitigate ICT and security risks through an independent and objective control function.
- Develop information security policies and training, as well as conducting reviews, assessments, and tests.
- Improve the monitoring and management of ICT operations, including the implementation of logging and monitoring procedures, as well as actively managing assets' lifecycles.
- Reinforce project and change management procedures; and
- Adopt appropriate business continuity management and develop response and recovery plans.

Following the Brexit transition period, the BOE and PRA expect firms and FMIs to continue to make every effort to comply with existing EU Guidelines and Recommendations that are applicable as at the end of the transition period, to the extent that these remain relevant.

79. A key element of the cyber risk regulatory framework is the Senior Managers and Certification Regime (SM&CR). The SM&CR establishes individual accountability and responsibility for senior managers of financial institutions along several Senior Manager Functions (SMFs). In terms

[70] This is also dependent on the nature of the business and the services affected.

of operations and technology, including cybersecurity, SMF24 function holders are accountable and responsible to a financial institution's board and the regulators (in this context the PRA and FCA) for that firm's operations and technology. Through this mechanism the regulators aim to facilitate the development of an appropriate cybersecurity governance and organizational culture, both key priorities. Interestingly, SMFs can be shared but not split, with the single exception of the SMF24, which could be split as well, for example between an equally senior Chief Operating Officer (COO) and a Chief Information Officer (CIO). A hierarchical dependency between SMF holders is prohibited. For example, a Chief Information Security Officer (CISO) subordinated to the CIO cannot be an SMF24 holder and personal accountability for cybersecurity rests with the CIO instead. The SM&CR together with the new comprehensive ORF promote the convergence of business and technology resilience, which should result in enhanced cyber risk management practices.

80. While the SM&CR does not extend to BOE supervised FMIs, a non-objection process is in place for the appointment of key senior managers and board members. The process involves interviews and capability reviews before the appointment of key senior managers and board members. HMT is currently consulting on legislation that would formally extend the SM&CR to FMIs.

Outsourcing and Third-Party Risk

81. In recent years outsourcing and third-party risk has been on both the macroprudential and microprudential supervisory agenda. Relying on the broad rules of the PRA Fundamental Rules and the FCA Principles for Business has become less tenable in the wake of the growth of outsourcing in the U.K. financial sector, especially to the cloud.[71] On the microprudential level the PRA and the FCA took a coordinated approach to setting expectations on outsourcing and third-party risk management. Effective cooperation between the authorities resulted in specific and aligned expectations that are at the same time principles-based and technology agnostic. These expectations are aligned with the EBA Guidelines on outsourcing arrangements as well (EBA/GL/2019/02) but also include additional details in certain areas to complement the PRA's and FCA's framework on operational resilience.[72] On the macroprudential level the FPC has recognized the potential systemic risk posed by critical third-party service providers and has been closely monitoring the use of cloud services in the financial sector since 2018.[73] In 2021, the FPC noted that since the start of 2020, financial institutions "had accelerated plans to scale up their reliance on [cloud service providers (CSPs)] and in future place vital services on the cloud" and concluded that the reliance on a small number of CSPs and other critical third parties (CTPs) for vital services could increase financial stability risks in the absence of greater direct regulatory oversight of the resilience of the services they [provide]". The Bank/PRA and FCA, working with HMT, are planning to develop additional measures to manage the risks stemming from CTPs, including (i) an appropriate framework for designating certain third party service providers as 'critical'; (ii) resilience standards for CTPs in respect of any critical services they provided to U.K. firms, which should build on the

[71] According to EY's Banking Public Cloud Adoption Index survey, 27 percent of banks plan to migrate 50 percent or more of their business to the cloud in the next two years.

[72] Financial Policy Summary and Record of the Financial Policy Committee Meeting on 30 June 2021, https://www.bankofengland.co.uk/-/media/BOE/files/financial-policy-summary-and-record/2021/july-2021.pdf

[73] Cloud services are a form of outsourcing, which in turn are a specific way to use third-party technology services.

operational resilience framework; and (iii) resilience testing of CTPs building on existing testing frameworks and sector exercises developed by the U.K. financial authorities e.g. CBEST and SIMEX. These could potentially be carried out in collaboration with overseas financial regulators and other relevant U.K. authorities.[74]

As noted by FPC, The Bank /PRA and FCA, working with HMT, are planning to develop additional measures to manage the risks stemming from CTPs, including: an appropriate framework to designate certain third-party service providers as critical; resilience standards; and resilience testing. A joint Discussion Paper with detail on these proposals is planned for 2022.

82. The PRA's policy statement on outsourcing and third-party risk management (PS7/21) extends the supervisory expectations and establishes contractual requirements. Financial institutions remain ultimately accountable for all activities they outsource to a third party, which is a key principle in the U.K. regulation on outsourcing in the financial sector. From March 2022 onward, financial institutions supervised by the PRA must ensure that material outsourcing contracts meet a series of regulatory requirements, including on access, audit, and information rights; data security; and the management of sub-outsourcing risk and business continuity, contingency planning and exit strategies. The new expectations enhance third-party risk management and the ability of the supervisor to monitor systemic risk stemming from third-party service concentrations and interdependencies; especially if backed up by commensurate supervisory activity.

83. The FCA's guidance for firms outsourcing to the cloud and other third-party IT services (FG16/5) sets out largely similar expectations. Firms supervised by the FCA should comply with the risk management expectations covered in Principle 3 and SYSC 1.2.1 of the FCA's handbook. Other sources of expectations include SYSC 8 and SYSC 13 of the handbook, the Electronic Money Regulations 2011, the Payment Services Regulations 2017, the directly applicable MiFiD II Org Regulation covering organizational requirements, and the EBA Outsourcing Guidelines.

84. Banks and insurance firms are required to notify the PRA and the FCA when entering or significantly changing a material outsourcing arrangement. In addition, FMIs are required to seek approval by the BOE on outsourcing critical activities. Under the European Market Infrastructure Regulation (EMIR), Central Counterparties are required to apply to the BOE for permission to outsource critical activities linked to risk management. Under the Central Securities Depositories Regulation (CSDR), Central Securities Depositories are required to apply to the BOE for permission to outsource any core services. Both CSDR and EMIR have been retained in U.K. law after the end of the Brexit transition period.

85. Currently the U.K. authorities have no legal powers to directly supervise the cyber resilience of critical third-party services, except for critical service providers to recognized payment systems which have been brought into the regulatory perimeter. Section165A of the FSMA 2000 provides the PRA with information gathering powers regarding third-party service

[74] Financial Policy Summary and Record of the Financial Policy Committee Meeting on 23 September 2021, https://www.bankofengland.co.uk/-/media/BOE/files/financial-policy-summary-and-record/2021/october-2021.pdf

providers, but this cannot be construed as supervisory power and is subject to safeguards, criteria, and requirements specifically related to the financial stability mandate. The FCA and PRA also have information gathering powers over service providers to insurers and, in the FCA's case, FCA-regulated investment firms under Section 165 of FSMA. However, these powers do not cover all critical ICT third-party service providers (e.g., global cloud service providers) and only apply to service providers to a subset of regulated firms.

86. The authorities have focused on firm-specific and thematic reviews of existing outsourcing arrangements, as well as related risk management and assurance processes. The plans to implement a RegTech solution to collect and analyze data on outsourcing and other third-party service agreements has the potential to enhance this work as well as the ability of the authorities to identify, monitor and manage third-party concentration risks.

87. Third-party cyber risks increasingly impact the scope and threat scenarios of CBEST testing. First, third-party service providers critical for the business services in scope of a CBEST assessment are expected to be involved by the assessed firm. Soft power is used by the U.K. authorities, in absence of hard legal powers, to incentivize firms to involve these third-party service providers. Second, there is an increased focus on supply-chain cyberattack scenarios as part of a CBEST assessment. The CBEST Implementation Guide explicitly notes that "Malicious Insider and Supply Chain Scenarios are a feature of the threat landscape for many firms [and] should always be analyzed and discussed during CBEST".

88. The authorities' cyber risk management expectations have gone through a major review and as a result now are much more specific in critical areas such as operational resilience and third-party risk. The strengthened regulatory framework for third-party risk supervision is still in early stages and insights on the implementation by supervised financial institutions will only become available in 2022, after the expectations become effective. Both the PRA and the FCA are developing approaches and tools to monitor progress and detect potential issues.

Recommendations

89. The authorities should continue reviewing cyber risk, and more broadly, technology risk management expectations with the aim to publish more specific guidance. Currently, expectations are too often implicit in high-level rules[75] and interpretation and implementation challenges exist. Regulators should also consider additional soft guidance, e.g., speeches and letters, to support cyber risk mitigation and resilience objectives.

