IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

Annual Planning Hot Topics 2024/25

BDO

BDO Financial Services' internal audit contact points

We hope you had a very enjoyable summer!

Welcome to the Planning edition of our monthly packs. In this issue, we explore the sector's Hot Topics to be considered for the 2025 plan to help Internal Audit teams appropriately address risks in their annual planning process. Alongside our pack, IA teams should also refer to the CIIA's Risk In Focus 2025 report, published this month, with which to benchmark your draft plan against market practices.

BDO's Banking & Building Societies Update summarises the key regulatory developments and emerging business risks relevant for all banks, building societies and, where flagged, for alternative finance providers (ie, peer-to-peer lenders, card providers, E-money services providers and debt management companies).

Our FS Advisory Services team are working with more than 50 banks and building societies as internal auditors and advisors, giving us a broad perspective on the issues facing the sector. We have aggregated insights from our in-house research, client base, the Regulators and professional bodies, including the Chartered Institute of Internal Auditors (CIIA), to support your audit plans and activities.

We hope this pack provides value to you and your colleagues; please do share with us any feedback you may have for our future editions.

Leigh Treacy
Partner

+44 (0)7890 562 098
leigh.treacy@bdo.co.uk

Chris Bellairs
Partner

+44 (0)7966 626 128
christian.bellairs@bdo.co.uk

Sam Patel
Partner

+44 (0)7970 807 550
sam.patel@bdo.co.uk

Bruk Woldegabreil
Associate Director

+44 (0)7467 626 468
bruk.woldegabreil@bdo.co.uk

Oliva Gledhill
Manager

olivia.gledhill@bdo.co.uk

Contents

01 Technology, Cyber, Digital and Data

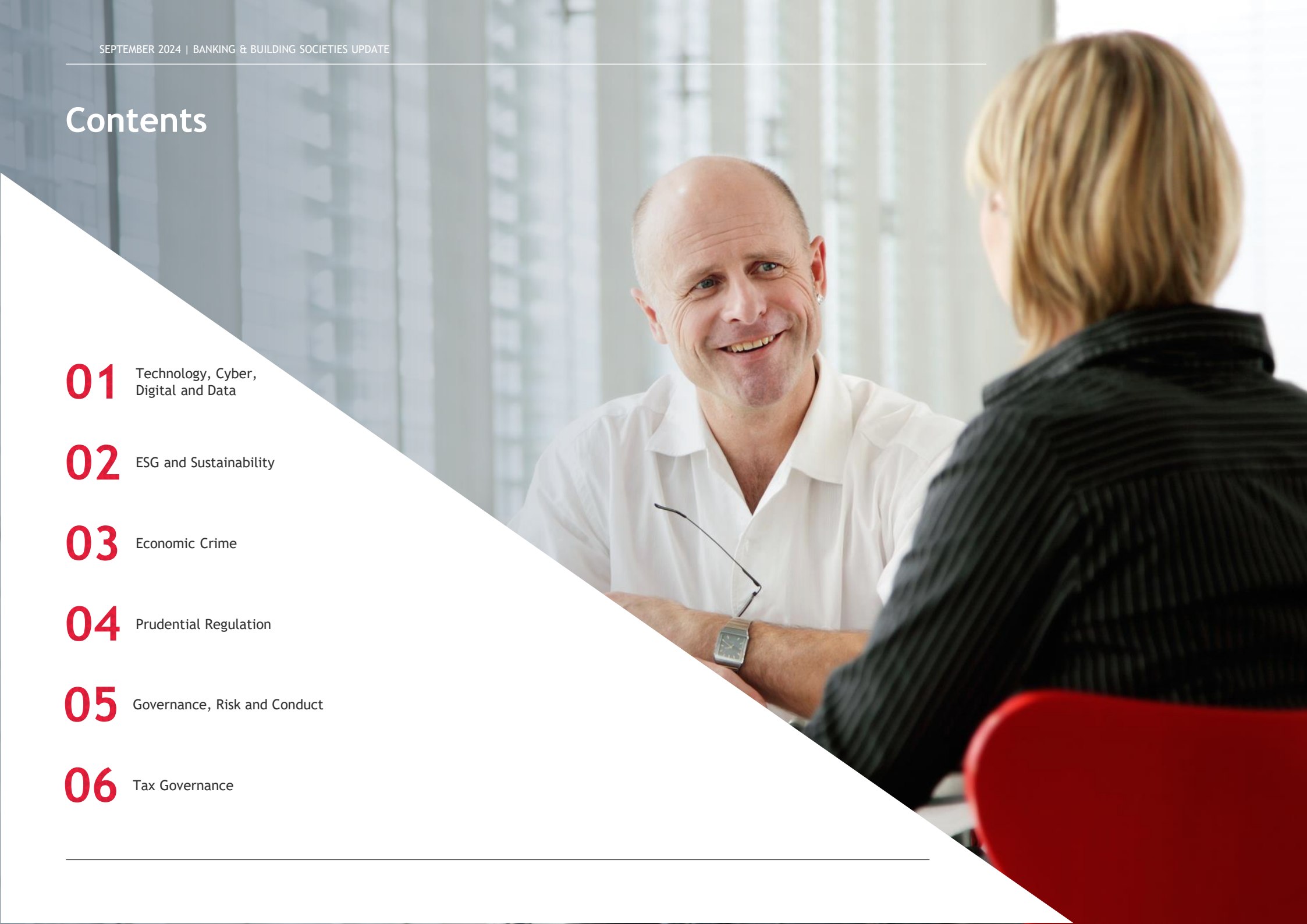
02 ESG and Sustainability

03 Economic Crime

04 Prudential Regulation

05 Governance, Risk and Conduct

06 Tax Governance



01

Technology, Cyber, Digital and Data Hot Topics

Sandi Dosanjh
Partner

sandi.dosanjh@bdo.co.uk

Steve Dellow
Director

steve.dellow@bdo.co.uk

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Cyber Security	Review of design and effectiveness of cyber security controls against the NIST or CIS frameworks to prevent or respond to a cyber security incident. Review compliance with cyber standards and/or regulation.	The financial services sector is highly dependent on technology and digital platforms to deliver products and services to customers, and enable its core functions, such as payment systems, trading platforms, clearing and settlement systems. The interconnectivity of systems means that a cyber incident can create a contagion risk across other processes which could compromise compliance, reporting or disclosure obligations which could impact credibility and trustworthiness in the market. Attempting to compromise an organisation via a successful breach is now big business, both at state and criminal enterprise levels. The threat is ever evolving as both technology in place at clients, and the means to hack them, are constantly changing. New mandatory requirements are being set in EU legislation such as the Digital Operational Resilience Act 'DORA' which comes into force 17 January 2025, the NIS2 Directive (17 October 2024). Effective cyber resilience controls remain a requirement of the UK Operational Resilience Act (31 March 2025). Many organisations maintain ongoing technology frameworks which they must align to such as PCI, ISO27001, Cyber Essentials+.	