Key themes of resiliency, outsourcing and third-party risk management regimes

Received (in revised form): 13th September, 2024

Mike Pierides*
Partner, Morgan, Lewis & Bockius, UK

James Mulligan**
Associate, Morgan, Lewis & Bockius, UK

Mike Pierides

James Mulligan

Morgan, Lewis & Bockius UK LLP, Condor House, 5–10 St Paul's Churchyard, London EC4M 8AL, UK

**Tel: +44 (0)203 201 5686; Mob: +44 (0)7894 095334; E-mail: mike.pierides@morganlewis.com*

***Tel: +44 (0)203 201 5496; E-mail: james.mulligan@morganlewis.com*

Journal of Securities Operations & Custody
Vol. 17, No. 2, pp. 102–118
Henry Stewart Publications, 1753-1802

Mike Pierides *leads Morgan Lewis's technology transactions, outsourcing and commercial contracts practice outside the US. His practice encompasses a wide breadth of commercial and technology transactions. Mike advises on major outsourcings, strategic restructurings following divestments or acquisitions, and technology-specific transactions such as licensing and 'as-a-service' arrangements. He is also active advising on new technologies such as artificial intelligence and blockchain.*

James Mulligan *advises multinational clients on technology transactions, outsourcing and commercial contracts. His practice encompasses a broad spectrum of financial services transactions, complex information technology and business process outsourcings and technology-specific transactions, such as licensing and 'as-a-service' arrangements. James has experience in highly regulated industries and has completed secondments to a global financial institution and a leading technology and financial services business.*

ABSTRACT

Throughout 2024, European Union (EU)-based financial entities have been analysing their third-party and intra-group technology contracts against compliance with the EU Digital Operational Resilience Act (DORA), and renegotiating with vendors where necessary, in order to comply from 17th January, 2025. McKinsey estimates that EU institutions typically earmarked €5–15m for DORA programme strategy, planning and design, although full implementation costs may be five to ten times that range.[1] The DORA analysis is also highlighting that certain companies are not compliant with existing regulatory expectations. Financial regulators and global standard-setting bodies have published high-level principles and also detailed expectations to ensure that companies have in place prudent third-party risk management controls, both at an enterprise level and for managing individual third-party arrangements. As securities markets participants become increasingly reliant on third-party service providers for tasks that they had not previously undertaken, leveraging technology and artificial intelligence (AI), supervisory focus is extending to operational resilience across third-party services relationships, not just outsourcing. In this paper, we explore key themes of existing outsourcing and third-party risk management regimes that apply to financial entities and their service providers. We note key differences between regulatory expectations on resiliency and outsourcing, highlight key best practices and challenges to implementing these expectations and, finally, consider the impact of AI solutions on such regulatory expectations.

Keywords: operational resilience, artificial intelligence, outsourcing, digitisation, financial regulation

DOI: 10.69554/AUIQ5402

SCENE SETTING

Key definitions

Outsourcing refers to an arrangement under which a service provider performs a task,

function, process or service that would otherwise be undertaken by the customer.[2] Outsourcing may be used in order to better manage costs, reduce risks of keeping a function in-house that a company is not fully equipped to perform, facilitate process automation and scalability and ultimately improve efficiency. In the context of over-the-counter derivatives, for example, commonly outsourced tasks include trade matching and confirmation, portfolio reconciliation, collateral management and trade reporting.[3] Services that a customer could not realistically undertake itself are generally not considered to be outsourcing, such as custody arrangements (due to regulatory obligations), market information services or discreet advisory services.

Operational resilience refers to the ability to deliver critical operations through disruption.[4] This involves identifying and protecting from threats and potential failures, responding and adapting to and recovering and learning from disruptive events. A securities market participant that is ill equipped for any of those tasks is potentially a risk to other market participants and consumers and could cause instability in the financial system. Cyber security is one component of resilience, but so too are operationally disruptive factors such as a pandemic, geopolitical risks and shifting work patterns to hybrid working.

Operational resilience covers a range of services, whether or not an organisation could have undertaken those services itself — a key difference to outsourcing — and European Union (EU) regulation focuses particularly on information and communication technology (ICT) services.

Why prudent third-party risk management matters

In February 2024, the European Central Bank (ECB) published data indicating that more than 10 per cent of outsourcing contracts covering critical functions of 109 EU-based financial institutions self-reported that they were not compliant with existing regulatory expectations.[5] Of those non-compliant contracts, the ECB found that over the last three years 20 per cent had not been subject to a proper risk assessment and 60 per cent had not been audited. The ECB cited this as a sign that insufficient consideration is given to outsourcing risks and signalled that outsourcing and resiliency will be a top priority on its supervisory agenda moving forward.

Regulators have taken enforcement action for deficiencies in third-party risk management controls. In the UK, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) have levied significant fines for outsourcing failures, including over £48m relating to an IT upgrade programme[6] and nearly £2m for deficiencies regarding business continuity and disaster recovery procedures.[7] The Central Bank of Ireland levied over €10m against a fund administration provider for outsourcing failures, in particular citing deficient record keeping and failures in appropriate checking of net asset value (NAV) calculations before a final NAV was released to the market.[8] These are just a few examples.

OVERVIEW OF KEY THEMES IN OUTSOURCING AND THIRD-PARTY RISK MANAGEMENT REGIMES

Regulatory convergence

Across key jurisdictions for global securities markets, regulatory expectations around outsourcing and third-party risk management have converged on certain themes, which are set out further below. Many of these themes are found in the 'Principles on Outsourcing' (Principles) maintained by the International Organization of Securities Commissions (IOSCO), an international policy forum for securities regulators whose membership regulates more than 95 per cent of the world's securities markets. IOSCO's

Principles were most recently revised in September 2021 and their application was expanded to include trading venues, market intermediaries and market participants acting on a proprietary basis, and regulated credit rating agencies.

