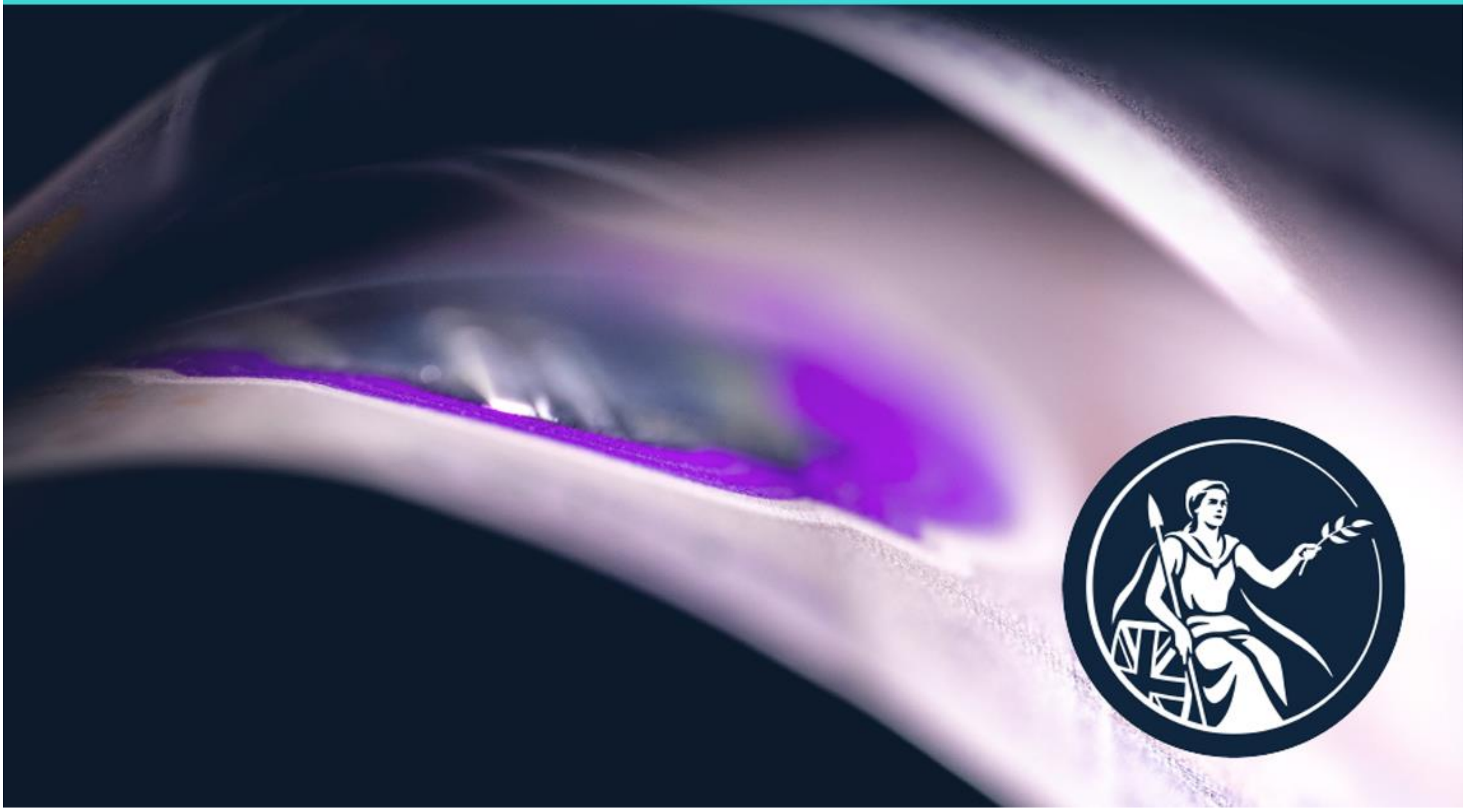
Bank of England

Prudential Regulation Authority

Appendices to Artificial intelligence and machine learning

Discussion Paper | DP5/22

October 2022



Appendices

Appendix 1 – Domestic developments

This section provides a high-level overview of significant domestic developments.

UK National AI Strategy

The **National AI Strategy** was published by the UK Government in September 2021, via the Department for Business, Energy & Industrial Strategy (BEIS), the Department for Digital, Culture, Media & Sport (DCMS), and the Office for Artificial Intelligence. The National AI Strategy supports the **Plan for Digital Regulation**, which was published in July 2021, and sets out various initiatives based around three fundamental pillars:

- investing in and planning for the long-term needs of the AI ecosystem to remain a science and AI superpower;
- supporting the transition to an AI-enabled economy, capturing the benefits of AI innovation in the UK, and ensuring AI technologies benefit all sectors and regions; and
- ensuring the national governance of AI technologies encourages innovation, investment, protects the public, and safeguards the UK's fundamental values, while working with global partners to promote the responsible development of AI internationally.

As part of the National AI Strategy, the UK Government committed to developing a national position on governing and regulating AI. The UK Government expressed its intention to publish a White Paper setting out the government's position on the potential risks and harms posed by AI technologies and the proposed approach to address them.

The UK government also published a policy paper setting out its emerging thinking on establishing a pro-innovation approach to regulating AI in July 2022. Please see table A below for a potential mapping of the cross-sectoral principles for AI regulation as set out in the policy paper to this DP.