▶ Three year rolling plan to cover off the design and operating effectiveness of the following 6 domains from NIST (or equivalent CIS for smaller organisations): • Year 1 – Govern; Identify • Year 2 – Protect; Detect • Year 3 – Respond; Recover. **Indicative number of days required – 25-30+** *Note – operating effectiveness testing is essential therefore the number of audit days for each year should be minimum 25-30+ (scope dependant). To operationalise this, internal audit functions should evaluate work performed to date to determine which of the six domains are remaining for coverage.* ▶ Penetration tests on behalf of third line to test actual sufficiency of cyber controls ▶ Cyber regulation compliance (DORA, Cyber Essentials, NIS2, ISO, PCI) ▶ Cyber incident response and resilience.

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Cloud environments	The proliferation of cloud technologies and underlying risks around transition, security and availability make this a high priority area for IA coverage.	Financial services organisations are increasingly leveraging cloud services for their infrastructure and application needs. This transition is driven by benefits such as scalability, cost-effectiveness, and accessibility. However, the adoption of cloud services also presents unique risks and challenges, particularly around: ▶ **Data Security and Privacy** - The potential for cyber threats and data breaches remains a persistent risk, given the sensitive nature of the data processed in cloud environments ▶ **Availability** - It is essential to evaluate the technical effectiveness of disaster recovery and business continuity strategies. This includes assessing cloud-specific recovery protocols, redundancy measures, and failover capabilities to ensure robust operational resilience ▶ **Governance and adoption** - as more and more organisations adopt cloud technologies risks can arise around the actual transition from on-prem technology to the cloud.	*Firms will be on different cloud journeys, so consider risks as outlined below. Internal audit teams should be consulted to determine optimum scope and timings.* Those in adoption phase: ▶ Cloud migration review ▶ Review of cloud adoption strategy (data migration, security standards, compatibility, compute resourcing) ▶ Review of M365 Modern Workplace (as applicable). **Indicative number of days required - 15-20** Those with more mature cloud environments should consider a three-year rolling programme covering the following: ▶ Security review (year 1) • Assessing the implementation of robust controls to safeguard confidential information stored in the cloud • Ensuring encryption standards are maintained both in transit and at rest. **Indicative number of days required - 15-20** ▶ Operations review (year 2) • Evaluating the effectiveness of disaster recovery and business continuity plans to mitigate downtime • Ensuring that cloud service providers offer sufficient redundancy and failover capabilities • Reviewing incident response procedures to handle data breaches and service disruptions promptly • Assessing the effectiveness of access controls and identity management solutions in the cloud environment. **Indicative number of days required - 15-20** (cont'd)