Regulatory guidance from the following key jurisdictions is also converging on these themes:

- *EU*: The European Banking Authority's Guidelines on Outsourcing Arrangements[9] (EBA Outsourcing Guidelines) set the most commonly referenced expectations for outsourcing arrangements in the EU. Storage of data in cloud environments has reshaped the information technology landscape of financial services, including securities markets. The European Securities and Markets Authority (ESMA) has published Guidelines on Outsourcing to Cloud Service Providers,[10] which detail its expectations for securities markets participants and similarly align with many of the themes of the EBA Outsourcing Guidelines. Regulators from EU member states including Luxembourg,[11] Ireland[12] and Germany[13] have published further guidance implementing these EU-wide expectations. At the time of writing, the ECB is consulting on publishing its own expectations for banking institutions outsourcing to cloud service providers, which are intended to overlay the EBA Outsourcing Guidelines and DORA.[14]
- *UK*: The PRA's supervisory statement (PRA SS2/21), applicable to banks and PRA-designated investment companies (among others), modernised UK regulatory expectations of outsourcing and third-party risk management and broadly aligned them with the EBA Outsourcing Guidelines. The FCA Handbook contains requirements and guidance around outsourcing by entities under its supervision.[15]
- *US*: In June 2023, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency jointly published their Interagency Guidance on Third-Party Relationships: Risk Management[16] (US Interagency TPRM Guidance), which sets out sound risk management principles for banking organisations at all stages in the life cycle of third-party relationships. This guidance is used by many non-banking financial entities as a reference framework and applies to all third-party relationships, not just outsourcing. It is also worth noting that in August 2021 the Financial Industry Regulatory Authority, Inc. (FINRA) published Regulatory Notice 21-29[17] (RN 21-29) to 'remind' of various obligations when outsourcing functions to third-party vendors, covering many of the key themes highlighted below.

Financial regulators in jurisdictions such as the Cayman Islands,[18] Singapore[19] and Hong Kong[20] have also recently updated their guidance around outsourcing by regulated entities, addressing the same key themes to varying degrees.

It is worth noting that the applicable regulatory regime will generally be that of the jurisdiction of the regulated service recipient. Some financial groups may centralise receipt of external services through a single 'service' entity (eg within a specific EU member state), which then provides services onwards on an intra-group basis (which in and of itself attracts a lower risk profile). This enables an organisation to centralise its compliance and third-party risk management functions through the service entity.

Key themes from an operational perspective

From an enterprise-wide perspective, the following key themes emerge:

(1) *Governance*: Organisations are generally expected to have in place a holistic,

enterprise-wide risk management governance framework that joins together key controls around compliance, legal, information security, procurement and operational risk. The structure of third-party risk management processes may vary — some are dispersed among business lines, while other organisations rely on centralised processes managed by compliance, information security, procurement and/or risk management functions — and it is essential that each process works together in order to ensure effective oversight and accountability (as noted below) and proper documentation of third-party risks.

(2) *Resiliency and business continuity*: Resiliency is a common theme within outsourcing regimes; regulators expect regulated entities to establish procedures and controls to ensure business continuity in the event of disruption and to protect proprietary and client-related information to which any outsourcing provider has access.[21] Good practices include maintaining protocols in the event of cyber incidents, timeframes for recovery of data, regular testing and back-up facilities and, critically, addressing these requirements in the contract with the third-party provider and flowing them down to its delegates as appropriate.

(3) *Oversight and accountability*: While this is not one of IOSCO's Principles, ensuring effective accountability for outsourced functions is a key theme throughout many regulatory regimes. In the UK, the PRA expects that companies' boards should 'bear responsibility for the effective management of all risks to which the firm is exposed including by appropriately identifying and [having an] understanding of the firm's reliance on critical service providers'.[22] In addition, under the UK Senior Managers and Certification regime, companies must allocate to a senior manager a prescribed responsibility for regulatory obligations relating to outsourcing.[23] The PRA expects management information on outsourcing to be clear, consistent, robust, timely and well targeted. The US Interagency TPRM Guidelines similarly expect banking organisations' boards of directors (or a designated board committee) to hold management accountable for implementing third-party risk management policies and procedures consistent with the bank's strategic goals and risk appetite, and for taking appropriate action to remedy significant deterioration in performance.[24] The EBA Outsourcing Guidelines contain similar expectations and require firms to maintain a register of all outsourcing arrangements, which is made available to national regulators upon request. This data is fed up to the ECB.[25]

(4) *Assessing criticality of services*: Regulatory expectations are generally segmented according to the materiality or criticality of the relevant service or outsourced task to the regulated entity's ongoing business or regulatory obligations. For material outsourcings, regulators typically expect greater due diligence, oversight and more extensive contractual protections. In the EU and the UK, the criticality of each outsourcing arrangement should be assessed and criteria include whether internal control functions are outsourced, the ability to substitute or reintegrate the function, or whether, in the event of a failure in performance of the outsourced task, the regulated entity would be unable to deliver core services to its clients or continue to meet regulatory obligations. Within securities operations, potential threats to the operation of clearing and settlement systems or the quality of the credit rating process are examples of critical factors. The US

Interagency TPRM Guidance highlights that banking organisations may approach criticality differently: some may assign criticality or risk level to each third-party relationship, whereas others may identify critical activities of the bank itself and, then, third parties that support such activities. Many regulated entities have a dedicated third-party risk management function whose responsibilities include assigning critical outsourcings. All regulators highlight that criticality may vary over time and, in the authors' experience, it is important that stakeholders from risk management, legal and compliance teams are each involved in formulating changes to an organisation's internal criticality criteria; changing this scope could significantly change a firm's contracting procedures and notifications that it submits to regulators.