Table A: Mapping proposed UK government principles to the DP

Cross-sectoral principles for AI regulation	Reference in DP
Ensure that AI is used safely	Chapter 3: Consumer protection – FCA Chapter 3: Insurance policyholder protection – PRA Chapter 3: Safety and soundness – PRA Chapter 3: Financial stability and market integrity – Bank and FCA Chapter 4: Existing regulations – Consumer Chapter 4: Existing regulations – Data Chapter 4: Existing regulations – Model Chapter 4: Existing regulations – Governance

Cross-sectoral principles for AI regulation	Reference in DP
Ensure that AI is technically secure and functions as designed	Chapter 3: Safety and soundness – PRA Chapter 4: Existing regulations – Consumer Chapter 4: Existing regulations – Data Chapter 4: Existing regulations – Model Chapter 4: Existing regulations – Governance Chapter 4: Existing regulations – Operational resilience
Make sure that AI is appropriately transparent and explainable	Chapter 2: Objectives and Remits Chapter 3: Benefits and Risks Chapter 4: Existing regulations
Embed considerations of fairness into AI	Chapter 3: Consumer protection – FCA Chapter 3: Insurance policyholder protection – PRA Chapter 4: Existing regulations – Consumer
Define legal persons' responsibility for AI governance	Chapter 4: Existing regulations – Governance
Clarify routes to redress or contestability	Chapter 4: Existing regulations – Consumer Chapter 4: Existing regulations – Governance

Digital Regulation Co-operation Forum

The **DRCF** is a national regulatory network supporting co-operation across the breadth of responsibilities for regulating digital services. Its members consist of the CMA, the ICO, Ofcom, and the FCA. The algorithmic processing **workstream** was set up to strengthen shared understanding of, and expertise in, algorithmic systems. It aims to do this by identifying areas where common practical approaches in different regulatory regimes can be streamlined and by developing solutions to deliver efficiencies for industry.

In 2021, the algorithmic processing workstream undertook a programme of stakeholder engagement leading to two publications in April 2022, covering the benefits and harms of algorithms,[1] and algorithmic audit.[2] The DRCF will carry out further work supporting improvements in algorithmic transparency as part of its workplan for 2022 to 2023, including

[1] **DRCF (2022) 'The benefits and harms of algorithms: a shared perspective from the four digital regulators'.**

[2] **DRCF (2022) 'Auditing algorithms: the existing landscape, role of regulators and future outlook'.**

improving DRCF members' capabilities for algorithmic auditing, researching the third party algorithmic auditing market and promoting transparency in algorithmic procurement.[3]

Other UK government and regulator activity

Data protection and security

Concerning data protection and security, DCMS published the UK **National Data Strategy** in September 2020, and created a **National Data Strategy Forum** and issued a **public consultation** on reforms to the UK's data protection regime in September 2021 and the **Data Protection and Digital Information Bill** has since been introduced. The consultation proposed some measures relevant to UK GDPR (specifically in relation to **Article 22: Automated individual decision-making, including profiling**) and the use of AI, in response to the recommendations in the **Taskforce on Innovation, Growth and Regulatory Reform report**.

In April 2019, the National Cyber Security Centre published **guidance** on assessing intelligent tools for cyber security, which covers off-the-shelf security tools that use AI, the development of in-house AI security tools, and the development of AI tools for non-security business functions. The ICO published **guidance on AI and data protection** in July 2020. In May 2021, the CMA and the ICO made a **joint statement** on competition and data protection law which sets out their shared views on the relationship between competition and data protection in the digital economy.

The Bank and FCA launched a plan to **transform data collection** in February 2021 to identify how data collection should improve to increase the value and reduce the burden to firms. The Bank and FCA **published an update** in April 2022 and will be broadening their engagement with regulated firms to understand challenges faced by firms in relation to data collection later in 2022.

Transparency and explainability

The ICO has published **guidance** relating to decisions made with AI, specifically covering how to explain AI in practice for technical teams. In February 2020, the FCA and the Alan Turing Institute published the paper on **AI transparency in financial services**, which presents an initial framework for thinking about transparency needs in relation to AI in financial services. In November 2021, Central Digital and Data Office within the UK Government set out the **algorithmic transparency standard** to help public sector organisations provide clear information about the algorithmic tools they use (including AI) and why they use them.

[3] **Digital Regulation Cooperation Forum: Plan of work for 2022 to 2023**.

Standards and assurance

The DRCF's **DP on algorithmic audit** covers these issues in more detail. The Centre for Data Ethics and Innovation's (CDEI) **The roadmap to an effective AI assurance ecosystem** sets out a potential approach to building an ecosystem to support assurance of AI systems in the UK.

Online harms

In December 2020, DCMS published the **Online Harms White Paper** that set out a programme of action to tackle content or activity that harms individual users or threaten the way of life in the UK. In March 2022, the **Online Safety Bill** was published with the aim of establishing a new regulatory regime to address illegal and harmful content online.

In 2019, Ofcom commissioned Cambridge Consultants to produce the report **Use of AI in online content moderation**, which examines the capabilities of AI in meeting the challenges of moderating online content. This topic was also covered by the CDEI in an August 2021 blog, entitled **The use of algorithms in the content moderation process**.