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Cloud environments			(cont'd from previous slide) ▶ Governance review (year 3) • Verifying that cloud usage complies with industry regulations such as GDPR, HIPAA, and PCI DSS • Conducting regular audits to check compliance with FCA, PRA, EBA guidelines, ISO/IEC 27017, and NCSC principles. **Indicative number of days required – 15-20** ▶ Innovation review (any time) • Supporting the organisation's digital transformation initiatives by ensuring cloud environments are conducive to agile development and deployment practices • Ensuring that DevOps practices in the cloud are secure and efficient, promoting continuous integration and continuous delivery (CI/CD). **Indicative number of days required – 15**
Outsourcing and third parties	Outsourcing remains prevalent in almost all of our clients and is a high priority for regulators.	Regulatory oversight of outsourcing has been progressively intensifying over the years, with firms required to manage third-party risk in accordance with the General Data Protection Regulation, as well as the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA). The PRA's recent supervisory statement, 'SS2/21 Outsourcing and Third-Party Risk Management,' seeks to augment the operational resilience requirements and promote enhanced robustness over the adoption of cloud services and other technologies, as outlined in the Bank of England's response to the 'Future of Finance' report. Additional regulatory guidance on outsourcing includes the European Banking Authority (EBA) 'Guidelines on outsourcing arrangements' and aspects of the EBA 'Guidelines on ICT and security risk management'.	▶ Assessing the IT third party supplier strategy and alignment to company policy ▶ Assessing IT third-party supplier risk management including a review of the identification and risk evaluation of third-party suppliers ▶ Alignment to specific regulatory requirements such as SYSC 8 and 13.9; SS2/21 Outsourcing and Third-Party Risk Management; EBA guidelines ▶ Evaluating IT third-party supplier governance and oversight to assess whether the mechanisms are adequate and effective ▶ Assessing supplier performance and compliance by reviewing management's indicators to ensure that they are relevant, reliable and consistent ▶ Assessing supplier contractual clauses around right of audit, SOC reports and due diligence. **Indicative number of days required – 20-25**

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Resilience	Regulators continue to drive the resilience agenda with the operational resilience transition period ending in March 2025. DORA (EU only) becomes live in January 2025. The digitised nature of many of our clients means their reliance on outsourced technology is higher than ever.	The Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) have placed operational resilience at the heart of their regulatory framework, recognising that a resilient financial system is critical to the health of the UK's economy. This focus is sharpening as institutions grapple with an array of challenges, from cyber threats to complex supply chain dependencies. Regulations compel firms to pinpoint their critical business services, those whose disruption could significantly affect customers, the firm, or the stability of the UK's financial market. Firms are encouraged to engage in a series of activities to comprehend the maximum tolerable period of disruption, identify vulnerabilities, and assess the adequacy and effectiveness of contingency plans. There's also a clear mandate for senior management to take charge and maintain oversight. The operational resilience regulatory transition period comes to a close on 31 March 2025 whereupon firms must have all important business services full resilient. More broadly, resilience of wider areas of the organisation which may not be designated an important business service should still have effective solutions to restore operations within an acceptable period of time. Third party resilience remains a challenge.	▶ Review of compliance with operational resilience regulation, *if not done previously* ▶ *If done previously*, review of any remaining work conducted since (notably scenario testing) and confirmation of resilience status as at 31 March deadline ▶ Business continuity management and disaster recovery review ▶ Third party resilience review ▶ Cyber incident response ▶ DORA reviews (see cyber risk above for more detail). **Indicative number of days required – 20-25**