90. The Bank/PRA and FCA should seek additional statutory powers to assess the resilience (including cyber resilience) of any critical services that third party service providers provide to regulated financial institutions, as recently suggested by the Bank of England Financial Policy Committee (FPC). This should include the ability to commission skilled persons

[75] Notable exceptions are the CBEST requirements and the policy statement on outsourcing and third-party risk management.

reviews. Currently, firms are incentivized to require adequate cyber risk management in the supply chain by the principle of the ultimate responsibility for any outsourced activity residing with the firm, and supervisory soft power. Like most jurisdictions at present, the PRA does not have express statutory authority to directly review or examine any critical services that cloud, and other third-party service providers provide to regulated firms, unless these firms' contracts with these service providers authorize such regulatory access (the PRA and FCA require firms to include clauses granting regulatory access in their contracts with cloud providers and other 'material' third party service providers). However, a more direct approach is advisable, because of the high levels of cyber risk stemming from the supply chain, the ongoing growth of outsourcing, and service provider market consolidation that leads to a lack of substitutability and the emergence of systemically important service providers. [76] In addition, while service agreements often include audit clauses, the supervisor can find it difficult or impossible to delve deeper into certain areas of concern at third parties without explicit statutory power. To avoid the risk of supervisory overreach, statutory powers should be limited to the services relevant to the Bank/PRA's and FCA's statutory objectives. As noted by FPC, The Bank /PRA and FCA, working with HMT, are planning to develop additional measures to manage the risks stemming from CTPs, including: an appropriate framework to designate certain third-party service providers as critical; resilience standards; and resilience testing. A joint Discussion Paper with detail on these proposals is planned for 2022.

91. The Senior Managers and Certification Regime should be extended to BOE supervised FMIs as currently being consulted on by HMT. This would further strengthen the accountability with respect to operational and cyber resilience, governance, and culture at FMIs and would result in a better aligned regime across all BOE, PRA and FCA supervised entities. [77]

92. Macro-level expectations regarding operational and cyber resilience should be considered to support financial stability and guide individual institutions. Progress could be made in not just expecting firms to set their impact tolerances but imposing upper limits in case of extreme but plausible scenarios affecting important services, as well as specific requirements for recovery testing. Proportionality could be implemented based on the existing firm categorization system. More specific supervisory expectations can also help financial institutions in contract negotiations with critical technology service providers and would support BOE's Future of Finance project goal of a safe and controlled cloud migration.

93. Firms would benefit from aligned cyber risk reporting processes and templates, including for reporting cyber incidents and material outsourcing arrangements. The absence of reporting templates typically results in less reliable and/or comprehensive records, which in turn impacts the effectiveness of the risk-based approach. Templates and report processing that are not

[76] Three large cloud service providers dominate the market, and their combined global market share has increased from 49.5 percent in Q1 2018 to 58 percent in Q1 2021. (Source: Statista, 2021) Meanwhile, a significant uptake of cloud services can be expected in the banking sector.

[77] The mission notes that the authorities have been preliminarily contemplating measures to this end.

aligned across authorities for reporting the same events, complicate internal processes at firms and may result in inconsistencies.

D. Supervisory Practices

94. The U.K. regulators have established mature, risk-based, and proportional supervisory processes. Three guiding principles drive the supervisory processes: (i) judgement is critical in decision making; (ii) supervisors aim to be forward looking and assess firms not just against current risks but also against plausible risk further ahead; and (iii) supervisors focus on issues that most likely pose the greatest threat to the objectives of their supervisory authority. Firms are classified in importance categories to reflect their potential impact on the objectives of a supervisory authority (e.g., financial stability) should they become distressed, allowing for a high degree of proportionality.

95. The U.K. regulators' cyber risk supervisory approach focuses on three key areas with to ensure the financial sector effectively mitigates the impact of operational disruptions while continuing to perform its critical activities. The key areas of focus are: (i) proactive supervisory interventions to mitigate firm-specific cyber risk; (ii) systemic cyber risk assessment and mitigation through sector level assessments and exercises; and (iii) industry collaboration to develop and disseminate good cybersecurity practices.

96. The risk-based approach to supervision is facilitated by holistic and formalized risk assessment models, to which cyber risk is an input. Risks are assessed with a view on potential systemic impact, considering operational, financial, and structural mitigants. While the details differ at the PRA and FCA, both approaches seek to determine residual risk, emphasize qualitative assessment and expert judgment over mechanistic scoring. To ensure consistency, assessments are peer reviewed and go through several levels of management review before finalization.

97. Regulators focus on ensuring firms develop appropriate capabilities within the three lines of defense to monitor and manage firm-specific cyber risk. Regulators review the functioning and reporting of senior managers (i.e., control owners); the appropriateness of the challenge provided by the risk function; and the strength of the assurance provided by internal audit, including the follow-up of remediation plans. The regulators may consider the work of external auditors as well.

98. Key elements of cyber risk supervision are supervisory engagement, thematic reviews, self-assessment, and testing. All elements are mature and are performed in a planned, controlled, and documented fashion. (The next sections provide further details.)

99. Supervisory activities are almost exclusively desk based, with little to no first-hand evidence gathering on the effectiveness of cybersecurity control measures beyond CBEST. Referred to as on-site examinations or reviews, these activities are often key elements of the supervisory process in jurisdictions with similarly complex and advanced financial sectors because of the higher level of assurance they can convey.

Supervisory Engagement

100. Supervisors meet bilaterally with SMF24 function holders of systemically important firms twice a year.[78] In these meetings supervisors discuss different aspects of the design of operational and cyber resilience control measures, business continuity and contingency plans, and information security strategies. These meetings are frequently used to review progress against remediation plans and to convey feedback and supervisory expectations regarding cyber resilience measures.

101. The Periodic Summary Meeting (PSM) sets the supervisory agenda and work program for the coming year, including cyber risk matters. PSMs are annual reviews of a firm's key and potential key risks, which may result in an additional assessment and more detailed investigation of the risk. Furthermore, the meeting could be used to identify the most suitable risk mitigating action. Annual PSMs could be complemented with Mid-Point Reviews (MPR).

102. Firm-specific supervisory findings and recommendations are communicated via formal letters and CBEST final remediation plan documents. A PSM feedback letter is generally used to communicate the key messages from the PRA supervisory team as well as the corrective measures (if any) that the PRA expect the firm to implement in the context of findings. Similarly, the FCA communicates its finding via a letter to the firm with an accompanying risk mitigation plan, which describes the individual findings, the mitigation steps, and the timeline for completion. The findings in the risk mitigation plans are not given risk rankings. As part of the CBEST process the supervisors agree with firms a final remediation plan document which outlines prioritization, ownership, and timing of the expected remediations. Finally, sector-wide thematic findings are shared by the PRA and FCA with all their supervisees or through a regulatory digest communication.

103. Supervisory findings and recommendations are followed-up as part of the continuous assessment process. In exceptional cases, such as repeat findings or unsatisfactory remediation, a skilled person report could be required, and/or a formal investigation could be launched, which in turn could lead to enforcement action.

Thematic Reviews

104. Cyber and operational resilience focused thematic reviews are used to assess emerging risks and identify prevailing industry practices (e.g., to understand the impact of COVID-19). These reviews target specific cybersecurity topics with the goal to make firms aware of potential common vulnerabilities identified by supervisors and help them with mitigation. Both IBD and FMID have conducted thematic reviews to understand the impact of COVID-19 on the cybersecurity posture and the resilience of daily operations of financial institutions (including working from home arrangements). Collaboration with the NCSC is sought to obtain additional expertise and guidance, including identification of best practices.

[78] Or the equivalent (e.g., COO, CIO, or CTO) function for FMIs for which the senior management certification regime is not applicable.

105. Cyber themes emerging from the CBEST and CQUEST assessments are periodically shared with all PRA and FCA regulated firms, and FMID regulated FMIs. Given the sensitivity of the information, these documents are not published. However, to increase transparency, the FCA published two cyber insights documents that do not contain sensitive information, sharing the practices and experiences of the Cyber Coordination Groups (CCG) attendees.[79]

106. The thematic review process is being redesigned to increase the completeness, coordination, and timeliness of the reporting. The aim is to implement annual regular and standardized thematic reporting. This entails increasing the number of data points recorded, aligning the PRA and FCA methodologies, and standardizing production and communication.

107. FMID analyses cyber risk exposures from an operational as well as a clearing perspective. In case the IT infrastructure of a participant is compromised, FMID actively monitors the central counterparties (CCPs) exposures to it.

Self-Assessment

108. A cyber resilience self-assessment questionnaire (CQUEST) is used to collect information on, and analyze, firms' practices and maturity levels. Returns are the basis, among others, of cross-sectoral and temporal analyses and help steer supervisory engagement. CQUEST is based on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF is widely regarded as capturing the best practice in cyber risk management and cyber resilience. CQUEST consists of 48 multiple-choice questions structured along the NIST CSF functions of Identify, Protect, Detect, Respond, and Recover. CQUEST also incorporates an additional domain focusing on Governance/Leadership and expectations of Board/Senior Execs in relation to cyber. CQUEST is much simplified compared to the NIST CSF, which in turn is a high-level outcome-centric framework. While it provides useful information, CQUEST is a "light-touch" supervisory tool because there is no requirement to substantiate the self-assessment with evidence, unless supervisors detect inconsistencies, over-confidence, or other discrepancies later.