Intellectual property

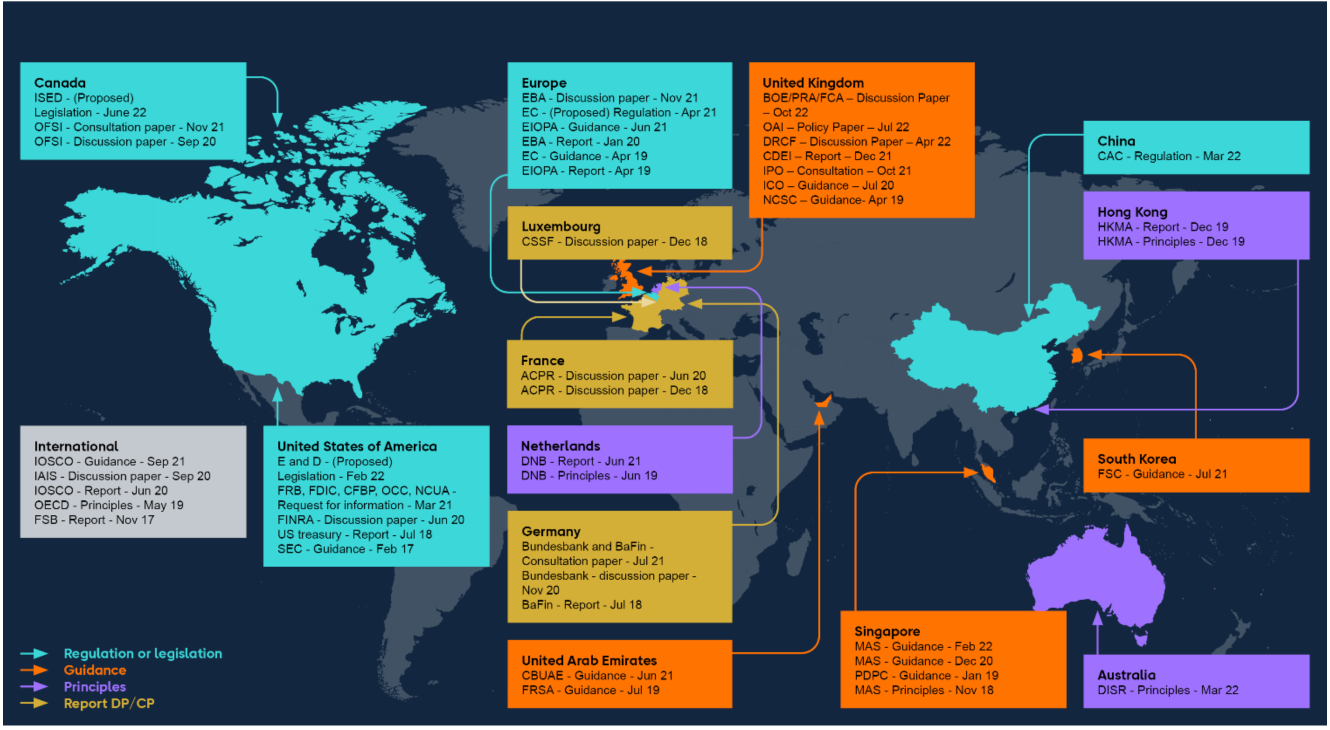
In October 2021, the Intellectual Property Office consultation and **government response** on AI and intellectual property, including copyright and patents. The consultation covers topics such as copyright in works made by AI, text and data mining using copyright material, and patents for inventions devised by AI.

Appendix 2 – International developments

Overview of international regulation

This section provides a high-level overview of significant international developments. There is a growing body of international publications on AI and while many of these are DPs or consultations, there is an increasing number of published principles and guidance including cross-sectoral legislation (Figure 1 shows a selection of regulatory publications). For more information, please see the table in the **linked spreadsheet**.

Figure 1: Map of global financial services regulatory publications on AI



Canada
ISED - (Proposed)
Legislation - June 22
OFSI - Consultation paper - Nov 21
OFSI - Discussion paper - Sep 20

Europe
EBA - Discussion paper - Nov 21
EC - (Proposed) Regulation - Apr 21
EIOPA - Guidance - Jun 21
EBA - Report - Jan 20
EC - Guidance - Apr 19
EIOPA - Report - Apr 19

United Kingdom
BOE/PRA/FCA – Discussion Paper – Oct 22
OAI – Policy Paper – Jul 22
DRCF – Discussion Paper – Apr 22
CDEI – Report – Dec 21
IPO – Consultation – Oct 21
ICO – Guidance – Jul 20
NCSC – Guidance- Apr 19

China
CAC - Regulation - Mar 22

Hong Kong
HKMA - Report - Dec 19
HKMA - Principles - Dec 19

Luxembourg
CSSF - Discussion paper - Dec 18

France
ACPR - Discussion paper - Jun 20
ACPR - Discussion paper - Dec 18

International
IOSCO - Guidance - Sep 21
IAIS - Discussion paper - Sep 20
IOSCO - Report - Jun 20
OECD - Principles - May 19
FSB - Report - Nov 17

United States of America
E and D - (Proposed)
Legislation - Feb 22
FRB, FDIC, CFBP, OCC, NCUA - Request for information - Mar 21
FINRA - Discussion paper - Jun 20
US treasury - Report - Jul 18
SEC - Guidance - Feb 17

Netherlands
DNB - Report - Jun 21
DNB - Principles - Jun 19

South Korea
FSC - Guidance - Jul 21

Germany
Bundesbank and BaFin - Consultation paper - Jul 21
Bundesbank - discussion paper - Nov 20
BaFin - Report - Jul 18

Singapore
MAS - Guidance - Feb 22
MAS - Guidance - Dec 20
PDPC - Guidance - Jan 19
MAS - Principles - Nov 18

United Arab Emirates
CBUAE - Guidance - Jun 21
FRSA - Guidance - Jul 19

Australia
DISR - Principles - Mar 22

There are broadly three categories of regulatory responses to AI in financial services which are sometimes used in combination.