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Artificial Intelligence	Remains a buzz phrase and represents key risks to key areas such as calculations and outputs where AI-based algorithms are used. Can also mean a loss of control as staff use internet-based AI software for processing company data assets.	▶ Whilst the uptake in artificial intelligence in financial services is currently slow, even minor usage has the potential to cause significant issues. Fundamentally, a lack of control around AI can result in: • Untested algorithms being used to generate what may be unsafe outcomes • Personal data or key IP being placed in non-secure environments (predominantly the Internet) • Uncontrolled changes made to AI models undermining established baselines • Use of inappropriate or incomplete inputs to a data model • A lack of clarity and transparency around where AI models are used for decision-making. ▶ ISO/IEC 42001:2023(E) provides a base level of expected controls and risks to be managed when using AI. Additionally, the provisional version of the EU AI Act, which came into force in August 2024, will also be useful as initial guidance for expected legislative requirements that organisations need to comply with.	▶ Review of governance around AI and any underlying strategy ▶ Verify the accuracy and reliability of data and algorithms being used, including the consistency of outputs and decisions ▶ Assess the culture and communication around AI and provide feedback and suggestions for enhancing trust, engagement and collaboration. **Indicative number of days required - 15-25**

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
IT change programmes	With technology roll-outs and enhancements underpinning many organisation's business strategy, digital transformation is a kay risk area.	With IT change programmes, technology is the enabler for new ways of working that can open up new markets, enable the deployment of new products more quickly/ efficiently, improve back-office efficiency, create data driven organisations, to mention a few. However, with this level of change, the potential to introduce excessive cost, failed processes and adverse customer experience (with associated regulatory intervention) is extremely high and borne out by the large number of organisations experiencing these issues. Internal Audit can provide a high level of specialised channel to ensure that the risks around project components are effectively managed and that governance stakeholders are provided with the right information for making 'go/no-go' decisions.	▶ Review programme governance, delivery frameworks and planning, to include: • Functional requirements gathering and scope definition • Agile change management and communication • Data Strategy, migration, and re-platforming • Testing and validation • Benefits definition, tracking and realisation. **Indicative number of days required – 20-25**
Data governance	With data at the heart of accurate management reporting and both internal and customer outcomes, the management of data quality and the ability to make effective use of that data is a high strategic priority for many of our clients.	All organisations rely on data to run their business and make strategic decisions to drive the organisation forwards. Data governance aims to generate value from data as an asset by minimising the risk of poor-quality data existing within an organisation that is subsequently used to make ineffective decisions which can prove costly. Furthermore, errors in transactional data can undermine customer outcomes and impact the organisation through incorrect calculation of key values such as pricing, interest, claims etc.	▶ Review of data governance processes, in particular: • Policies and procedures • Roles and responsibilities • Data discovery, evaluation and classification • Data mapping • Data quality controls • Master data management. ▶ Specific data migration reviews ▶ Evaluation of the accuracy of outputs from key calculation engines, including use of data analytics and data visualisation ▶ Data retention and deletion ▶ Holistic approach to data governance for managing broader tenets of data such as availability and confidentiality. **Indicative number of days required – 20-25**

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Payments	Review of organisation's stated payments technology control in order to ensure that attestation returns to providers are accurate or that requirements around implementation of payments technology have been met.	Key payments providers such as Faster Payments and SWIFT require attestations or independent assurance over the implementation of required technology security and availability safeguards in order for customers (i.e. banks, insurers etc) to be permitted ongoing access to the payments mechanism.	▶ SWIFT attestation reviews **Indicative number of days required – 15-20** ▶ PSD2 implementation and compliance reviews **Indicative number of days required – 20-25** ▶ Faster Payments implementation and compliance reviews. **Indicative number of days required – 20-25**
IT governance	Review of approach to managing key facets of IT in order to meet organisation objectives.	Failure to manage the IT function may result in failure of key IT initiatives and inability to evaluate and mitigate technology risk.	Governance review to cover: ▶ Governance, roles and responsibilities ▶ IT strategy ▶ IT risk management ▶ IT cost management ▶ Resource management ▶ Benefits realisation. **Indicative number of days required – 15-25**

Technology, Cyber, Digital and Data

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
IT general controls	Review of mitigation of risk of unauthorised access and change to key applications, operating systems and databases. Incoming changes to FRC focus on non-financial internal control raises the profile of this for area.	Despite the FRC stating that it will not take forward over half of its original proposals for corporate governance, the revised Governance Code published in January 2024, will place increased focus on internal controls extending beyond finance and including operational and non-financial areas. Whilst external audit may look at a number of applications material to the financial statements, there may be other applications with underlying operating systems and databases upon which important business services are dependant. Ensuring that access and change is carefully managed is fundamental to the ongoing confidentiality, integrity and availability of the underlying data and transactions within those systems.	▶ For applications, operating systems and databases: • Joiners, leavers, movers • Privileged access • Recertification • Change management. **Indicative number of days required – 25-35**