(5) *Planning and due diligence*: Regulators generally expect companies to be satisfied and to provide evidence that the outsourcing provider has the ability and capacity to undertake the outsourced task effectively at all times. Due diligence includes assessing, prior to selection, the impact of a sudden interruption of service and the availability of alternative service providers; becoming locked into a specified provider's technological or operational platform is a key risk for business continuity and operational resilience. Regulators expect companies to put in place documented selection processes, assess concentration risk and, in the UK and EU, notify the supervisory authority before entering into or significantly changing a material outsourcing arrangement. Well-documented due diligence procedures may prove critical in the event of a supervisory inspection and can save significant time and resource if third-party arrangements require reassessment, possibly in the event of a restructuring of service recipients or corporate acquisition. It is worth noting that some organisations use a single platform to process planning, diligence and small and medium-sized enterprise (SME) approvals, and such solutions may themselves constitute a critical service.

(6) *Security and privacy*: Preserving the security and confidentiality of data is critical within securities operations, as unauthorised disclosure of business-sensitive or client information could pose harm to clients and investors, damage a regulated entity's reputation, or cause instability in financial markets.[26] Storage of data in cloud environments has reshaped the IT landscape of financial services and, as noted above, certain regulators have published regulatory guidance specifically on outsourcing to the cloud. Regulators expect companies to fully assess a provider's information security programme and to remain informed of any emerging threats and vulnerabilities, for which incident reporting is a key factor. Certain regulators mandate contractual obligations which specify reportable incidents, reporting timelines and details that need to be reported.[27]

(7) *Exit strategies*: Most outsourcing arrangements involve to varying degrees the loss of operational control, data and expertise for the outsourced function. Regulators generally expect companies to formulate strategies for managing the transfer of the task back to the company in the event of termination and clarity over who owns the relevant data, documented in a written contract (although, as IOSCO explains, the written contract and exit strategies should be viewed as separate concepts[28]).

(8) *Contractual arrangements*: Most regulators expect companies to have in place contract terms covering specific key issues, proportionate to the risks, size and complexity of the outsourced services.[29] These key issues are explored

further below. While market standard terms have developed to an extent, outcomes remain dependent on the parties' negotiating power. For example, certain dominant providers typically have the leverage to limit the audit rights they give and, as a consequence, outsourcing providers that utilise them may resist certain conditions for sub-outsourcing; and, as a consequence, outsourcing providers that utilise them may resist certain conditions for sub-outsourcing; on the other hand, regulated financial entities with greater leverage in negotiations may push for remedial measures that go beyond the regulatory requirements. Regulatory approaches towards non-compliance with the contractual requirements vary: the UK PRA is one of the few regulators that expects regulated entities to make it aware if a material outsourcing provider is unable or unwilling to agree to the specified contract terms. Regulators in the EU expect to be made aware as part of the annual submissions of outsourcing registers.

It is worth noting that custody services are generally deemed to be non-outsourcing where the appointment of an independent third party is mandated by law. In the EU and the UK, requirements for custody arrangements under the Alternative Investment Fund Managers Directive (AIFMD) regime and the rules for undertakings for collective investment in transferable securities (UCITS) specify operational controls, policies and procedures and contractual terms as between the regulated company and custodian. There is some alignment with the contractual themes discussed below, such as requiring specific termination rights and information and access rights for the regulated entity, and in other areas those requirements are service-specific, such as imposing strict liability on the provider for loss of a financial instrument in custody.

Key themes from a third-party risk management perspective

Prudent risk management through the written agreement between the regulated entity and the service provider is a central pillar of many outsourcings and third-party risk management regimes. As to the form of agreements, there is no 'one size fits all': agreements vary from detailed framework agreements with individual statements of work per service towers to standard-form agreements which may attach financial services-specific outsourcing terms.

Regulators generally expect contracts to address the following:

- *Performance standards and oversight*: Regulators expect agreements to define performance standards, which may involve both quantitative and qualitative service levels and associated incentivisation mechanisms, as well as appropriate monitoring tools. These are inevitably a focus of negotiation and are service-specific.
- *Sub-outsourcing or delegation*: Regulators generally expect a company to specify any conditions that must be met in order for the service provider to delegate its performance of critical functions and obligations to disclose any material changes to such delegation. Pre-approval may not always be appropriate, however, and during negotiations, the parties may agree on categories of subcontractors to which delegation would be permissible on a pre-approved basis; for example, those which do not involve processing any customer data might be pre-approved, whereas delegation of any service which has a client-facing component might be subject to a regulated customer's pre-approval. Alternatively, a company may be entitled to receive a long notice of additional delegation and the right to terminate the contract or relevant service if it does not agree with the provider's proposal; this approach is

solution-specific and, for example, it may not be practical for multi-tenant cloud environments. Any sub-outsourcing must typically flow down the prime contract's terms to the subcontract. In the EU, it is worth noting that the EBA Outsourcing Guidelines defines 'sub-outsourcing' as subcontracting all or a material part of the outsourced function or service, and not simply any part thereof. Delegates and sub-processors (ie any entity that processes data on behalf of the service provider) are not always the same and may be treated separately in the contract in order to maintain flexibility. One key challenge is that some service providers may not have end-to-end visibility of which services and/or clients are supported by each of its third-party subcontractors, making it difficult to comply with certain disclosure requirements.

- *Service locations*: Regulators typically expect regulated entities to be informed of all locations from which services will be provided and, if relevant, where data will be kept and processed. This can create tension between transparency for the customer and flexibility for a provider to make changes to its services model. A balanced approach may specify regions of service delivery and data location, within which the service provider does not require further notices to the customer, unless the regulated entity is focused on a particular location or geography as part of its preferred risk profile. Where that is the case, then similarly to delegation restrictions this may be framed as a right to be notified and to terminate the relevant service being delivered or supported from that jurisdiction, with appropriate termination assistance from the provider. From the regulated customer's perspective, it is worth noting that most regimes do not mandate any particular location from which the customer's oversight must be undertaken.
- *Access and audit rights for the regulated entity and its regulator(s)*: The right to audit a service provider's performance is integral to policing performance. Key negotiating issues include frequency, cost allocation, type of audit reports and physical access to facilities. In the EU, in the case of material outsourcings, the audit right must be 'unrestricted' and require full access to relevant business premises, although this is often balanced with an understanding that the service provider should not breach any confidentiality obligations owed to third parties.
- *Cooperation with regulators*: Regulators generally expect a regulatory cooperation obligation to be expressed in the agreement, tying into information and access rights. There is little to no specific guidance regarding the extent of the expectation, however, and some providers may push for a negotiated outcome, ie a customer can be responsible for cost of cooperation and/or cooperation being bound by reasonableness.
- *Reporting obligations*: Reporting obligations are service-specific to the governance arrangements between the parties. From a customer's perspective, the regulated entity must ensure that it receives all information that it is obligated to report to its supervisors about the third-party arrangement.
- *Accessibility and availability of data*: Regulators generally expect the agreement to require that data owned by the regulated entity can be accessed in the event of insolvency of discontinuation of the service provider's business operations. These are fairly typical contractual requirements with which customers and service providers will be familiar.
- *ICT and data security standards and incident handling procedures*: As securities markets and operations become increasingly digitalised, ICT security specifications, testing requirements and incident handling have