Cross-sectoral legislation on AI

These establish a framework and harmonised rules for the use of AI across sectors, which sometimes also prohibit the use of AI in certain circumstances or use-cases. Prominent examples include:

The EU proposal for a **Regulation** of the European Parliament and of the Council on 'Laying Down Harmonised Rules on Artificial Intelligence' (also known as the 'AI Act') was published in April 2021. The proposed AI Act would apply across multiple sectors and apply to certain financial services. AI systems used to generate credit scores or evaluate creditworthiness are currently the only financial services use case that the proposed AI Act would classify as high-risk and therefore subject to stricter requirements.

Similarly, there is pending legislation in Canada. **Bill C-27**, includes the Artificial Intelligence and Data Act (AIDA). If passed, the Act will establish the first country-wide requirements for the design, development, and use of AI systems. Additionally, it will ban certain conduct in relation to AI systems that may cause serious harm to individuals or their interests.

In February 2022, the **Algorithmic Accountability Act**, was passed by the US Congress following reports that AI systems result in discriminatory outcomes. The Bill, if enacted, will authorise the Federal Trade Commission (FTC) to enforce its requirements. Certain businesses, meeting the relevant thresholds, (including banks and insurance companies) that deploy augmented critical decision processes or automated decision systems would be required to conduct impact assessments, identify any biases and security issues, and submit annual reports to the FTC of their results.

The Chinese provisions, known as the **Internet Information Service Algorithmic Recommendation Management Provisions**,[4] are the only AI-specific legislation of which we are aware covering financial services and have already come into effect (in March 2022). The rules appear to apply to all algorithmic recommendation technology, including technology that uses AI, across all sectors. Under the provisions, for instance, companies will be prohibited from using algorithms to extend unreasonably differentiated treatment in trading conditions, such as trading prices, on the basis of consumers' tendencies, trading habits and other such characteristics.

Sector-specific principles or guidance on AI

These tend to set out principles, guidance, or broad supervisory expectations related to areas such as fairness, ethics, risk management, accountability, and transparency. Examples of this approach include principles developed by the **De Nederlandsche Bank**, **Hong Kong Monetary Authority**, and **Monetary Authority of Singapore** (MAS). These high-level principles are sometimes followed by subsequent publications, projects, and policy tools, such as the **Veritas initiative** led by MAS. Similarly, the **European Insurance and Occupational Pensions Authority's** independent Consultative Expert Group issued a set of high-level governance principles with accompanying guidance for insurance firms on how to implement them in practice. Examples of high-level guidance from financial services regulators and standard setting bodies include guidance issued by the **Central Bank of the UAE**, **IOSCO**, and the South Korean **Financial Services Commission**.

Sector-specific reviews of existing rules

[4] Please note that the hyperlinked reference is not an official translation.

These tend to provide a review of existing rules and guidance to assess whether they remain appropriate to developments in AI in financial services. Examples of this include a DP by the **European Banking Authority** and the **Request for Information by US authorities**. This can be done in a technology neutral manner, recognising the difficulties in defining AI or demarcating where the risks associated with advanced analytical approaches first arise.

Appendix 3 – Data – current regime

The following tables give a broad overview of certain key existing legal requirements and guidance relevant to use of data in AI systems and processes.

Table B: Data quality, sourcing, and assurance

Regulations/rules/ guidance/principles	Comment
BCBS 239	Lists a set of principles aimed at strengthening risk data aggregation capability and internal/external reporting processing procedures. Risk data aggregation, according to BCBS 239, is defined as ‘defining, gathering, and processing risk data, according to the bank’s risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite. This includes sorting, merging, or breaking down sets of data’. The principles are applicable to data that are critical in enabling a bank to manage the risks it faces, and also to all key internal risk management models. Under the topic area of risk data aggregation capabilities, there are four principles which address factors that make up data quality these are: accuracy and integrity, completeness, timeliness, and adaptability. Overall, BCBS 239 provides for adequate controls across the lifecycle of data, with up-to-date and accurate risk data being captured in a timely manner. Any risk data aggregation must be documented, and automated if possible and BCBS 239 states that banks should strive towards a single authoritative source of risk data for each type of risk. BCBS 239 states that Globally Systemically Important Banks (G-SIBs) should comply with its principles within three years of their designation and strongly suggests that national supervisors apply these principles to domestic systemically important banks three years after their designation. It states that national supervisors may choose