02

ESG & Sustainability Hot Topics

Sasha Molodtsov
Partner

sasha.molodtsov@bdo.co.uk

Adam Soilleux
Director

adam.soilleux@bdo.co.uk

ESG: Sustainability governance, risk and regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Anti-Greenwashing Rule (AGR)	Effective since 31 May 2024. Applies to **All FCA authorised firms** making claims about the sustainability of their products or services	The AGR is another key requirement introduced by the FCA, who have already indicated via several communication channels that it will be monitoring firms' sustainability-related claims about their products and services. In addition to the rule itself, the FCA has issued detailed guidance (FG24/3).	▶ Assess the completeness of AGR project/implementation plans to understand how compliance has been esnured with the AGR as of 31 May 2024 ▶ Assess the extent to which there are controls in place to ensure sustainability-related claims and references within the TCFD report are clear, fair, not misleading, and able to be substantiated ▶ Test a sample of sustainability-related claims made about products and / or services and assess compliance against FG24/3. **Indicative number of days required - 15**
Sustainability Disclosure Requirements (SDR)	Phased implementation staring with the AGR from 31 May 2024. In-scope sustainable investment product naming and marketing rules will apply from 2 December 2024, on-going product reporting December 2025 and entity-level disclosures from December 2026.	The SDR labelling, naming,-marketing and disclosure requirements apply to: 1. Investment funds and managers, primarily those marketed and marketing to retail investors in the UK, in respect of the labelling and classification, disclosure, naming, and marketing and distribution rules 2. Firms that manage or distribute those products, who also fall under the scope of these rules effective as of 31 July 2024.	▶ Assess the completeness of firms' SDR project / implementation plans to assess how firms have ensured compliance with the relevant requirements upon first use of a sustainable investment product label ▶ Assess the process by which products have been categorised into one of the four sustainable investment product labels, including the selection of a "robust, evidence-based standard of sustainability" ▶ Assess SDR product marketing and disclosure material for compliance with the relevant SDR requirements. **Indicative number of days required - 15**
Taskforce on Climate-related Financial Disclosures (TCFD)	Continued roll-out of mandatory reporting. Latest cohort of firms to be subject to mandatory reporting is asset managers with >£5bn AUM, who had to report by 30 June 2024.	FCA, PRA and FRC are reviewing the quality of reporting of firms in-scope for mandatory reporting. Additionally, whilst TCFD is a reporting framework, the four pillars of governance, strategy, risk management and metrics and targets act as a sensible baseline to develop a broader sustainability-related framework.	▶ Assess the design of the controls around the production of the TCFD entity-level and product-level reports ▶ Assess the content of the TCFD reports against regulatory expectations and industry good practice ▶ Assess the suitability and sufficiency of the Management Information ("MI") reported to relevant governance forums in respect of the sustainability-related objectives, and review how firms are, or plan to monitor progress against these. **Indicative number of days required - 15**

ESG: D&I

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Diversity and Inclusion	Assessment of firms Diversity, Equity, Inclusion and Belonging (can also be included within talent, culture and broader ESG remits) arrangements to ensure regulatory compliance, and in line with industry and market expectations.	Existing FCA and PRA expectations for healthy cultures, Board diversity and succession planning. FCA and PRA (FCA CP23/20 and PRA CP 18/23) want to boost diversity and inclusion to support healthy work cultures, reduce groupthink and unlock talent – applicable to all CRR and Solvency II firms and FSMA firms with a part 4A permission to reduce discrimination and misconduct, and improving risk management and decision making within firms. FCA 2023 'Non-Financial Misconduct' survey to all wholesale Banks, Insurers and Asset Managers as a result of Treasury Select Sexism in the City enquiry, high profile FS cases and NFM proposals as part of FCA CP. **For listed firms** • FS Corporate Governance Code updates • FTSE Leaders and Parker Review expectations. **IA Standards** • CIIA 'Auditing D&I' technical guidance **Industry led public charters/membership bodies** • Women in Finance Charter • Race at Work • Progress Together • Diversity Project.	▶ **Governance and responsibility** ▪ Review Terms of Reference for the Board and Board Nomination Committee (NomCo) ▪ Review statements of responsibility for Board members, Chair of the Nomination Committee (NomCo), Chief Executive Officer and the Chief People Officer ▪ Review governance structure for reporting D&I matters internally across the Bank (i.e. to Senior Management/SMF's). ▶ **D&I documentation** ▪ Review D&I strategy, D&I plans / Charter. ▶ **Reporting & M.I** ▪ Review the data that is reported internally to Senior Management and the Board in relation to D&I, including the Group Scorecard ▪ Review the data that is reported externally (ie gender pay gap, ethnicity pay gap). ▶ **Employee lifecycle** ▪ Review the processes to attract and recruit new employees ▪ Review processes in place to retain, promote and encourage internal mobility for employees ▪ Review employee exit process ▶ **Board succession planning** ▪ Review how the Board performs succession planning (ie focus on skills, experience and effectiveness of its members) ▪ Review ExCo succession planning and consideration of D&I. ▶ **Non-Financial Misconduct** ▪ Review design and effectiveness of whistleblowing and speak up arrangements. **Indicative number of days required - 15**