become critical, particularly in how these are flowed down to subcontractors. Regulatory expectations have led to providers developing more detailed ICT security policies and, in some cases, regulated entities insist on the application of their own security policies. Key negotiation points include whether a customer has a right to conduct penetration testing, notification timeframes, incident categorisation and information formats.

- *Business continuity planning*: Contracts are generally expected to address the third-party provider's responsibility for maintaining business continuity plans, including providing specific recovery time and recovery point objectives. Contractual rights of step-in by a regulated customer, in the event of major service disruption, is not generally mandated and appropriateness may be service-specific; instead, a form of enhanced cooperation obligations is increasingly requested by regulated financial entities.
- *Customer complaints*: Regulators generally expect the contract to specify whether responsibility for responding to and/or resolving customer complaints falls on the regulated entity or the service provider. Where the regulated entity is responsible, it is important that it receives prompt notification and assistance from the provider.
- *Insurance*: Whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested. These are fairly typical provisions and achieving a contractual outcome to each party's satisfaction should not be a significant challenge.
- *Termination rights*: Many regulatory regimes specify termination triggers that are expected to be included in the written agreement, and each includes its own scope for negotiation. For example, under the EBA Outsourcing Guidelines: (a) where the provider is in breach of applicable law is a standard termination right, although providers may seek to build in material breach standards and, where appropriate, periods for rectification; (b) impediments capable of altering performance of an outsourced function, for which a provider could also seek to apply a material breach threshold — however, customers may insist upon the anticipatory nature; (c) material changes affecting the outsourcing arrangement or service provider, such as undue sub-outsourcing; and (d) upon instruction by a supervisory authority.
- *Exit assistance*: Upon termination of the arrangement, service providers are generally expected to facilitate the transfer of the outsourced function to another service provider or its reincorporation into the institution or payment institution. Exit support is a standard expectation in outsourcing arrangements, rather than cloud arrangements where exit services will typically be much more limited given the nature of the solution and the extent of the services. Depending on the context, regulated entities may push for extensive exit support extending to, for example, collocation or extensive knowledge transfer, which can be burdensome on a provider at the end of a relationship but potentially justified. This may come down to how much a provider would charge for the same.

The above list is not exhaustive and jurisdiction-specific guidance addresses additional areas. For example, the US Interagency TPRM Guidance notes that in order to prevent disputes between the parties regarding ownership licensing of a bank's property, it is common for a contract to address the service provider's use of the bank's intellectual property and, specifically, whether any data generated by the service provider becomes the bank's property.

Increasing focus on operational resilience

Increasingly, many of the above expectations are being extended to all third-party service relationships, not just outsourcing, as financial regulators emphasise the importance of operational resilience throughout supply chains.

This is in part because the types of technologies or functions that form part of a company's services have changed and companies are increasingly reliant on third-party service providers for tasks that they had not previously undertaken. The global disruption in July 2024 arising from a defective update to widely used security software, crashing computers across multiple industries, highlights the operational dependence on ICT systems and the performance of so-called 'nth-party' service providers; notably, this disruption was not caused by malware or a similar malicious attack.

Another factor is the extreme market volatility and amplified trading activity during the COVID-19 pandemic, which placed significant strain on critical functions of regulated entities within securities markets, among other industries.[30] For example, in post-trading processing, market intermediaries reported increased fail volumes in settlements and the Depository Trust & Clearing Corporation (DTCC) reported in its 2020/21 survey that 58 per cent of sell-side companies experienced challenges in settlement and payments during peak volatility in 2020.[31] Broader shifts in working patterns and workforce attrition have also focused regulators' minds on ensuring that companies are operationally resilient to disruptions.

Cyber security is one key pillar, and legislators and regulators are increasingly active in this regard,[32] but as the examples above demonstrate, operational resilience is not specific to cyber security.

In December 2023, another global standard-setting body relevant to securities markets participants, the Financial Stability Board (FSB), published 'Enhancing Third-Party Risk Management and Oversight'.[33] This is a toolkit for financial institutions and financial authorities that looks holistically at third-party risk management, wider than just outsourcing, and highlights key themes from recent regulatory approaches towards operational resilience. Most of the 'tools' highlighted by the FSB align with the themes identified above — criticality of services, due diligence and ongoing monitoring, exit strategies and business continuity planning — and others receive greater emphasis in the context of operational resilience — mapping of service relationships, use of service supply chains and incident reporting.

The US Interagency TPRM Guidance has been ahead of others in this regard, applying its expectations to all third-party relationships of relevant entities, and in March 2024 the acting US Comptroller of Currency indicated in a speech that new regulations aimed specifically at strengthening baseline operational resilience for larger depository institutions may be forthcoming.[34] In the UK, the FCA and PRA have published rules that require financial services companies to identify important business services, map processes, set impact tolerances and test under different scenarios,[35] and both have been granted statutory powers to directly oversee critical third-party service providers who pose risks to the stability of the UK financial system in the event of a failure in, or disruption to, their services. The FCA and PRA are jointly consulting on proposed minimum resilience standards and fundamental principles that they would enforce against such critical third parties under their new statutory powers.[36]

EU DORA

DORA establishes a comprehensive legislative framework designed to strengthen EU financial entities' operational resilience by

ensuring prudent risk management of a broad array of ICT services, including all of a regulated entity's cloud, software-as-a-service (SaaS), digital data and IT infrastructure arrangements. Beginning on 17th January, 2025, financial entities based in the EU must have in place processes and policies, as well as mandatory contract provisions with their third-party technology vendors, that comply with DORA.