Regulations/rules/ guidance/principles	Comment
	to apply the principles, in a proportionate way, to a wider range of banks.
BCBS 328	Addresses the corporate governance of a bank. As part of this governance, a key principle is 'risk identification, monitoring, and controlling', which stresses the importance of having accurate internal and external data to mitigate risk and make strategic business decisions. Specifically gives special attention to the completeness and accuracy of the data. BCBS 328 specifies that the implementation of these principles for firms 'should be commensurate with the size, complexity, structure, economic significance, risk profile, and business model of the bank and the group (if any) to which it belongs. This means making reasonable adjustments where appropriate for banks with lower risk profiles, and being alert to the higher risks that may accompany more complex and publicly listed institutions. SIFIs are expected to have in place the corporate governance structure and practices commensurate with their role in and potential impact on national and global financial stability.'
Principle for Financial Market Infrastructures (**PFMI**)	States that trade repositories must ensure that the data it maintains are accurate and current in order to serve as a reliable central data source.
UK Data Protection Legislation: **UK GDPR** and **DPA 2018**	Contain detailed principles and rules that are specific to ensuring that personal data is high quality (eg that is accurate and not misleading) and that it is processed only within certain parameters. Lays out clear requirements for the lawful processing of special category personal data and defines the rights of individuals ('data subjects') whose personal data is processed. Apply to all processing of personal data by firms.

Regulations/rules/ guidance/principles	Comment
Solvency II	PRA rules transposing Solvency II require firms to have internal processes and procedures in place to ensure the completeness, accuracy, and appropriateness of the data used in the calculation of their technical provisions. Solvency II is a prudential regime for insurance firms and groups.
Markets in Financial Instruments Regulation (MiFIR)	Specifies requirements for the reporting of trade transparency information, including the information required and the timeframes in which it must be reported and transaction reporting information submitted to the FCA to facilitate detection of market abuse (see **Commission Delegated Regulation (EU) 2017/590**).
Article 18 of Commission Delegated Regulation (EU) 2018/959	Refers to competent authorities assessing the degree to which the quality of the data used by an institution in the Advanced Measurement Approach (AMA) framework is maintained.
UK EMIR/UK SFTR	Specifies requirements for the reporting of trading data to trade repositories in relation to OTC derivatives and securities financing transactions including securities lending and repos.

Table C: Data privacy, security, and retention

Regulations/rules/ guidance/principles	Comment
UK Data Protection Legislation: UK **GDPR and DPA 2018**	Give individuals rights in relation to their personal data and requires firms to process personal data fairly and transparently. This includes requiring firm to identify a lawful basis for processing personal data, tell individuals how their personal data is being used, process personal data securely and delete it when it is no longer needed.
PFMI	States that trade repositories (TR) need to attend to operational risks and specific operational risks that a TR must manage include risks to data integrity, data security, and business continuity. Furthermore, a TR's rules, procedures, and contracts should be clear about the legal status of the transaction records that it stores. The legal basis should also determine the rules and procedures for providing access and disclosing data to participants, relevant authorities, and the public to meet their respective information needs, as well as data protection and confidentiality issues.
SYSC 4.1.1R and Rule 2.4 of the **General Organisational Requirements Part of the PRA Rulebook** for CRR firms.	SYSC 4.1.1R requires common platform firms to have sound security mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access, and prevent information leakage. This is mirrored in PRA Rule 2.4 of the General Organisational Requirements Part of the PRA Rulebook for CRR firms.
Payment Service Regulations 2017 (Reg 69(3)(g) and 70(3)(f))and SCA-RTS	States that account information service providers (AISPs) and payment initiation service providers (PISPs) are not permitted to use, access or store any information for any purpose except for the provision of the account information or payment initiation service explicitly requested by the payer. Furthermore, in order to address data security and privacy in payment services, the provision of data architecture and infrastructure is also addressed through the UK payments

Regulations/rules/ guidance/principles	Comment
	regime. Under Article 36(3) of the Regulatory Technical Standards on Strong Customer Authentication (SCA-RTS), AISPs must have in place suitable and effective mechanisms to prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the user's explicit consent. This means that where a customer only provides explicit consent to the AISP for a sub-set of their account data to be accessed (eg their current account but not their credit card account), only this should be accessed by the AISP. It also defines regulatory technical standards for strong customer authentication and common and secure open standards of communication**.**

Table D: Data architecture, infrastructure, resilience and outsourcing

Regulations/rules/ guidance/principles	Comment
BCBS 239	Specifies that banks should design, build, and maintain data architecture which fully supports its risk data aggregation capabilities and risk reporting practices in times of stress or crisis and normal times, and that it is taxonomised. It is specifically stated that banks should have strong risk data architecture and IT infrastructure.
BCBS 328	Includes a principle that the sophistication of the bank's risk management and internal control infrastructure (inclusive of data architecture and IT infrastructure) should keep pace with the bank's risk profile.
MiFiD II (retained EU law)	Requires investment firms and market operators engaged in algorithmic trading and data reporting services providers to perform testing on algorithmic trading and IT systems and have appropriate business continuity arrangements in place to ensure the timely resumption of trading and reporting in case of disruptive incidents.

Regulations/rules/ guidance/principles	Comment
Payment Service Regulations 2017 (Regulation 98) and the SCA-RTS	Specifically addresses the data infrastructure/architecture aspect in conjunction with the aspect of privacy/security. Stating the requirement for payment service providers to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services it provides, including establishing and maintaining effective incident management procedures. Furthermore, in order to safeguard the confidentiality and the integrity of data, Article 35 of the SCA-RTS requires that a secure encryption is applied between banks and open banking service providers when exchanging data.
Ring-fencing	Specifies that everything which is applicable to be reported on a consolidated basis would also need to be reported at the level of the ring-fenced bank sub-group, therefore the architecture/ infrastructure for data applicable to would also need to be at sub consolidated level.
Outsourcing and **SS2/21**	The Rulebook states that a firm must ensure that it takes reasonable steps to avoid undue additional operational risk when relying on a third-party for the performance of operational functions which are critical for the performance of relevant services and activities on a continuous and satisfactory basis. The SS sets out the expectations of how PRA-regulated firms should comply with regulatory requirements and expectations relating to outsourcing and third-party risk management. Such as the PRA expects firms to implement appropriate measures to protect outsourced data and set them out in their outsourcing policy.