ESG: Sustainability governance, risk and regulation

Other topics to consider

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
ESG strategy	For firms subject to TCFD reporting (phased roll out since 2020), the development of at least a climate-related strategy is mandatory.	Regardless of mandatory sustainability-related requirements, all regulated firms should have at least demonstrated consideration of developing an ESG strategy, which is proportionate to the materiality of sustainability-related risks faced, including regulatory risks. ***N.B. where a firm is "not ready" for such an audit because they have not begun their ESG strategy journey, we can support with this. It may be worth sharing this document with them.***	▶ Assess the materiality assessment conducted by Management to identify and determine the potential impact of sustainability-related risks to its business ▶ Assess the extent to which mandatory sustainability-related legal and regulatory requirements are being complied with ▶ Assess the quality and coherence of firm's documented ESG / sustainability / corporate social responsibility strategy and framework against regulatory requirements, but also industry practice and expectations. **Indicative number of days required - 15**
Carbon / greenhouse gas (GHG) emissions reporting	Streamlined Energy and Carbon Reporting requirements for medium-large sized firms from 1st April 2019. Phased mandatory TCFD reporting from 2020. Energy Savings Opportunity Scheme (ESOS), phased implementation, phase 3 from 6 August 2024.	These climate-related reporting requirements require the collation, calculation and reporting of GHG emissions data. Given statutory audits only conduct substantive audit procedures over sustainability-related reporting, there is heightened risk of misstatement, and there is growing interest in this data from a range of stakeholders aside from just the regulators.	▶ An assessment of the governance arrangements for GHG reporting controls in terms of collection, processing and reporting, by assessing the completeness, accuracy, timeliness of qualitative and quantitative data, including for quality assurance ▶ A review the governance oversight and control environment including the clarity of roles responsibilities and accountability, formalisation of processes, KPI monitoring, control and methodology ▶ An assessment of the assumptions and methodology framework applied within the GHG emissions preparation and finalisation against a relevant framework such as the GHG Protocol and the Partnership for Carbon Accounting Financials ("PCAF") guidance. **Indicative number of days required - 15**
Other ESG strategy "deep dives"	COP 16 Biodiversity – October 2024, Colombia. Transition plan taskforce sector specific guidance – June 2024. Climate biennial exploratory scenario (CBES) – May 2022.	In addition to climate and D&I, other ESG and sustainability agendas are gaining attention from regulators and other stakeholders in the financial sector. As a result, financial institutions must continue to develop their ESG and sustainability strategy to meet these emerging topics. Additional regulatory requirements will be introduced, for example through the IFRS ISSB S1 and S2 sustainability and climate reporting requirements.	*TBC depending on sustainability topic, but will follow similar scope areas to the ESG strategy review ie, governance, strategy, materiality assessments, mapping against regulatory requirements, assessing project plans etc.* **Indicative number of days required - 15**

ESG: Sustainability governance, risk and regulation

Other topics to consider

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
EU Corporate Sustainability Reporting Directive (CSRD)	For third country firms (eg UK) that have significant operations in the EU, must comply with the CSRD on a phased implementation basis from 2024 onwards.	Extensive set of rules and requirements, as well as the need for mandatory assurance over disclosures. Depending on size and nature of operations in the EU will depend on year of reporting. Phased implementation between 2024-28.	▶ An assessment of the governance arrangements for CSRD reporting controls in terms of collection, processing and reporting, by assessing the completeness, accuracy, timeliness of qualitative and quantitative data, including for quality assurance ▶ Assess the methodology by which the firm has conducted is “double materiality assessment” ▶ A review the governance oversight and control environment including the clarity of roles responsibilities and accountability, formalisation of processes, KPI monitoring, control and methodology ▶ An assessment of the assumptions and methodology framework applied as per the CSRD and technical guidance. **Indicative number of days required - 15**