DORA applies to financial institutions, investment companies, fund management companies and other regulated financial entities based in the EU.

Mandatory contract provisions

DORA extends many of the same contractual requirements contained in the EBA Outsourcing Guidelines to all contracts with third-party ICT service providers, both intragroup and external, albeit with some additions, as noted in Figure 1.

Key differences between DORA and existing EU outsourcing regulatory regimes

Many of the outsourcing regimes noted above include the same concepts (such as assessing criticality) and require similar, if not the same, contract terms for outsourcings that support critical or important functions as those listed above. There are additional requirements under DORA, however, that will likely create gaps between compliance with existing outsourcing regulatory regimes and compliance with DORA.

The key gaps between DORA and those existing regimes are as follows:

(1) *The scope of ICT services is broader under DORA*, extending beyond services that the financial entity could otherwise undertake itself, eg digital data subscription services, SaaS, certain software licensing.
(2) *All contracts for ICT services must contain mandatory contractual provisions under DORA*, not just those supporting critical or important functions. This will require remediating certain contracts that may have fallen outside of outsourcing contract remediation projects as well as amending contracting procedures for ICT services going forward.
(3) *There are additional mandatory contract provisions*, such as participation by the ICT services provider in the financial entity's digital operational resilience training, providing assistance with ICT incidents at no additional cost (or at a cost determined *ex ante*) and supporting adherence to the ICT security standards and business continuity planning requirements under DORA. In respect of ICT services supporting critical or important functions, there are more extensive provisions under DORA in respect of subcontracting such services.
(4) *A separate policy must be adopted addressing compliance with the contractual requirements for third-party ICT services supporting critical or important functions*, in addition to maintaining a register of all third-party ICT services arrangements (similar to the register of material outsourcings).

In certain instances, financial entities may themselves act as an ICT service provider, such as where they provide platform solutions to other financial institutions as their customers. For example, where a bank provides a portfolio management platform to investment companies, it would be a service provider of ICT services (and likely supporting critical functions), while having its own vendor relationships. This will affect how regulatory expectations will fall, the contractual positions they take with customers, and the policies and procedures they must have in place.

Key considerations for contract remediation

Financial entities already subject to, and compliant with, the existing EU outsourcing

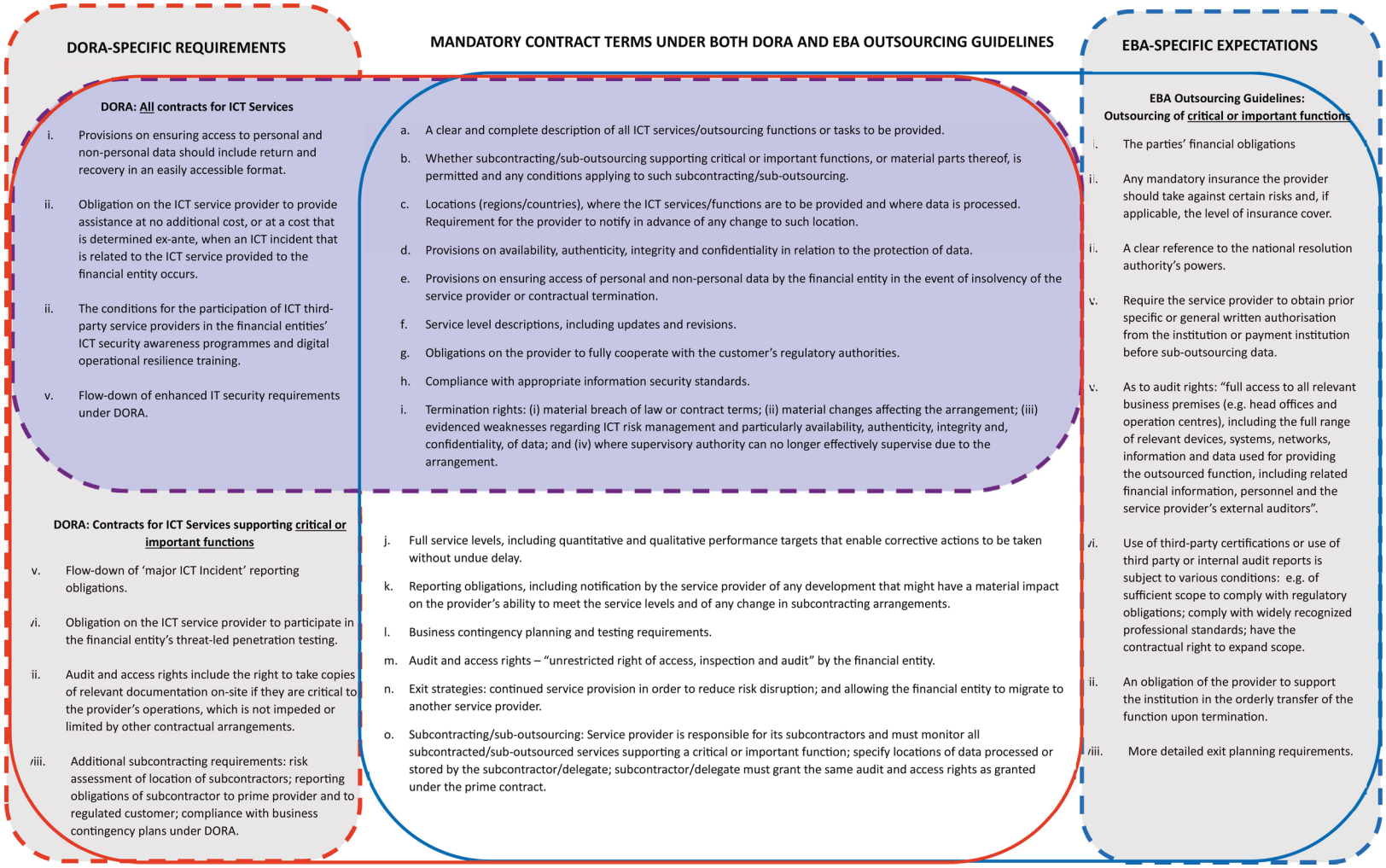

Figure 1 Mandatory contract terms

regulatory regimes have been undertaking a contract remediation process to close the gaps in order to also meet the DORA requirements.