109. The authorities have process in place to ensure the consistency and relevance over time of CQUEST. The questionnaire is subject to an 18-months review cycle (24-months for FMIs) so it can keep pace with the changing threat landscape and the PRA and FCA coordinate assessments and share reports for dually supervised firms.

Testing

110. The authorities have pioneered and implemented a comprehensive testing regime that strongly supports the supervisory objectives of all authorities. The elements of the regime are the CBEST testing program, the cyber stress tests, and the industry crisis exercises.

[79] Cyber Coordination Groups (CCGs) are convened by the FCA since 2017 to help firms share knowledge and discuss good cybersecurity practices.

Threat Intelligence-led Penetration Testing (CBEST)

111. To assess the effectiveness of their internal control system and cyber resilience, systemic firms are subjected to the CBEST penetration testing program. CBEST is an intelligence-led penetration testing exercise that aims to assess firms' preventive cybersecurity controls, as well as their ability to detect and respond to a range of external and internal attackers.[80] CBEST also includes a threat intelligence capability assessment. CBEST tests are conducted against live production systems and cover the end-to-end processes supporting the business services agreed in scope. To closely mimic real-world threats and attack vectors, the framework prescribes a penetration test on the firm's live production systems by accredited threat intelligence and penetration testing organizations. CBEST provides very useful outcomes for the supervisees, including a threat intelligence assessment, a description of relevant threat scenarios, the penetration testing report, a capabilities assessment, and a remediation plan.

112. CBEST testing is the most effective supervisory tool for assessing and strengthening cyber resilience, but it comes at a high price. There is broad consensus among participants on its significant value, but the breadth, complexity, length, and cost make it unsuitable for all but the largest firms and FMIs.

113. While a three-year cycle is the norm for CBEST testing, a retest could be required to verify and validate the effectiveness of remediation actions or to assess resilience against new emerging threats. Also, supervisors include the follow-up on findings in the continuous assessment process, which results in earlier assurance on remediation than the next round of test.

114. Risks related to CBEST testing activities are directly managed as part of the assessment. Testing boundaries for critical scenarios, such as denial of service attacks and ransomware, are defined case by case, without triggering actions that could impact live services. Non-intrusive alternatives, such as security configuration reviews, remain unexplored in CBEST.

115. The availability of high quality and innovative threat intelligence and penetration testing services is crucial to the CBEST program. The assessment is dependent on the attack vectors employed, and the expertise, and often preferences, of testers, which means that the attack surface is only partially covered. Procedures like a controlled leg-up can mitigate this risk to an extent. In contrast to the experience of regulatory authorities in other jurisdictions, the U.K. authorities are of the opinion that there is a sufficient supply of accredited threat intelligence and penetration testing services.

116. The PRA accreditation scheme and the underlying independent certification underpin the quality of the CBEST program, but information leaks pose a risk. CBEST penetration testers

[80] "Penetration test" means that the effectiveness of cyber defenses is tested with actual hacker methods, for example exploiting vulnerabilities, planting backdoors, phishing, circumventing access controls to access sensitive information, and so on. "Threat intelligence-led" means that the attack scenarios are developed based on credible information about current and emerging cyberattack tactics, techniques, and procedures (TTPs). Typically, penetration testing providers and threat intelligence providers are different. Threat intelligence may be provided by specialist arms of national security agencies as well.

and threat intelligence providers must be accredited by the PRA, which entails: (i) membership and accreditation of the Council of Registered Ethical Security Testers (CREST), an independent non-profit organization focusing on examining and certifying relevant capabilities; (ii) meeting significant minimum experience levels, including work in the financial sector; and (iii) references from institutions. It is especially important to maintain and verify these requirements, as the CREST certification provides a baseline only, and the integrity of the examinations might have been impacted by information leaks.[81]

117. The PRA works to further improve an already effective penetration testing regime. In 2020 a new CBEST implementation guide was published which addresses among others, cross-jurisdictional assessments, risk management and planning, and enhanced execution requirements. In addition, the PRA reviewed the CBEST templates and improved the reporting guidelines. The authority also announced an increased attention on malicious insider and supply chain attack scenarios, which have become hot topics globally. In addition, they recently began a pilot of STAR-FS, a lighter weight threat-intelligence led penetration test. STAR-FS is intended for a wider set of financial institutions and maintains the same level of regulatory assurance and technical rigor as CBEST. Furthermore, STAR-FS is suitable to increase the frequency of penetration testing at firms that are already subjected to CBEST. Supervisory involvement in STAR-FS is going to be scaled back, but the scope, findings, and remediations plans will be reviewed. On the international stage, the recent focus in developing CBEST has been on cross-jurisdictional assessments.

Cyber Stress Testing

118. Cyber stress testing picks up where CBEST leaves off. The macroprudential counterpart of CBEST is the cyber stress test mandated by the FPC to determine firms' ability to withstand cyber incidents of a magnitude that can cause material economic harm, that is, severe but plausible cyberattacks with potential systemic impact. This means a greater tolerance for disruption than in the CBEST scenarios. Cyber stress tests are intended for the largest firm and so far, only a subset of the systemically important institutions have participated. The first round of tests was done in 2019 as a pilot with voluntary participation. Due to the COVID-19 pandemic, tests planned for 2020–2021 were postponed. At the time of the review planning work was underway for a stress test in 2022.

119. A key scenario of the stress test is disruption of payments. In the event of a cyber incident the FPC expects the financial system to honor critical payment obligations by the end of the value date. This is consistent with the CPMI-IOSCO requirement to complete settlement by the end of the day the disruption occurred. Notably though, there is a CPMI-IOSCO requirement of a two-hour recovery time, which is stricter. The argument in favor of the end of value date limit is that there can be instances, where recovering too early could have a worse impact on financial stability than failing to meet the two-hour objective. Indeed, insufficient threat elimination or difficult to detect data integrity attacks are such instances. The risk of premature resumption stands for the end of value date objective too. The FPC concluded that firms need to be able to identify such

[81] Reportedly, CREST training material and certification exam notes that appear to belong to a CBEST accredited vendor have been leaked to the internet in 2020.

circumstances at the earliest possible stage of an incident. The stress test would be used to address this point, and others, in the context of a compromised data integrity scenario.

120. Currently, cyber stress tests do not include impact calculations on capital and liquidity buffers and financial stress tests do not include cyber incident-based scenarios. Stresses caused by cyber incidents are difficult to model and quantify. Compounding the difficulty, scarcity of data makes the outcome less reliable. Irrespective of the type of the stress test, this is a research area worth considering and there are early examples of cyber stress tests that include capital impact calculations.

Sector Crisis Exercise

121. The goal of the sector crisis exercise is to rehearse the collective response of the financial sector to major operational disruption. The attack scenarios are quite like the cyber stress tests, but the focus is on collective response capacity. The exercise aims to: (i) test the effectiveness of decision-making and crisis communication arrangements; (ii) validate collective contingencies; (ii) enable participants to practice their response protocols; and (iv) to improve the sector-level response coordination with other jurisdictions.

122. The governance and the support infrastructure of the exercise are proportional to the complexity and magnitude of the undertaking. Effective delivery of the exercise involving dozens of participating firms and hundreds of their experts is the responsibility of the Sector Exercising Group (SEG), which is a substructure of the Cross Market Operational Resilience Group (CMORG). The SEG represents FMIs, investment firms, retail firms, and authorities. The CMORG Project Management Office provides operational support. An online simulation platform has been used to support the exercise, featuring secure communication facilities, and simulated traditional and social media feeds.

123. The exercise is collaborative, with voluntary participation, and no pass/fail type assessment. This is in line with the prevailing international practice. There is a growing interest in participation, which indicates the value added. In 2018 the exercise allowed the authorities to test the sector's response ahead of the G7 cross-border cyber incident coordination exercise.

Incident Reporting

124. The cyber incident notification guidelines leave the firms to decide when to notify the authorities of an event, which results in reporting inconsistencies. Systemic banks and insurance firms are expected to report cyber incidents under the PRA's and FCA's general notification requirements as soon as practically possible. Currently, there is no published and specific framework, rule, or guidance on reporting cyber incidents, leaving firms to develop their own internal processes and reporting strategies. Inconsistencies in reporting processes between firms were observed and resulted in reclassifications of (reported) incidents. Implicit expectations of the FCA appear to be stronger, resulting in broader reporting.

125. United Kingdom DT's cyber trend reporting processes is heavily based on professional judgement, which could impact information flow. Professional judgement is key in determining the need as well as the appropriate level for escalation of a reported incident, which makes the process highly dependent on the experience and capabilities of a limited set of individuals. Similarly, information on cyber incidents is currently not collated and fed into risk summary and trend reports but shared with ORRD as deemed necessary (i.e., based on professional judgement).