Table E: Data governance

Regulations/rules/ guidance/principles	Comment
BCBS 239	Specifies that it is the responsibility of the board to promote strong data governance, such as policies on assessment, management, sourcing, confidentiality, integrity, and availability.
UK Data Protection Legislation: UK **GDPR and DPA 2018**	States that the controller is accountable for compliance with UK GDPR principles, and sets out when a data protection officer must be in place. A controller and processor must designate a data protection officer if core activities require large scale regular and systematic monitoring of data subjects; or core activities consist of large-scale processing of special categories of data.
Solvency II Conditions Governing Business 6.1	Specifically requires a firm to have an effective actuarial function which will assess the sufficiency and quality of data used in calculations of technical provisions.
Payment Service Regulations 2017 (Regulation 98)	Includes a requirement for payment service providers to provide to the FCA an updated and comprehensive assessment of the operational and security risks relating to the payment services it provides and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks annually.

Appendix 4 – Model Risk Management – current regime

The following tables give an overview of the existing PRA regime relevant to various aspects of MRM for PRA-regulated firms:

Table F: Effective governance framework, policies, procedures, and controls to manage model risk

Regulations/rules/ guidance/principles	Comment
SS3/18 'Model risk management principles for stress testing'	Looks at the governance surrounding the use of stress testing models and states the PRA's expectation that firms should focus their validation and independent review activities commensurate with the overall use, complexity, and materiality of models across the lifecycle of the model, including the issue of controls, to ensure those models that pose most significant risks are adequately managed. The SS is relevant to PRA authorised banks, building societies and PRA-designated investment firms only.
SS11/13 'Internal Ratings Based (IRB) approaches'	States that the appropriate SMF(s) (not expected to be more than two) should provide an annual attestation on the firm's arrangements for approving rating and estimation processes under **Article 189 of the Capital Requirements Regulation (CRR)**. Article 189 of the CRR requires all material aspects of the rating and estimation processes to be approved by the firm's board or designated committee and senior management. These parties must possess a general understanding of the firm's rating systems and detailed comprehension of its associated management reports. There are separate requirements that apply to senior management. PRA SS11/13 also lists criteria for the process of temporary changes to PRA approved models, including that information in regards to the adjustments should be presented to senior management. The SS is applicable to CRR firms using or seeking to use IRB approaches.
SS13/13 'Market risk'	States that risk management functions should be aware of weaknesses of the models. The SS also sets out the expectation that the firm should demonstrate compliance

Regulations/rules/ guidance/principles	Comment
	with the risk management standards set out in CRR. Specifically **Article 368**, which requires firms to complete an annual review of its overall risk management process and sets out the qualitative requirements in regards to the governance of internal models; Such as having sufficient numbers of skilled staff, and states the procedures for monitoring, testing and review of the models. Furthermore, the SS set out the expectation that appropriate individuals in a Significant Influence Function (SIF) role should provide written attestation that the firm's internal approaches for which it has received a permission comply with the requirements in Part 3 Title IV of the CRR, and any applicable market risk supervisory statements to the PRA on an annual basis. The SS is applicable to firms to which CRD IV applies and sets out the PRA's expectations of firms in relation to market risk. It should be considered in addition to requirements set out in Articles 325–377 of the CRR and the Market Risk Part of the PRA Rulebook.
SS5/18 'Algorithmic trading'	States that the PRA expects the governance framework for algorithmic trading to define lines of responsibility for the review and approval process for algorithms, and the ownership of controls. It also states that the firm should identify a senior management function who will have responsibility for the algorithmic trading. The PRA expects the firm's board to have, and maintain, an understanding of the firm's algorithmic trading and the risk controls viewed as most important to mitigate and contain the risks from algorithmic trading. The SS is applicable to firms that engage in algorithmic trading, and are subject to the rules in the Algorithmic Trading Part of the PRA Rulebook and Commission Delegated Regulation (EU) 2017/589.

Regulations/rules/ guidance/principles	Comment
SS12/13 'Counterparty credit risk'	Specifically references CRR Article 286(4) in terms of governance. Article 286(4) of the CRR states that firms using the Internal Model Method must have a formal process in which senior management are made aware of the limitations and assumptions of the model, and the impact of these on the reliability of the model output. With further requirements on policies and processes of internal models being set out in Article 286: management of CCR — Policies, processes, and systems. (Listed under section 6: Internal Model Methods, of chapter 6: Counterparty credit risk, of Regulation (EU) No 575/2013). The PRA sets out an expectation that an appropriate individual in a SIF should provide the PRA with an annual attestation that the firm's internal approaches (for which it has received a permission) comply with the requirements in Part 3 Title II of CRR, and any appropriate PRA counterparty credit risk supervisory statements. This SS is applicable to CRR firms.
SS17/16 'Solvency II: internal models – assessment, model change and the role of non-executive directors'	Sets out the PRA's expectations regarding the role of non-executive directors (NEDs) when considering a firm's internal model. The PRA expects members of the board to understand and have the ability to explain key areas of the model; such as key strengths and limitations and assumptions and judgements. It also states that firms should be able to produce clear evidence showing how boards are overseeing the validation process and how the boards are involved in tracking validation issues through to resolution. Furthermore, the PRA generally expects firms' executive management to be responsible for the internal sign-off of major model changes and at least to be made aware of minor changes where appropriate. Prior to application to the PRA for the approval of the model, firms must ensure their applications are stable and approved by their internal governance processes. Further policies and procedures surrounding internal models are also set out within the

Regulations/rules/ guidance/principles	Comment
	Solvency Capital Requirement - Internal Models part of the PRA rulebook.