Designing a suitable and efficient path to contract remediation can be a daunting task, especially where financial entities have hundreds of contracts in place with technology vendors. To achieve this, and based on the authors' experience, the contract remediation project should be organised methodically into phases and take account of the following key considerations:

- Assessment of the contract portfolio should identify ICT service types, criticality or importance of the ICT services and in-scope EU territories. It may help to segment contracts into those that are brief, standard-form technology contracts and other more complex outsourcing contracts.
- Where possible, automating the diligence of individual contracts can create efficiencies, although it is critical that the outputs of automated reviews are validated.
- Preparing a contract addendum may be the most efficient method of remediation, which is then adapted for individual contracts, and companies can leverage any addenda previously used for compliance with mandatory contract terms for regulated outsourcings. Such an addendum could take a modular form enabling jurisdiction-specific issues to be added or removed, eg to address nuances around incident reporting, and also to adapt remediation for each contract based on the outcome of diligence.
- The mandatory contract terms under DORA may be divided into 'legal' terms (eg audit provisions, termination rights) and 'business' terms (eg service definitions). For the latter, a bespoke remediation process may need to be agreed and documented with applicable business SMEs, to be completed before 17th January, 2025, or as soon as possible thereafter.
- Where remediation is required, it may be prudent to prioritise certain providers based on criticality of services and/or complexity of contracts, as noted above.

Now more than ever, it is extremely valuable to understand how solutions and/or services are integrated in the operations of securities markets participants, in order to address the evolving challenges to ensuring operational resiliency.

The authors' experience is that this is an area in constant flux, with the vendor community acknowledging the changes faced by their customers. Each party will seek to apply their own DORA-compliant terms uniformly and the mechanisms for change under the contract will be key; challenging discussions are taking place as change is implemented. Entrenched approaches (from both customers and suppliers) are resulting in significant challenges to agree contract amendments where required or to get to contract at all, and also losing sight of an industry-wide view (by the supplier) and truly understanding how solutions are integrated within operations (by the customer). As with implementing regulatory expectations around outsourcing, hopes that mandatory contract terms become uniform will likely be displaced by the reality of each party's negotiating power.

IMPACT OF AI ON RESILIENCY AND OUTSOURCING REGIMES

The final section of this paper explores the impact of artificial intelligence (AI) on the themes identified above, given that the use of AI within securities markets, and financial services more generally, is under more regulatory scrutiny than ever.

A significant (and growing) portfolio of software applications used by securities markets participants already use AI and most,

if not all, companies will have some form of AI embedded in their supply chain of software and services. According to Ignites, an asset management-focused media outlet, 59 per cent of asset managers deploy generative AI for IT-use cases, such as code generation and debugging, and 56 per cent deploy generative AI (GenAI) for marketing-use cases, such as drafting customised marketing materials.

In trading, AI models allow traders, brokers and financial institutions to optimise trade execution and post-trade processes, reducing the market impact of large orders and minimising settlement failures. In other parts of securities markets, buy-side companies seek AI-enabled personalisation of content in substance and delivery or use AI tools to enhance information sourcing and data analysis. On the retail-facing side, the deployment of AI-enabled robo-advisers is receiving much attention amid predictions of more personalised wealth management products that are cost-effective and charge lower fees.

In each case, financial entities should look to leverage what they already have in place based on existing prudential requirements. The following themes are most pertinent in the context of AI:

- Documented due diligence procedures for third-party vendors;
- Enhanced cooperation obligations between the parties and with regulators;
- Data security and integrity;
- Auditability;
- Transparency of any material changes in AI models (such as input data, training and algorithms);
- Protection of confidentiality and intellectual property;
- Appropriate remedial measures, including manual work-arounds (where appropriate) and suspension or termination rights.

Regulators expect that financial entities will have in place appropriate controls, policies and procedures, and surveillance and monitoring to comply with the existing regimes, and supervisory bodies are unlikely to hold off on raising issues in examinations and investigations while their AI-specific policy approaches are evolving.

In saying that, there has been a significant volume of AI-specific publications of which financial entities (and their service providers) should be aware. The U.S. Department of the Treasury's report on Managing AI-Specific Cybersecurity Risks in the Financial Services Sector,[37] released in March 2024, in response to last October's U.S. Presidential Executive Order on Safe, Secure, and Trustworthy Development and Use of AI, summarises AI-use cases and risk trends and identifies opportunities, challenges and best practices to address AI-related operational risk, cyber security and fraud risk challenges. The Securities and Exchange Commission's (SEC) 2024 Examination Priorities[38] report noted AI as a focus area of emerging technologies, and that its recent enforcement focus has included 'AI washing' by issuers, brokers and advisers, as well as technology governance in a broader sense.