126. FCA leverages the incident data maintained on the central record to identify trends and inform supervisory strategies. A team within the Technology Resilience and Cyber department (TRC) is responsible for a structured process for managing and recording cyber incidents, which is informed by an FCA-wide harm taxonomy to measure the severity and impact of the incident (i.e., harm to the firm itself, to its customers and to the stability of the market). This process includes collecting post incident reports to ensure that root causes for the incident are recorded, as well as a wide variety of information including details on compromised third parties (if any) and data breach details (if applicable). This information is fed into several internal dashboards.

127. The U.K. Financial Services Cyber Incident Response Framework provides firms with guidance on incident reporting and expected response across government, regulators, and law enforcement. The framework provides regulatory affairs and compliance teams with guidance on handling U.K. regulator interactions and mandatory reporting requirements, including the financial services authorities, the Information Commissioner's Office (ICO), the National Cyber Crime Unite (NCCU) of the National Crime Agency and the Police's National Fraud Intelligence Bureau (NFIB). Furthermore, the framework elaborates on the NCSC incident thresholds and classification structure. Finally, it provides incident management and response teams with best practices on information sharing and coordination.

Response Framework

128. The Authorities' Response Framework (ARF) is used as a single mechanism to coordinate their response to cyber threats and incidents. ARF invocation is by consensus among all financial authorities, although any one authority can organize a call to discuss invocation. Given their strong relationship and ongoing cooperation in cyber matters, reaching consensus has been fast. Wider government may also be included in the response, depending on the severity of the incident. There is a defined incident severity categorization system in place. Once the ARF is invoked, an agreed upon Lead Financial Authority assumes responsibility for information sharing and coordination. For significant cyber incident the NCSC provide technical advice. The lack of formally documented rules on which authority leads in which type of incident does not seem to hinder agreement on the basis that there are agreed principles for decision-making on which authorities leads the ARF (e.g., consumer detriment (FCA), safety and soundness or financial stability (Bank), economic or societal harm or a risk to public finances (HMT)).

129. The authorities always maintain the ARF to remain effective. The ARF is owned by HMT but is jointly maintained by all financial authorities, based on an annual performance review, in which the NCSC also participates.

130. Coordination and information sharing protocols between financial institutions, FMIs, industry groups and the authorities are set out in the Sector Response Framework (SRF). The SRF supports collaborative engagement between firms and financial authorities in case of critical incidents. The criteria for classifying an incident are clearly set out in the Industry Incident Lexicon within the SRF.

131. The SRF architecture is complex both because of the large number of participating entities and their complex interrelationships, which may have an adverse impact on response agility. There are over ten organizations or cooperation mechanisms on the SRF map that are involved in some capacity in information sharing and response, not counting international organizations and individual firms. Key among these is the information sharing groups at the sub-sector level (i.e., retail and wholesale), the Finance Sector Cyber Collaboration Centre (FSCCC), the CMBCG, U.K. Finance's Incident Communication Group (ICG), the NCSC, and of course the ARF members. The CMBCG is pivotal to the SRF as a strategic coordination and decision-making group. The ICG also plays a strategic role in coordinating external communications with the CMBCG.

Resources

132. The PRA and FCA work on upskilling generalist supervisors in cyber risk to reduce pressure on cyber risk specialists. The objective is to pull cyber knowledge into the generalist supervision teams for systemic banks and insurance firms. This should enable a reinforcement of the teams' ability to make professional judgements related to cyber risks and more selectively request involvement from the cyber risk specialists.

133. The skilled person reports provide a tool to externally acquire highly specialized cyber expertise. A skilled person review can be commissioned for the following purposes: to identify, measure and address risks; to monitor the development of identified risks; to limit or reduce the impact or likelihood of identified risks; and to define and implement adequate responses for materialized risks. In 2020, three Lot J—Technology and Information Management reports were completed across banking and insurance, which suggests a limited use of the tool.

134. The FMID is appropriately resourced and has access to independent expertise. The Bank of England has established a team of more than 50 supervisors for 10 FMIs and a critical service provider, which is composed of supervisors with a general risk expert profile and cyber/IT experts. Access to subject matter experts at the PRA has been formalized and is used for periodic supervisory assessments and CBEST exercises.

Coordination and Cooperation

135. Procedures for coordination, information sharing, and collaborative supervisory activities between the PRA and the FCA are detailed in a Memorandum of Understanding.

136. Generally, supervised institutions tend to actively collaborate with supervisory authorities in the context of technology and cybersecurity risk. This mirrors the more collaborative stance on cybersecurity issues between institutions.

137. The authorities actively participate and have key roles in international cyber resilience guidance development. In 2016, the G7 formed a Cyber Expert Group (CEG), co-chaired by the U.S. Department of the Treasury and the Bank of England. HMT and the FCA are also members, alongside other financial authorities across the G7. Since its creation, the CEG has developed several public documents, including Fundamental Elements for Cybersecurity; Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector; Fundamental Elements for Third Party Risk Management; and Fundamental Elements for Threat Led Penetration Testing. In addition, the CEG has developed a Cyber Incident Response Protocol (CIRP) to improve coordination in the event of a cyber incident with cross-border implications for G7 countries. The Bank of England's supervisory and policy teams participate and contribute to international committees and working groups hosted by the Financial Stability Board (FSB) and the Bank for International Settlements (BIS), which includes the Committee on Payment and Market Infrastructures (CPMI) and the Basel Committee for Banking Supervision (BCBS).

138. Collaboration with other relevant international supervisory authorities on CBEST is actively considered, and recognition of other threat intelligence-led penetration testing regimes is possible if minimum requirements have been met. Specifically, the PRA and FCA have been collaborating with the ECB to ensure alignment between the CBEST and TIBER-EU frameworks. The first pilots were completed in 2020 for collaboration with other European authorities as well. Supervisory authorities of the United States and several Asian jurisdictions have acted as observers in CBEST exercises. Collaboration and recognition of other threat intelligence-led penetration testing programs is crucial in reducing the burden for firms and supervisors alike.

139. International cooperation and supervisory coordination form integral parts of the BOE's supervisory approach for FMIs that are systemically important for more than one jurisdiction. The BOE has concluded Memorandums of Understanding with a wide range of authorities in international jurisdictions, organizes colleges for each of its CCPs and participates in international oversight forums. A context of participation and mutual recognition of supervisory threat-intelligence led cyber testing has been established, i.e., authorities from international jurisdictions have been involved in CBEST testing and the Bank of England has participated in other international cyber testing.

Enforcement

140. The FSMA 2000 provides the PRA and FCA with appropriate powers to take enforcement, criminal or civil action against regulated and non-regulated firms and individuals who are failing or have failed to meet the standards. Examples of possible enforcement actions include: (i) prohibiting an individual from performing functions in relation to regulated activities and withdrawing approvals; (ii) suspending a firm for up to 12 months from undertaking specific regulated activities; (iii) suspending an individual for up to two years from undertaking specific controlled functions; (iv) censuring firms and individuals through public statements; and (v) imposing financial penalties on firms and individuals. In the past three years the PRA has not imposed penalties related to non-compliance with cyber risk related regulations while the FCA has fined one firm.

Recommendations

141. Supervisors should conduct additional cybersecurity control effectiveness verification activities to complement desk-based analytical work, supervisory engagement, and CBEST testing. These on-site examination activities provide value in at least three areas: (i) independent verification of information provided during supervisory engagements; (ii) as a result, encouraging candor in providing accurate cyber risk related information; and (iii) developing in-depth knowledge on the way supervised firms are organized and operated (including the corporate culture).

142. U.K. authorities should further strengthen their operational and cyber resilience supervisory teams. There is a strain on specialized cyber expertise and the expected increase in cyber risk regulatory and supervisory work compounds the problem. While upskilling non-specialist supervisors is useful, there are limitations to what it can achieve.

143. The authorities should consider additional opportunities to strengthen the penetration testing framework. These include:

(i) Internal threat intelligence and/or testing capabilities of firms, subject to meeting CBEST accreditation criteria, could be leveraged to reduce costs. Allowing firms to use their internal capabilities could also stimulate the adoption of testing regimes like STAR-FS.

(ii) Grey box testing and purple teaming,[82] which would bring additional learning opportunities for CBEST participants. While grey-box testing would less closely mimic a real cyber-attack, it would allow for more comprehensive testing within the time limits. Purple teaming could improve the benefits of the exercise by providing the detection and response teams with deeper insights in faster feedback cycles.

(iii) A generic threat intelligence report for smaller firms, which could assist in further broadening participation in threat intelligence led testing,[83] effectively supporting the authorities' objective to include a wider set of financial institutions while maintaining adequate regulatory assurance and technical rigor.

(iv) Security reviews of key protections against vulnerabilities that cannot be included in the penetration testing of live production systems. Examples include denial of service attacks, ransomware attacks, and data integrity attacks. The prevalence of these attack categories has been growing and pose a significant risk. Penetration testing cannot be used in these risk scenarios, but configuration reviews, for example, of network perimeter defenses, traffic scrubbing, anti-malware

[82] Grey box testing is an approach in which testers are given some information on the target environment, for example of a such nature and extent that a persistent and well-resourced attacker can reasonably obtain. Purple teaming means that the testers and the defenders regularly meet and exchange information during the test.