ESG: Sustainability governance, risk and regulation

Regulatory Requirements and Expectations

Existing regulatory requirements and key expectations

Asset & Portfolio Managers	Banking	All/ Other Firms (Payments, capital markets, brokers)
FCA's Anti-greenwashing rule: Effective as of 31 May 2024. **FCA's SDR Regime for funds:** in addition to the anti-greenwashing rule, naming and labelling regime for qualifying sustainable investment funds, consumer-facing, pre-contractual and ongoing disclosures. Phased implementation from 31 May 2024 onwards. **TCFD reporting (FCA):** Asset managers with greater than £50bn of AuM the rules first applied from 1 January 2022 with the deadline for publishing their first report on 30 June 2023 and on demand disclosures starting on 1 July 2023. **Asset managers** with AuM of £5-50bn to report by 30 June 2024. **FCA PS22/3: Diversity and inclusion on company boards and executive management.** In-scope companies are required to make these disclosures in their annual reports for financial years starting on or after 1 April 2022. **FCA (Part 4A FSMA permission) D&I Policy Statement** – expected end of 2024. **FRC Stewardship Code** **FCA COBS requirements**	**Climate change risk management:** The PRA required banks and insurers to have a risk management framework and a strategic approach in place by the end of 2021. Clarifies that TCFD reporting is expected. **FCA's Anti-greenwashing rule**: Effective as of 31 May 2024. **Decarbonisation or transition plan:** Not yet mandatory but the government has confirmed that it will be made mandatory in the near future and firms are encouraged to adopt early implementation **FCA PS22/3: Diversity and inclusion on company boards and executive management.** In-scope companies are required to make these disclosures in their annual reports for financial years starting on or after 1 April 2022. **FCA and PRA D&I Policy Statement** FCA (CRR, Solvency II and Part 4A FSMA permission scope) D&I Policy Statement – expected end of 2024.	**FCA's Anti-greenwashing rule**: Effective as of 31 May 2024 for all FS firms. **FCA ESG Rules for Listed Companies:** In Commercial companies with a UK premium listing must disclose, on a comply or explain basis, against the recommendations of the TCFD. **Energy and Carbon Report Regulation 2018 for all quoted companies:** requires to report on GHG emissions **Wider scope of listed companies and UK-registered companies with over 500 employees and £500 million turnover:** Introduces mandatory climate-related disclosures in line with the TCFD framework for financial years beginning on or after 6 April 2022. This can include for example larger banks and insurers. **FCA PS22/3: Diversity and inclusion on company boards and executive management:** In-scope companies are required to make these disclosures in their annual reports for financial years starting on or after 1 April 2022. **FCA (Part 4A FSMA permission) D&I Policy Statement:** Expected end of 2024. **LSE Guide to ESG Reporting:** Issuers are expected to report on 8 priorities covering for example strategy to materiality, data and debt finance.