In the UK, the new Labour government stopped short of announcing a comprehensive AI bill in July 2024 as part of its first package of legislation, and so at time of writing the regulatory approach remains to be determined. From a financial services-specific perspective, in April 2024, the FCA reiterated its technology-agnostic, outcome-focused approach in its update on its approach to AI.[39]

As for the EU, the EU AI Act entered into force on 1st August, 2024 and the majority of its provisions will be enforced from August 2026. Non-retail use cases in securities markets will likely fall within the scope of 'general purpose' AI, with a more limited set of requirements, mainly around transparency. EU regulatory guidance for such use cases is most likely to come under existing regimes, and transparency

will be key. The following conclusion from ESMA's report on Artificial Intelligence in EU Securities Markets, published in April 2023, highlights some of the challenges with meeting some of the themes identified above:

> Complexity and lack of transparency, although arguably not inherent features of AI, may, in fact, represent barriers to the uptake of innovative tools due to the need to maintain effective human oversight and upskill management. Some firms appear to be limiting or foregoing their use of AI and ML algorithms because of operational concerns such as the compatibility of AI and their legacy technology.

Finally, throughout 2024, companies have been grappling with developing AI-specific policies and procedures. In the authors' view, companies should take a holistic approach and leverage policies and procedures that they already have in place, or are preparing as part of implementing DORA, which would cover the procurement and use of AI. As noted above, AI will likely already be embedded in a company's supply chain of software and services.

CONCLUSION

In recent years, major ICT disruptions, supply chain disruptions, geopolitical risks and shifting work patterns have all highlighted the importance for securities markets participants to reinforce their operational resilience. While implementing the requirements of DORA has been a priority for EU-based financial entities throughout 2024, it also serves as a reminder of existing regulatory expectations around third-party risk management and outsourcing, which have converged on certain themes. Regulated entities and their service providers are pushing for uniformity in their contractual compliance with those areas; however, the outcome will depend on each party's negotiating power.

AI adds another dimension to considering these themes, and with so much regulatory policy in flux, financial entities should look to leverage what they already have in place and consider holistically how procurement and use of AI fits into their third-party risk management framework.

NOTE

This article is provided as a general informational service and it should not be construed as imparting legal advice on any specific matter.

References

(1) McKinsey (June 2024), 'Europe's new resilience regime: The race to get ready for DORA', available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-new-resilience-regime-the-race-to-get-ready-for-dora (accessed 13th September, 2024).
(2) International Organization of Securities Commissions (IOSCO) (October 2021), 'Principles on Outsourcing: Final Report', available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf (accessed 13th September, 2024).
(3) *Ibid*.
(4) Basel Committee on Banking Supervision (BCBS), 'Principles on Operational Resilience', p. 7, available at https://www.bis.org/bcbs/publ/d516.pdf (accessed 13th September, 2024).
(5) European Central Bank (ECB) (February 2024), 'Rise in Outsourcing Calls for Attention', available at https://www.bankingsupervision.europa.eu/press/publications/newsletter/2024/html/ssm.nl240221.en.html (accessed 13th September, 2024).
(6) See Financial Conduct Authority (FCA)

(December 2022), 'TSB fined £48.65m for operational resilience failings', available at https://www.fca.org.uk/news/press-releases/tsb-fined-48m-operational-resilience-failings (accessed 13th September, 2024).

(7) See Financial Conduct Authority (FCA) (May 2019), 'FCA and PRA jointly fine Raphaels Bank £1.89m for outsourcing failings', available at https://www.fca.org.uk/news/press-releases/fca-and-pra-jointly-fine-raphaels-bank-1-89-million-outsourcing-failings#:~:text=Raphael%20%26%20Sons%20plc%20(%E2%80%9CRaphaels,combined%20fine%20of%20%C2%A31%2C887%2C252) (accessed 13th September, 2024).

(8) See Central Bank of Ireland (March 2022), 'BNY Mellon Fund Services (Ireland) DAC fined €10,780,000 and reprimanded by the Central Bank of Ireland for regulatory breaches relating to outsourcing', available at https://www.centralbank.ie/news/article/press-release-bny-mellon-fund-services-(ireland)-dac-fined-reprimanded-for-regulatory-breaches-relating-to-outsourcing-24-march-2022#:~:text=The%20Central%20Bank%20has%20determined,Provider%20in%20Ireland%20to%20date (accessed 13th September, 2024).

(9) European Banking Authority (EBA) (February 2019), 'Final Report on EBA Guidelines on Outsourcing Arrangements', available at https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (accessed 13th September, 2024).

(10) European Securities and Markets Authority (ESMA) (May 2021), 'Guidelines on Outsourcing to Cloud Service Providers', available at https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf (accessed 13th September, 2024).

(11) Commission de Surveillance du Secteur Financier (CSSF) (April 2022), 'Circular 22/806 on Outsourcing Arrangements', available at https://www.cssf.lu/wp-content/uploads/cssf22_805eng.pdf (accessed 13th September, 2024).

(12) Central Bank of Ireland (December 2021), 'Cross-Industry Guidance on Outsourcing', available at https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp138/cross-industry-guidance-on-outsourcing.pdf (accessed 13th September, 2024).

(13) Federal Financial Supervisory Authority (BaFin) (2021), 'AT 9 (Outsourcing) of Minimum Requirements for Risk Management (MaRisk)', available at https://www.bundesbank.de/resource/blob/623102/bca5bafd72a669115b15c4125e063feb/mL/minimum-requirements-for-risk-management-mindestanforderungen-an-das-risikomanagement-marisk-data.pdf (accessed 13th September, 2024). BaFin has also published relating specifically to cloud outsourcing.

(14) European Central Bank (ECB) (June 2024), 'ECB consults on outsourcing cloud services', available at https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240603~e625aaca33.en.html (accessed 13th September, 2024).

(15) See Financial Conduct Authority (FCA) (May 2024), 'Outsourcing and Operational Resilience', available at https://www.fca.org.uk/firms/outsourcing-and-operational-resilience; and Financial Conduct Authority (FCA), 'FCA Handbook', SYSC 8.1 and 13.9, available at https://www.handbook.fca.org.uk/handbook/SYSC/ (both accessed 13th September, 2024).

(16) Federal Reserve System (June 2023), 'Interagency Guidance on Third-Party Relationships: Risk Management', available at https://www.federalreserve.gov/supervisionreg/srletters/SR2304a1.pdf.(accessed 13th September, 2024).