[83] Supervised entities have indicated firm-specific threat intelligence analyses are costly and often cover broadly applicable attack vectors internal teams have already identified. Generic threat intelligence analyses have proven to be valuable in other jurisdictions and could significantly reduce the cost for individual firms.

systems, or data integrity protection systems would add valuable assurance on the effectiveness of relevant mitigations. In addition, this would facilitate purple teaming.

(v) Finally, the red team could be allowed greater freedom to develop a cyberattack that has not yet been observed and set out in a scenario. [84]

144. The CQUEST cybersecurity questionnaire could be usefully augmented with requiring that firms provide evidence to support the self-assessment. Currently, ascertaining the accuracy of the self-assessment is quite difficult; and besides some internal consistency checks there are no steps made in this regard (by design). However, requiring the attachment of supportive documentation to the answers implying higher maturity would convey stronger assurance over CQUEST results.

145. Prioritize developing the proposed cyber resilience maturity assessment framework of the core assurance framework to gain better insight in the cyber resilience posture of the supervised FMIs, and to communicate the supervisory expectations according to defined maturity levels. When fully developed, the proposed maturity assessment framework—aligned with international standards—will provide a convenient structure, defined maturity levels and linked indicators to support better insights obtained from supervisory engagement, inspections, and operational control effectiveness assessments. The maturity assessment could further clarify the supervisory expectations regarding the operationalization of the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures and provide a meaningful basis for further improvements of the cyber resilience posture.

146. The usefulness of cyber stress testing could be greatly improved with quantifying the impact on liquidity and capital buffers. Risk to the broader economy caused by systemic cyber events is primarily transmitted through liquidity shortfalls (in the short term) and deterioration of capital positions (in the longer term). Therefore, ways of including liquidity and capital impact calculations in the cyber stress tests should be researched. Alternatively, such calculations could be done in the financial stress test, based on severe but plausible cyber incident scenarios.

147. Broad international representation and key functions in standard setting bodies could be further leveraged to promote internationally better aligned supervisory expectations and tools. The international financial system, including some of the globally largest firms supervised by U.K. regulators, would greatly benefit from better alignment of regulatory and supervisory expectations across jurisdictions. An incoherent set of cybersecurity guidance might negatively impact the U.K. regulators' objectives as well. Furthermore, conflicting, redundant, or confusing approaches (including questionnaires and intelligence-led testing) could result in unnecessary duplication of effort. This duplication may drain resources available at supervised firms from actual cybersecurity enhancing activities.

[84] Industry participants reported recurring of attack vectors across different tests, like phishing, which is already well understood and tested internally. In addition, more resourceful cyber attackers do not necessarily follow scenarios developed by threat intelligence providers.

ONGOING REVIEW OF THE FUTURE OF THE REGULATORY FRAMEWORK: SOME OBSERVATIONS

A. Executive Summary and Key Recommendations[85]

148. The U.K. government launched in 2020 a Financial Services Future Regulatory Review (FRF review) setting out proposals for redesigning the regulatory framework within which the financial services regulators operate. Under the proposals, U.K. financial regulators' rule-making powers will be significantly expanded to areas previously covered by retained EU law so that regulatory and supervisory requirements that apply to firms will be set out in rules rather than in the current mix of legislation and rules, while being subject to enhanced accountability and other arrangements. While the onshoring of EU legislation was an immediate response after EU exit, it was not designed to provide the long-term approach to regulating financial services.

149. There are clear benefits to delegating responsibility to the regulators for setting regulatory requirements that are often technical and complex. The process of repealing relevant retained EU law and concurrently replacing it with regulators' new rules will maintain continuity of regulatory requirements and going forward would provide more flexibility for the financial regulators to update standards to respond to emerging risks. Several other proposals move in the right direction (i.e., granting the Bank of England (BOE) a general rulemaking power in relation to central counterparties (CCPs) and central securities depositories (CSDs), introduction of a new Designated Activities Regime (DAR).

150. Proposed accountability and other measures could constrain U.K. financial regulators' ability to discharge their new rulemaking responsibilities. For the most part, proposed changes may substantially change intergovernmental relationships. Taken in totality, measures simplifying the rulebook, delegating rulemaking, and expanding the regulatory remit to new activities are initiatives the IMF sees as beneficial in maintaining or strengthening the United Kingdom's approach to regulation and supervision. Other proposed transparency and accountability oversight measures, which could lengthen the procedures for adopting regulations or require post adoption review processes will need to be designed and implemented carefully, to ensure the FCA and PRA maintain their focus on their primary objectives and can retain their operational independence as well as their ability to act in a timely manner (see Table 3).

[85] This chapter was prepared by Luc Riedweg and Peter Windsor (both IMF), and Thomas Curry (IMF Expert).

Table 3. United Kingdom: Main Recommendations		
Recommendation	**Priority**	**Timeline**
1. *Preserve* the primacy of PRA and FCA's objectives of safety and soundness and market integrity in principle and in practice over any secondary objectives and ad hoc policy priorities	High	NT
2. *Ensure* that the final accountability and transparency mechanisms adopted under the FRF review safeguard regulatory independence and pose no constraints for operational and oversight effectiveness	High	NT
NT = Near Term (now to one year); MT = Medium Term (within 1 to 3 years)		

B. Financial Services Future Regulatory Framework Review

151. The Internal Monetary Fund is generally agnostic about supervisory architecture and institutional arrangements. There is no clearly superior model. However, effective supervision is predicated on certain foundational conditions and attributes being in place which include independence, accountability, credibility, adequate resources, and strong regulatory capacity. The primary focus should be squarely placed on safety and soundness and ensuring that financial markets function well. The legislative framework supporting the supervisory authority is particularly important. As emphasized by the IMF, regulatory and supervisory independence increase the efficiency and effectiveness of regulation and help markets operate more smoothly and efficiently. Conversely, political pressures and industry interference not only weaken financial regulation generally, but they also hinder regulators and the supervisors who enforce the regulations from taking timely and appropriate action.[86]

152. The operational independence of financial regulators is a key feature of the U.K. financial services regulation. U.K. financial regulators have separate and independent mandates, set out in statute, reflecting the United Kingdom's 'Twin Peaks' model. The PRA and the FCA have responsibility for the supervision of a wide range of firms, the PRA for prudential matters and the FCA for conduct matters. The FCA is also the prudential regulator for all firms that are not dual-regulated firms (i.e., those that are not authorized by the PRA and regulated by both the PRA and the FCA).[87] In the United Kingdom, Parliament establishes the legislative parameters within which HM Treasury (HMT) sets the regulatory perimeter' through secondary legislation, specifying which financial activities should be regulated. The PRA has been given a general objective to promote the safety and soundness of PRA-regulated firms and an appropriate degree of protection for current and prospective policyholders, and a secondary objective to facilitate effective competition. The FCA has a strategic objective of ensuring the relevant markets function well. There are three operational objectives in place to support this strategic objective (protection for consumers; protecting and enhancing the integrity of the U.K. financial system; and effective competition in the interests of consumers). The PRA and FCA are operationally independent, and HMT cannot require the

[86] See IMF Paper "*Should Financial Sector Regulators be Independent?*," 2004.

[87] The PRA regulates around 1,500 banks and major investment firms, as well as building societies, credit unions, and insurers. The FCA is the regulator for nearly 60,000 firms in total, the vast majority of which are solo-regulated firms.

regulators to take specific actions—with a few limited exceptions where it may direct the two agencies.

153. While the onshoring of EU legislation was an immediate response after EU exit, it was not designed to provide the long-term approach to regulating financial services. The European Union (Withdrawal) Act 2018 converted applicable EU legislation, including EU prudential rules for banks and insurers into U.K. law. As a result, prudential requirements that apply to regulated firms are currently mainly set out in retained EU law. At the end of the transition period, the United Kingdom is left with a relatively complex regulatory framework. The prudential regime is governed by piecemeal legal provisions and combines primary legislation, a range of statutory instruments, on-shored binding technical standards, and PRA and FCA rules and guidance, which makes it difficult for firms to navigate. The U.K. authorities have always made clear that the onshoring was transitional as the intention is not to keep detailed regulatory provisions in law.