Table G: Robust model development and implementation process

Regulations/rules/ guidance/principles	Comment
SS3/18 'Model risk management principles for stress testing'	Looks at the development of the model, use of data in the development and the underlying assumptions/ judgments made. The SS states an expectation, in relation to models, that there should be appropriate testing, any uncertainties should be adequately understood, and they should be monitored periodically. Furthermore, it states that firms should ensure they have sufficiently detailed model documentation, so that an independent third party with relevant expertise is able to understand how the model operates. The SS is applicable to PRA authorised banks, building societies, and PRA-designated investment firms.
SS11/13 'Internal Ratings Based (IRB) approaches'	Includes specific expectations on how IRB models should be developed. Focusing on the estimation, documentation of models' input parameters, and functional forms, in order to deliver a particular result. This SS gives further information on how assessment is made for compliance with CRR Article 174, which on its own is very broad in the context of model development. It lists attributes that should be met within the model development stage such as the model should not have material biases, the inputs into the model should be accurate and complete, the data used to build the model must be representative of the institution's population of actual obligors or exposures, and how human judgement and model results are to be combined. The SS is applicable to firms to which CRR applies.

Regulations/rules/ guidance/principles	Comment
SS13/13 'Market risk'	Lists specific expectations regarding how models should calculate capital requirements for market risk are developed. It sets out the PRA's expectations of firms in relation to market risk (including data standards and how a firm should demonstrate that it meets the risk management standards set out in **Article 368** of the CRR). Furthermore, **CRR Article 367** of the CRR sets out the attributes an internal model is required to have when used to calculate capital requirements for position risk, foreign exchange risk, and commodities risk. The SS is applicable to those firms to which CRD IV applies. The SS should be considered alongside the requirements set out in Articles 325–377 of the CRR, and the Market Risk Part of the PRA Rulebook.
SS5/18 'Algorithmic trading'	Focuses on the testing and deployment of the algorithms. It sets out expectations of the relevant functions and the role they have in ensuring that the automated risk controls operate as intended, such as authorising the design of tests and signing off the results of such tests. Further expectations are set out in regards to the competency of the testing team and specific assessments in regards to the algorithmic trading system, as well as inventories and documentation. The SS applies to firms that engage in algorithmic trading and are subject to the rules in the **Algorithmic Trading Part of the PRA Rulebook**, and **Commission Delegated Regulation (EU) 2017/589**.
SS12/13 'Counterparty credit risk'	Sets out the expectations regarding specific factors/calculations to be taken into account within counterparty credit risk models. The high-level expectations set out regarding the development of the models are mainly concerned with assumptions and limitations. It states that highly conservative modelling assumptions should be used, and that a process is expected to be in place for estimating the potential impact that limitations and assumptions may have on the key model outputs of exposure and capital requirements. Furthermore, it states that the impact of a

Regulations/rules/ guidance/principles	Comment
	model assumption should be assessed relative to plausible alternative assumptions. This SS is applicable to CRR firms.
Solvency II and **Solvency Capital Requirement - Internal Models**	Covers a broad range of requirements in regards to insurers' internal models, addressing specific criteria for the risks covered by the model and the method of calculation. It sets out statistical quality standards for calculations, such as the need for underlying assumptions within the model to be justified and data used within the model to be accurate, complete, and appropriate. It further states the expectation for documentation and how it should provide a detailed outline of the theory, assumptions, and mathematical and empirical bases underlying the internal model.
FRTB Basel Standards	The framework introduces a more robust process for assessing whether individual risk factors can be deemed as 'modellable' by a particular bank. After determining which risk factors within the identified desks are eligible to be included in the bank's internal models for regulatory capital. A risk factor's eligibility for modelling is determined by evaluating the relative quality of the data based on factors such as availability of historical data and the frequency of observations.

Table G: Model validation and independent review

Regulations/rules/ guidance/principles	Comment
SS3/18 'Model risk management principles for stress testing'	States that all model components should be subject to independent valuation. Any validation work undertaken by model developers and users as well as any material changes to already validated models or overlays should be subject to review by an independent party. The nature and extent of validation and independent review should be appropriate with the overall use, complexity, and materiality