(17) Financial Industry Regulatory Authority (FINRA) (August 2021), 'Vendor Management and Outsourcing, FINRA Regulatory Notice 21-29', available at https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.

pdf; see also Morgan Lewis & Bockius (August 2021), 'Outsourcing: FINRA Outlines Onboarding And Supervision Suggestions for Use of Third-Party Vendors', available at https://www.morganlewis.com/pubs/2021/08/outsourcing-finra-outlines-onboarding-and-supervision-suggestions-for-use-of-third-party-vendors (both accessed 13th September, 2024).

(18) See Cayman Islands Monetary Authority (CIMA) (April 2023), 'Corporate Governance for Regulated Entities', available at https://www.cima.ky/upimages/regulatorymeasures/Rule-CorporateGovernanceforRegulatedEntities_1685565552.pdf; and Cayman Islands Monetary Authority (CIMA) (August 2015), 'Statement of Guidance: Outsourcing, Regulated Entities', available at https://www.cima.ky/upimages/commonfiles/1499756196StatementofGuidanceOutsourcingRegulatedEntities.pdf (both accessed 13th September, 2024).

(19) Monetary Authority of Singapore (MAS) (December 2023), 'Guidelines on Outsourcing (Banks)', available at https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/bd/guidelines-on-outsourcing/guidelines-on-outsourcing-banks.pdf (accessed 13th September, 2024).

(20) See, in the context of cloud outsourcing, Hong Kong Monetary Authority (HKMA) (August 2022), 'Guidance on Cloud Computing', available at https://www.hkma.gov.hk/media/chi/doc/key-information/guidelines-and-circular/2022/20220831c1.pdf (accessed 13th September, 2024).

(21) International Organization of Securities Commissions (IOSCO), ref. 2 above, Principle 3.

(22) Bank of England (BoE) Prudential Regulation Authority (PRA) (March 2021), 'Supervisory Statement SS2/21: Outsourcing and Third Party Risk Management', p. 15, available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf (accessed 13th September, 2024).

(23) Prudential Regulation Authority (PRA), 'Allocation of Responsibilities 4.1(21) (banks), PRA Rulebook', available at https://www.prarulebook.co.uk/pra-rules/allocation-of-responsibilities (accessed 13th September, 2024).

(24) Federal Reserve System, ref. 16 above, p. 20.

(25) European Banking Authority (EBA), ref. 9 above, Ch. 11.

(26) International Organization of Securities Commissions (IOSCO), ref. 2 above, Principle 4.

(27) See Morgan Lewis & Bockius (March 2024), 'Luxembourg's Financial Services Regulator Enhances ICT Incident Reporting Framework', available at https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/luxembourgs-financial-services-regulator-enhances-ict-incident-reporting-framework (accessed 13th September, 2024).

(28) International Organization of Securities Commissions (IOSCO), ref. 2 above, Principle 7.

(29) *Ibid*., Principle 2.

(30) See International Organization of Securities Commissions (IOSCO) (July 2022), 'Operational Resilience of Trading Venues and Market Intermediaries During the COVID-19 Pandemic & Lessons for Future Disruptions', available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD706.pdf (accessed 13th September, 2024).

(31) Depository Trust and Clearing Corporation (DTCC) (April 2021), 'Managing Through a Pandemic COVID-19, DTCC White Paper', available at https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/Managing-Through-a-Pandemic-Covid19-Whiteaper.pdf (accessed 13th September, 2024).

(32) For example: as to the UK, the UK Government announced in July 2024 a new Cyber Security and Resilience Bill which will update the existing UK regulatory framework and, specifically for

the financial sector, see the annual cyber resilience best practices (CBEST) for the financial sector published by the FCA, the PRA and the Bank of England (BoE): Bank of England (BoE), '2023 CBEST thematic', available at https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/2023-cbest-thematic; as to the EU, the NIS 2 Directive on cyber security was published in December 2022, alongside DORA, and must be transposed into national law by 17th October, 2024 — many of its requirements set the basis for cyber security risk management measures and reporting obligations across multiple sectors; as to the US, the New York Department of Financial Services (NYDFS) published in November 2023 a secondment amendment to 23 NYCRR Part 500 (Cybersecurity Rules), which requires, among other things, new risk assessment requirements, additional cyber security policy content requirements and notification obligations following a cyber incident and extortion payments: New York State Department of Financial Services, 'Second Amendment to 23 NYCCR 500', available at https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf (both accessed 13th September, 2024).

(33) Financial Stability Board (FSB) (December 2023), 'Enhancing Third-Party Risk Management and Oversight', available at https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/ (accessed 13th September, 2024).

(34) Office of the Comptroller of the Currency (OCC) (March 2024), 'Thoughts of Operational Resilience', available at https://www.occ.gov/news-issuances/speeches/2024/pub-speech-2024-23.pdf (accessed 13th September, 2024).

(35) See Bank of England (BoE) (March 2022), 'PRA, SS1/21, Operational resilience: Impact tolerances for important business services', available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf; and Financial Conduct Authority (FCA) (March 2021), 'PS21/3 Building operational resilience', available at https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience (both accessed 13th September, 2024).

(36) Financial Conduct Authority (FCA)/ Prudential Regulation Authority (PRA)/ Bank of England (BoE) (December 2023), 'CP26/23 – Operational resilience: Critical third parties to the UK financial sector', available at https://www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector (accessed 13th September, 2024).

(37) U.S. Department of the Treasury (March 2024), 'Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector', available at https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf (accessed 13th September, 2024).

(38) U.S. Securities and Exchange Commission (SEC) (October 2023), '2024 Examination Priorities', available at https://www.sec.gov/files/2024-exam-priorities.pdf (accessed 13th September, 2024).

(39) Financial Conduct Authority (FCA) (April 2024), 'AI Update', available at https://www.fca.org.uk/publication/corporate/ai-update.pdf (accessed 13th September, 2024).