154. In October 2020, HMT launched a consultation on the Financial Services Future Regulatory Framework Review (FRF Review) setting out proposals for redesigning the regulatory framework within which the financial services regulators operate. The main objective is to determine how the financial services regulatory framework should adapt to the United Kingdom's new position outside of the EU. As part of this, it is proposed to "move back to a more British style of regulation, with the rules made by regulators rather than set out in law"[88] in accordance with the Financial Services Markets Act 2000 (FSMA) model, which sets out the current framework for financial services regulation and empowers the PRA and the FCA to make rules in certain specified areas. Under the proposal, U.K. financial regulators' rule making powers would be expanded so that the regulatory and supervisory requirements currently set in retained EU law that apply to firms will all be set out in rules, while being subject to enhanced accountability arrangements. After a first consultation in October 2020, HMT has published for consultation a second package of detailed proposed measures.[89] Key proposals include:

- *Division of responsibilities*. The U.K. government and Parliament will continue to set the overall framework while U.K. financial regulators will be responsible for designing and implementing the direct requirements that apply to firms which are currently set out in retained EU law. As a result, the vast majority of the prudential and conduct requirements regime would be implemented in PRA and FCA rules. The Financial Services Act of 2021 is consistent with the proposed FRF Review approach in that rule making powers to implement Basel 3 standards are delegated to the PRA within a policy framework set out in the law. If the revised division of responsibilities was already in place, issues identified with the Solvency II Review and PRA independence in the Detailed Assessment Report on Observance of the ICPs would have been mitigated.

- *New regulatory objectives*. HMT's second consultation proposes to introduce new statutory secondary objectives for the FCA and PRA in addition to their primary objectives to facilitate the

[88] "Strong and simple", speech delivered by Sam Wood, deputy-governor, Mansion House, November 2020.

[89] HMT, Financial Services Future Regulatory Framework Review, Phase II Consultation. October 2020 and HMT, Financial Services Future Regulatory Framework Review: Proposals for Reform, November 2021.

long-term growth and international competitiveness of the United Kingdom economy subject to alignment with international standards.

- *Principles, have regards, and obligations.* It is also proposed to amend the existing regulatory principles to clarify that growth should occur in a sustainable way that is consistent with the government's commitment to achieve a net zero economy by 2050. HMT would also have the ability to apply additional ''have regards" considerations and to place obligations on the regulators to make rules in relation to specific areas of regulation.

- *Accountability to Parliament and HMT*. Additional Parliamentary oversight mechanisms are not recommended although existing informal mechanisms would be formalized. Engagement mechanisms that exist between HMT and the regulators would be strengthened: U.K. financial regulators would be required to respond to HMT recommendation letters and review their existing rules under unspecified circumstances that the government considers it is in the "public interest".

- *The Production of Cost-Benefit Analysis*. U.K. financial regulators would be required to publish a framework for conducting cost benefit analysis (CBA), and establish a new independent statutory panel dedicated to supporting the development of the regulators' CBAs.

- *Other important aspects* include granting the Bank of England (BOE) rulemaking power in relation to central counterparties (CCPs) and central securities depositories (CSDs) and introducing of a new Designated Activities Regime (DAR).

155. Responses to HMT consultation and parliamentary hearings illustrate a range of views in the United Kingdom.

- Unsurprisingly, some respondents from the private sector argued for more scrutiny and accountability of the regulators' supervision and a mechanism to challenge supervisory decisions. Industry respondents also made a number of proposals around independent scrutiny of the regulators.

- U.K. financial regulators have welcomed the proposed delegation by Parliament of responsibility for promulgating regulatory requirements for firms. More cautious views were expressed concerning the proliferation of regulatory objectives[90] and enhanced accountability and scrutiny mechanisms.[91]

[90] Senior Bank policymakers have previously set out the benefits of a regulatory framework in which the high-level objectives, responsibilities and powers of regulators are set out by Parliament and Government, while the technical requirements to achieve those objectives are designed and maintained by operationally independent regulators accountable to Parliament. [...] Regulation works best if regulators' objectives are clear and focused, ensuring a transparent division of responsibilities and accountability (see Written evidence submitted by the BOE to the Treasury Select Committee's inquiry, March 2021).

[91] Senior Bank policymakers have previously set out the benefits of a regulatory framework in which the high-level objectives, responsibilities and powers of regulators are set out by Parliament and Government, while the technical requirements to achieve those objectives are designed and maintained by operationally independent regulators

(continued)

- The report of the U.K. Parliament Treasury Committee emphasized these points, noting: "The regulators have a key role to play in designing and developing the rules with appropriate Parliamentary oversight. […] The independence of regulators to be free from political interference is one of the key aspects of United Kingdom financial services regulation, and it is, arguably, one of the reasons why the United Kingdom is a world-leading financial centre. *[…] The Government should be sparing in its approach: the strategic and operational objectives, combined with principles and "have regards" that are set out in their remit letters, are already numerous and expanding, to the point where regulators have to choose which to prioritize on a regular basis when drafting new policy proposals. The creation of too many activity-based principles would add a further layer of issues to which regulators must have regard. […]. We believe that effective scrutiny of regulatory proposals should be carried out through a targeted approach*".[92]

156. Proposed measures would bring significant changes for U.K. financial regulators. Several proposals are simply codifying existing practices (e.g., requirement for regulators to respond in writing to statutory consultations from parliamentary committees, requirement to notify the relevant parliamentary committee when financial regulators publish a consultation). But for the most part, proposed changes may substantially change relationships between the regulators, HMT, and Parliament.

157. There are clear benefits to delegating responsibility to the regulators for setting regulatory requirements that are often technical and complex. Resulting from the onshoring approach, most regulatory requirements including technical regulations are currently located in primary and secondary legislation that cannot be modified without an Act of Parliament. The legislative amendment process can be time consuming and may consume an excessive amount of parliamentary time to address purely technical requirements. The new proposed model would therefore provide more flexibility for the financial regulators to update standards in order to respond to emerging risks.

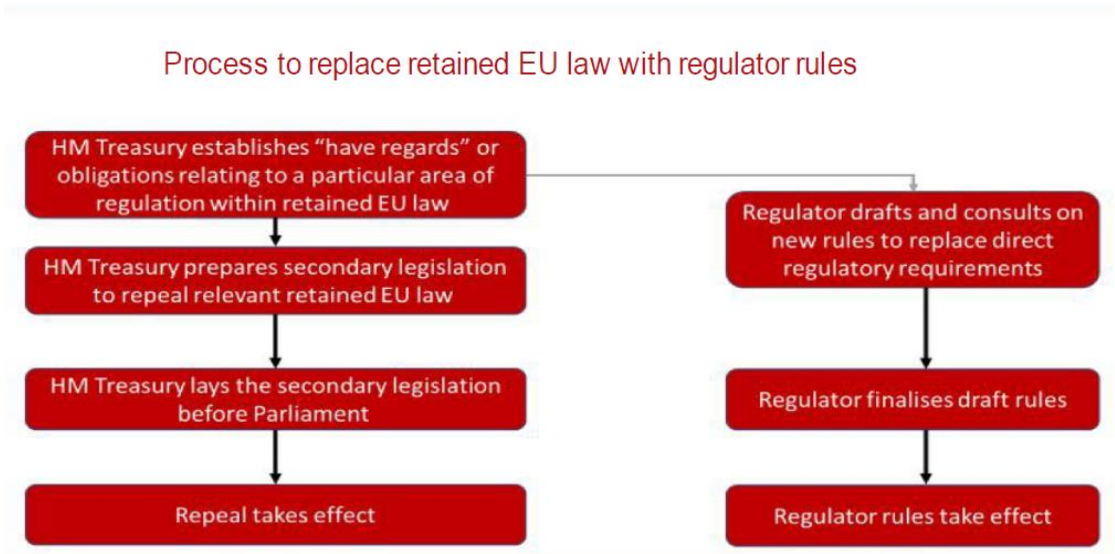
158. The process of repealing relevant retained EU law and concurrently replacing it with regulators' new rules will maintain continuity of regulatory requirements. Implementing the new model of financial services regulation will require the repeal of retained EU which will take effect at the same time as the regulators' new rules come into force to replace it (as depicted in Figure 8). This is a prudent and sensible approach that will avoid any "gap" in regulation. This process—repealing and replacing—will take place over several years. As explained in the

accountable to Parliament. […] Regulation works best if regulators' objectives are clear and focused, ensuring a transparent division of responsibilities and accountability (see Written evidence submitted by the BOE to the Treasury Select Committee's inquiry, March 2021).mechanisms, and to be clear on what each is seeking to achieve, before adding new measures. This could also help to inform possible improvements to, and rationalization of, existing measures. […] And where there may be a case for adding a new mechanism, or strengthening or re-purposing certain existing mechanisms, we would be concerned if any additions created overlapping or conflicting obligations, or duplicative mechanisms, prevented a balanced representation across all our stakeholders, reduced our operational and regulatory effectiveness to address emerging harm or meet changing circumstances, or introduced additional costs that would be borne by firms and consumers (see Written evidence submitted by the FCA to the Treasury Select Committee's inquiry, February 2021).

[92] House of Commons, Treasury Committee, "*The Future Framework for Regulation of Financial Services*", July 2021.

consultative document, "*in many cases it may be appropriate for the regulators to ensure continuity with the current provisions in retained EU law. However, there will also be instances where it is appropriate for the regulators to take the opportunity to tailor the rules to reflect the specifics of U.K. markets, and to make targeted improvements, in line with their objectives*". In that respect, the objectives assigned to U.K. financial regulators and the desired outcomes to be pursued are of the utmost importance (see below the discussion on objectives that are distinct from safety and soundness and market integrity).