Regulations/rules/ guidance/principles	Comment
	of the models, model components, adjustments to model results, or changes to a model.
SS11/13 ‘Internal Ratings Based (IRB) approaches’	Sets out PRA expectations that firms will have a validation process that includes standards of objectivity, accuracy, stability and conservatism, accuracy of calibration, and discriminative power that it designs its rating systems to meet and processes that establish whether its rating systems meet those standards. Further expectations are detailed in respect to the validation process itself and the types of evidence that are expected. The SS also makes reference to **CRR Article 185** which further lays out the requirements firms need to meet to validate their internal estimates, such as the requirement to assess over a long period of time and analysis or use of appropriate data.
SS13/13 ‘Market risk’	Specifically states a firm should be able to demonstrate that it meets the risk management requirements set out in **CRR Article 368**; where it is stated that an institution shall conduct an independent review of its internal models.
SS5/18 ‘Algorithmic trading’	Sets out that the PRA expects a firm to have an algorithm trading policy which, at a minimum, should outline the testing and validation process for algorithmic trading, including who has responsibility for these activities. The PRA expects the testing and validation process to have a clear scope and purpose, and for firms to confirm the prioritisation and frequency with which testing and validation should be undertaken.
SS12/13 ‘Counterparty credit risk’	Covers model validation and states that quantitative models should be reviewed by an independent team, with a degree of rigour proportional to materiality.
SS17/16 ‘Solvency II: internal models – assessment, model	Sets out the PRA’s expectations for validating internal models. With the review aspect to be clearly documented and to focus particularly on key assumption and expert

Regulations/rules/ guidance/principles	Comment
change and the role of non-executive directors' and **Solvency Capital Requirements – Internal Models 14**.	judgements and the sensitivity/ material impact of these. It also states that models should be validated on a regular cycle and measure performance, with an assessment of accuracy completeness and appropriateness of data used.

Appendix 5 – List of selected relevant publications

Table H: Surveys and reports on the use of AI in financial services

Title	Author	Date
Machine learning in UK financial services	The Bank and FCA	2022
The final report of the AI Public Private Forum	The Bank and FCA	2022
Implementation of fairness principles in financial institutions' use of AI	MAS	2022
CFPC 2022-03: 'Adverse action notification requirements in connection with credit decisions based on complex algorithms'	Consumer Financial Protection Bureau ('CFPB')	2022
Proposed revision to guideline E-23 on model risk management	Office of the Superintendent of Financial Institutions ('OSFI')	2022
AI and Big Data	European Insurance and Occupational Pensions Authority ('EIOPA')	2022
OECD Framework for the classification of AI systems: a toll for effective AI policies	OECD	2022
AI in Business and Finance	OECD	2021
AI Barometer	CDEI	2021
AI in Financial Services	The Alan Turing Institute	2021
AI governance principles: towards ethical and trustworthy AI in the European insurance sector	EIOPA's Consultative Expert Group	2021

Title	Author	Date
Request for information and comment on financial institutions' use of AI, including machine learning	Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the CFPB and the National Credit Union Administration	2021
Big data and AI: principles for the use of algorithms in decision-making processes	Bundesanstalt für Finanzdienstleistungsaufsicht ('BaFin')	2021
Discussion Paper on machine learning for IRB models	European Banking Authority ('EBA')	2021
The impact of Covid on machine learning in UK banking	The Bank	2020
Transforming Paradigms: A global AI in Financial Services Survey	Cambridge Centre for Alternative Finance and World Economic Forum	2020
AI Barometer	CDEI	2020
Report on Big Data and Advanced Analytics	EBA	2020
Machine learning in UK financial services	The Bank and FCA	2019
Recommendations of the Council on Artificial Intelligence	OECD	2019
Big data meets AI	BaFin	2018
FEAT Principles Final	MAS	2018
Artificial intelligence and machine learning in financial services	Financial Stability Board	2017

Table I: Publications that may be relevant to data use in AI

Principles/regulation/guidelines	Source
FCA Handbook – Article 18: Data quality	FCA
Ring-fencing	PRA
Solvency II	PRA
UK Data Protection Act 2018 (GDPR)	UK Government
The Payment Services Regulations 2017	UK Government
Payments Service Directive 2 (PSD2)	European Union
Markets in Financial Instruments Directive (MiFiD II)	European Union
Principles for effective risk data aggregation and risk reporting (BCBS 239)	BCBS
Corporate governance principles for banks (BCBS 328)	BCBS
Principles for Financial Markets Infrastructures (PFMI)	BCBS

Table J: Publications with relevant model risk principles and guidelines

Principles/regulation/guidelines	Source
SS3/18 ‘Model risk management principles for stress testing’	PRA
SS11/13 ‘Internal Ratings Based (IRB) approaches’	PRA
SS13/13 ‘Market risk’	PRA
SS5/18 ‘Algorithmic trading’	PRA

Principles/regulation/guidelines	Source
SS12/13 'Counterparty credit risk'	PRA
Solvency II	PRA
SS17/16 'Solvency II: internal models – assessment, model change and the role of non-executive directors'	PRA
Guidelines on the management of interest rate risk arising from non-trading book activities	EBA
Fundamental review of the trading book: A revised market risk framework (FRTB)	BCBS

Table K: Publications that may be relevant to governance of AI

Principles/regulation/guidelines	Source
FCA Handbook – SYSC System and Controls	FCA
SS21/15 'Internal governance'	PRA
SS5/16 'Corporate governance: Board responsibilities'	PRA
SS28/15 'Strengthening individual accountability in banking'	PRA
SS35/15 'Strengthening individual accountability in insurance'	PRA
SS2/21 'Outsourcing and Third Party Risk Management'	PRA
PRA Rulebook – General Organisational Requirements 2.1	PRA

Principles/regulation/guidelines	Source
Corporate governance principles for banks (BCBS 328)	BCBS