Figure 8. United Kingdom: Moving to a Comprehensive FSMA Model



Sources: HM Treasury, Financial Services Future Regulatory Framework Review: Proposals for Reform, November 2021.

159. Several other proposals move in the right direction. Granting the BOE a general rulemaking power in relation to CCPs and CSDs would help ensure that the BOE has adequate powers to regulate and supervise these FMIs.[93] The introduction of a new Designated Activities Regime (DAR) would enable regulators to make rules for certain activities outside the current financial service's regulatory perimeter in FSMA and other relevant legislation. HMT would specify the scope of designated activities through secondary legislation. Regulators would make rules about how the designated activity would be carried out and firms would be required to follow those rules.

160. However, a proliferation of wider policy priorities, objectives and "have-regards" could divert focus from safety and soundness and financial stability. In the run up to the GFC, several jurisdictions, including in the United Kingdom, encountered a potential conflict between financial stability objectives and competitiveness considerations. The FSA was obliged to meet its

[93] The BOE is responsible for the regulation and supervision of CCPs and CSDs as part of its overall statutory objective to protect and enhance the stability of the U.K. financial system (these FMIs are essential to the stability of the financial system). However, the BOE has very limited rulemaking powers over CCPs and CSDs, since prior to EU exit the regulations relating to them were largely set at EU level through the European Market Infrastructure Regulation (EMIR) and the Central Securities Depositories Regulation, with the BOE responsible for supervision and enforcement of the EU regulations in the U.K.

main objectives[94] in ways consistent with the "principles of good regulation" prescribed by FSMA, which included the desirability of maintaining the competitive position of the United Kingdom when making and enforcing regulations. Competitiveness considerations were eliminated after the GFC. Since the PRA and FCA were established to replace the FSA, objectives assigned to U.K. financial regulators have been clear and focused. There is indeed a strong argument that one of the reasons for regulatory failure leading up to the GFC was excessive concern for competitiveness leading to a generalized acceptance of a 'light-touch' approach to regulation and supervision.[95] The PRA's existing secondary objective to facilitate effective competition in financial services, for example by facilitating entry and promoting competition between participants is distinct from an objective to support the international competitiveness of the United Kingdom's financial sector when making and enforcing regulations. This approach is, however, being increasingly questioned:

- Substantial changes are already in effect and proposed measures would go further. First, "competitiveness" has been listed as an aspect of Government economic policy to which the regulators should have regard in Recommendations Letters issued by the Chancellor since 2015.[96] Second, the Financial Services Act of 2021, which grants the PRA rulemaking authority to implement Basel III standards added additional considerations that the PRA must have regard to when making rules implementing the outstanding Basel III standards, including "*the likely effect of the rules on the relative standing of the United Kingdom as a place for internationally active credit institutions and investment firms to be based or to carry on activities*" Third, the second consultation document further proposes (i) elevating facilitating the long-term growth and international competitiveness of the U.K. economy as new statutory secondary objectives for the FCA and PRA, and (ii) introducing more have regard to considerations.

- While the introduction of these new objectives and have regard to considerations may not formally affect the primacy of the "primary" objectives assigned to the PRA and FCA, they could operate to increase the weight assigned by the PRA and FCA to non-prudential considerations in the discharge of their functions. It is important that a proliferation of wider policy priorities, objectives and "have-regards" with an increased focus on competitiveness does not delay, dilute, or divert focus from safety and soundness and financial stability. The primacy of PRA and FCA's

[94] Encouraging market confidence in the U.K. financial system, public awareness and understanding of the U.K. financial system, securing adequate consumer protections, reducing the incidence and impact of financial crime, enhancing financial stability.

[95] See "A new approach to financial regulation judgment, focus and stability", HMT, July 2010, and "Financial Services Future Regulatory Review: Phase II consultation", HMT, October 2020. A competitiveness objective was not retained when the PRA and FCA were established.

[96] The BOE Act 1998 requires HMT, at least once in each Parliament, to make recommendations to the PRC about aspects of the economic policy of the government to which the PRC should have regard when considering how to advance the objectives of the PRA and when considering the application of the regulatory principles set out in the FSMA.

objectives of safety and soundness and market integrity should be maintained in principle and in practice, as required by international standards.[97]

161. Accountability and engagement mechanisms are both essential and already well established in the United Kingdom:

- Key principles and fundamental pre-requisites that underpin effective supervision result from international standards and are reflected in best practices. Regulatory independence includes mechanisms for holding financial regulators accountable for carrying out their responsibilities while allowing them to remain free of interference in their operations. As required by the BCPs[98], and ICPs[99] supervisors must be accountable through a transparent framework for the discharge of their duties. To support the policy-making process, meaningful engagement in a transparent manner with all stakeholders is also important to ensure that requirements are well calibrated and understood. Given important policy issues that include but are not limited to regulatory issues, consultation between regulators and other public authorities can be beneficial. Considering perspectives, inputs and concerns raised by stakeholders is certainly important for financial regulators.

- In the United Kingdom, financial regulators are accountable to the Parliament, which has a key role in objective setting and high-level policy making through primary legislation. Engagement mechanisms exist between HMT and the regulators while existing legislation already provides a large number of formal accountability mechanisms between the regulators and HMT in specific circumstances.[100] Stakeholder engagement during the policy-making process is also well established. In this regard, the FSAP team has observed that U.K. financial regulators are extremely transparent in their approach to regulating firms.[101] Key processes to promote transparency include regular communications on the supervisory approach and the main supervisory expectations, a structured consultation process, and regular evaluations conducted in a transparent manner. Respondents to the consultation also noted that the regulators conduct extensive stakeholder engagement on their proposed policies, and that the consultation requirement works well. Similarly, the U.K. government considers that existing

[97] E.g., BCP 1, EC 2: "the primary objective of banking supervision is to promote the safety and soundness of banks and the banking system. If the banking supervisor is assigned broader responsibilities, these are subordinate to the primary objective and do not conflict with it."

[98] CP 2: The supervisor possesses operational independence, transparent processes, sound governance, budgetary processes that do not undermine autonomy and adequate resources and is accountable for the discharge of its duties and use of its resources.

[99] ICP 2: Supervisor The supervisor is operationally independent, accountable, and transparent in the exercise of its responsibilities and powers, and has adequate resources to discharge its responsibilities

[100] HMT may appoint an independent person to conduct a review of the economy, efficiency, and effectiveness of the FCA's use of resources (FSMA, section 1S.). HMT may direct the PRA or FCA to carry out investigations into specific events if that is in the public interest (Financial Services Act 2012, section 77). HMT may direct the PRA or FCA to act, or refrain from acting, in relation to specified matters to ensure that the United Kingdom meets its international obligations (FSMA, section 410). In 2014, HMT conducted a review of enforcement decision-making at the financial services regulators.

[101] See TN on Banking Supervision and Detailed Assessment Report on Observance of Insurance Core Principles, in particular ICP 2.

mechanisms governing the regulators' relationship with HMT, both formal and informal, are largely effective.

162. The introduction of enhanced accountability, scrutiny and engagement mechanisms should not have the effect of constraining financial regulators' agility. To encourage "*systematization of regulators' review of rules*", the FRF Review 2021 Consultation is seeking comment on whether there should be a power for HMT to require the regulators to review their rules where the government considers that it is in the public interest. This also would allow for an independent person to be appointed to conduct the review. It also consults on whether cost benefit analyses (CBA) for proposed regulations should be improved (the government proposes notably the creation of new statutory panel(s) dedicated to supporting the development of the regulators' CBAs).[102] HMT would be empowered to require regulators to conduct a rule review and regulators would have to respond to recommendation letters.[103] While those reviews are intended to be used in exceptional circumstances, the term "public interest" is broad. Considering the effectiveness of existing mechanisms noted above, it is not immediately apparent that cooperation and accountability arrangements would not be sufficient given regulators' increased responsibilities.[104] As the authorities finalize the draft legislation and calibrate the requirements, it will be important to carefully weigh the pros and cons of adopting additional accountability measures. Imposing additional obligations, individually or in combination, may indeed prevent or delay the PRA and FCA from effectively discharging their primary prudential objectives:

- *Potential impact on operational independence*. One proposal would introduce a new avenue for challenging the regulators' rulemaking (e.g., requiring regulators to have another look at their rules or appointment of an independent person to conduct a review). The argument seems to assume that regulators do not have an institutional interest in ensuring that their rules remain relevant and achieve their intended purpose over time. This proposal also suggests that the regulators are conflicted or do not have the technical expertise needed to review their own regulations. The ability to challenge existing rules while maintaining the operational independence may be viewed as too optimistic given that setting out requirements and enforcing them through day-to-day supervision forms a continuum. Even though regulators would retain authority to take decisions without an explicit political 'veto', imposing a new requirement for the PRA and FCA to respond to HMT Recommendations Letters may put financial regulators in a delicate situation should they decide to not adopt some of these recommendations.

[102] Two options have been proposed. The government is consulting whether it would be most effective for the panel to provide its input "pre-publication" as part of the development of CBA for individual consultations, or for the panel to provide its input "post-publication" and scrutinize the approach post-implementation, at a more aggregate level.

[103] The first consultation also proposed to include systematic consultation between agencies and HMT at an early stage in the policy-making process, before proposals reach the public consultation stage. Given the detailed measures proposed in the second consultation, the government is continuing to consider whether any further arrangements for how the regulators may be required to consult HM Treasury are necessary.

[104] For more details, see the TN on Banking Supervision.

- *Resource implications*. As some of these proposals would be resource intensive for U.K. financial regulators and could divert the regulators' attention from other important tasks, authorities will need to weigh the benefits of enhanced accountability mechanisms against additional resource burdens to ensure that adequate resources are still devoted to core activities (i.e., supervising regulated firms).

- *Regulators' agility*. Overall, the proposals will make regulatory rulemaking more agile, by enabling the regulators to make rules in areas which are currently covered by retained EU law. However, certain proposals also have the potential to delay the introduction of new or updated rules (or make it more complicated) in response to emerging risks or changing circumstances. It is unclear whether the scope of a CBA would be extended to supervisory guidance and whether inadequate CBA analyses could be subject to judicial review. While important for financial regulators, CBA can be resource intensive, time consuming and may encounter significant challenges as the costs are traditionally easier to measure than the long-term benefits to financial stability. Therefore, it will be very important to (i) introduce new requirements in a proportionate manner, focusing primarily on major rules, and (ii) ensure that inputs provided by the existing statutory panel, or any revised panel, do not excessively emphasize the short-term costs and are provided on a regular basis (at a specified frequency) rather than on a case-by-case basis.

163. Going forward, preserving the primacy of the U.K. financial regulators' general objectives in principle and in practice will, therefore, be paramount. Accountability and scrutiny mechanisms should also operate in a way that preserves the day-to-day independence of the financial U.K. regulators and does not reduce operational and regulatory effectiveness. Maintaining robust and high-quality regulatory standards that naturally encourage investment and growth is the best way to preserve the United Kingdom's role as a major financial centre.

Appendix I. Using Financial Payments Data and Machine Learning for Financial Integrity Surveillance

This Appendix describes the data points used and methodological approach for the IMF staff's surveillance of financial integrity risks using the isolation forest model.

A. Data Points Used

1. SWIFT data. The model uses SWIFT message types 103, 103+, 103R that represent payments between the customers of financial institutions. The SWIFT data is aggregated on the level of a financial institution and anonymized by replacing the name of the financial institution with the corresponding country name. SWIFT data includes the countries of financial institutions that originated and received the payments, as well as countries of correspondent financial institutions that facilitated the payment. The SWIFT data is monthly going back to January 2013. The data includes the currency, number and value of transactions that passed through each of these payment corridors (originator-correspondents-beneficiary)—a hypothetical example:

Period	Message Type Code	Message_ Type _Name	Ordering _Country	Counterpar ty _Country	Beneficiary _Country	Currency	Total Number of Transaction s	Total Value of Transaction s
Nov-13	MT103+	Single Customer Credit Transfer	Country X	Country Y	United Kingdom	USD	85	5326336

2. Compliance with AML Standards. The level of compliance with international AML Standards is based on the results of assessments by the Financial Action Task Force (international AML/CFT standard setter) and respective regional bodies. The index of compliance with the AML Standards is based on the assessment's ratings of effectiveness of a given country's AML/CFT regime. Where not available (mostly earlier periods) the index is based on the technical compliance of a given country's legislation with the AML/CFT Standards. The AML compliance index is a time series, which takes into account new and follow-up assessments.

3. Portfolio and direct investments. Investment data from the Coordinated Portfolio and Direct Investment surveys.

4. Foreign trade. Export data from IMF's Direction of Trade data is used, which appears to be more accurate than the imports data.

5. Corruption. Control of corruption indicator from the World Governance Indicators.

6. **Financial Secrecy and Tax Haven Indexes.** Financial Secrecy Score and Tax Haven Score from the Tax Justice Network.

7. **Gross Domestic Product.** Data on the current prices GDP from the World Economic Outlook Database.

B. Methodological Approach

- **Cross-Border Payments Only**. Only cross-border payments are used, dropping the payments that originate and are received in the same country.

- **Normalization of Outflows from Ordering Countries**. The (i) *value of transactions* and (ii) *the average transaction* sent through a given payment corridor are normalized using z-scores[1] and the means and standard deviations for the outflows from *the ordering country*, as not to bias the results towards the advanced economies and established financial centers that have higher value of transactions and the average transactions.

- **Normalization of Flows from Payment Corridor**. The (i) *value of transactions* and (ii) *the average transaction* of a given payment corridor are also normalized using z-scores and means and standard deviations for the flows via a particular *payment corridor* (unique payment chain of originator-correspondents-beneficiary, in other words a unique set of banks involved in the transaction). The intention is to detect appearance of the new payment corridors or payment corridors that are processing unusually high overall values or have high average transaction value, which may potentially indicate abuse of a financial institution.

- **AML Index Factor**. The AML Compliance data is incorporated into the model by using interaction of the AML index with the variables (i) *value of transactions normalized by ordering country* and *by payment corridor* and (ii) *average transaction normalized by ordering country* and *by payment corridor*. The AML index for the ordering country is used to indicate the higher risk of outflows from a country with lower effectiveness of the AML/CFT regime. The normalized *value of transactions* and the *average transaction* is multiplied by the AML index of the ordering country, which ranges from 0 to 1 (0 being the lowest level of compliance with the AML/CFT Standards), so the *value of transactions* and the *average transaction* are weighted proportionate to the degree of weakness of the AML compliance, thus increasing the likelihood of a payment corridor being an outlier [2].

- **Economic Activity Factor**. Economic activity, such as trade and portfolio/direct investment, provides the economic rationale for the financial flows, representing lower risk of money laundering. A ratio of the *value of transactions* between the two given countries and the portfolio/direct investment between these two countries is introduced. The lower the amount of

[1] A z-score measures a specific values distance from the mean of a group of values. Z-scores are measured in standard deviations from the mean. For example, a z-score of 1.0 is 1 standard deviation from the mean and a z-score of 0 indicates the value is identical to the mean of the group of values.

[2] The threshold for the outlier payments is set at the 0.0001 percent of all payment corridors.

investments between the two countries, the higher this ratio, thus increasing the likelihood of being an outlier.

- Portfolio and direct investment have semiannual and annual frequency respectively, so for this ratio all of the flows between the two countries are summed up over 6 or 12 months correspondingly, which is then added to all payments between the two countries over the respective periods.

- **Trade Activity**. Similarly, a ratio of the *value of transactions* between the two given countries and the foreign trade activity (both imports and exports) between these two countries is introduced. The lower the amount of trade between the two countries, the higher this ratio, thus increasing the likelihood of being an outlier.

- **Tax and Financial Secrecy Indexes**. Flows to/from countries with high financial secrecy or harmful tax practices represent higher risk that the transaction is an illicit and tax avoidance related financial flow (ITAFF). Variables are introduced that are the result of multiplication of the *financial secrecy* and *tax haven indexes and* (i) *value of transactions normalized by ordering country* and *by payment corridor* as well as (ii) *average transaction normalized by ordering country* and *by payment corridor*. The higher are the indexes for the financial secrecy and tax haven, the higher is the weighting of the corresponding payments, thus increasing the likelihood of being an outlier.

- **Corruption Risks**. Outflows from countries with higher perceived corruption represent a higher risk that the transaction is an ITAFF. Corruption perception variables are incorporated by multiplying the control of corruption indicator by the (i) *value of transactions normalized by ordering country* and *by payment corridor* and (ii) *average transaction normalized by ordering country* and *by payment corridor*. The higher are the corruption perceptions, the higher is the product of this multiplication, thus increasing the likelihood of being an outlier.

- **Trade and Investment Data**. Trade and investment data have longer lag in availability as compared to the SWIFT data and in order to run the model once the SWIFT data is available, the trade and investment data are extrapolated. The average of previous periods is then used, adjusted for the projected GDP growth and also for the seasonality of the trade data, which is monthly.

- **Macro-Criticality and GDP**. A measure of macro-criticality of the outflows adds a focus on outflows big enough to have a potential to destabilize external or domestic stability of the ordering country. A ratio of the *value of transactions* (nominal values, not normalized) to the GDP of ordering country is also added.

- Based on the algorithm's results, the variables with the highest contribution to the output (based on the Shapley values analysis), are the (i) foreign direct investment, (ii) foreign portfolio investment and (iii) the foreign trade. In other words, whether the high financial flows between the two countries correspond to the high trade or portfolio or direct investment flows is the most important determinant of whether the payments would be identified as unusual or outliers.