03

Economic Crime Hot Topics

Vladimir Ivanov
Senior Manager

vladimir.ivanov@bdo.co.uk

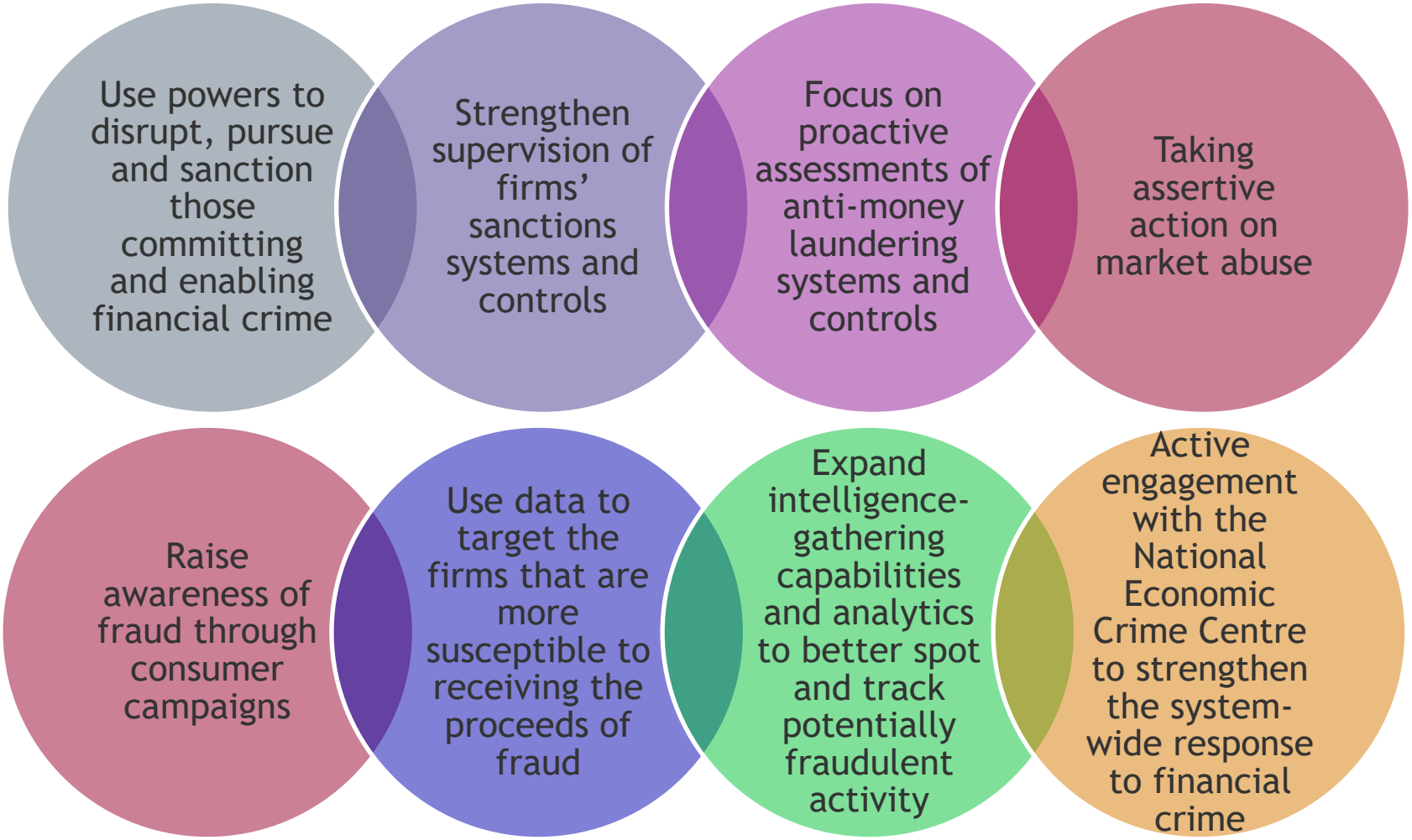
Karen Monks
Senior Manager

karen.monks@bdo.co.uk

Economic Crime

FCA Business Plan 2024/25

Reducing and preventing financial crime



Economic Crime

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Sanctions risk management	Sanctions compliance is absolute – Firms who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. As a result, firms must have robust systems and controls to manage this risk. The FCA continues to assess whether firms are maintaining adequate systems and controls to mitigate the risk of breaching sanctions and facilitating sanctions evasion.	The unprecedented size, scale, and complexity of sanctions imposed by the UK Government and international partners since Russia's invasion of Ukraine, has further increased our focus on firms' sanctions systems and controls. Over the last 18 months, the FCA have engaged in a substantial programme of work assessing the systems and controls relating to sanctions compliance for over 170 firms across a range of sectors. This has involved assessing firms' controls, using a new analytics-based tool, as well as the use of specific intelligence and reporting.	**Design Effectiveness** ➢ Reviewing policies, procedures, and processes for sanctions screening, including the process for reviewing and escalating alerts for consideration ➢ Reviewing the processes for ensuring the completeness, accuracy and timeliness of the data supplied by the source sanctions screening systems ➢ Assess the effectiveness of the institution's policy for reviewing sanctions alerts ➢ Evaluating the appropriateness of the monitoring of sanctions alert closure. **Indicative number of days required - 10-12** **Operational Effectiveness** ▶ Assess the quality of investigations conducted into Sanction Screening alerts. **Indicative number of hours required - 0.75 hours per sanction screening alert + 0.25 hours of QA**

Economic Crime

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Fraud risk management - ECCTA failure to prevent offence	The Economic Crime and Corporate Transparency Act 2023 ("ECCTA") received Royal Assent on 26 October 2023. We are currently awaiting the publication of guidance by the government on reasonable fraud prevention procedures. It is important to note that whilst the Act has received Royal Assent, the offence will only come into force once it has been published. In line with the guidance published under the Bribery Act and the Corporate Finances Act, we expect the guidance under ECCTA to cover the following six pillars: 1. Governance 2. Policies and procedures 3. Due Diligence 4. Risk Assessment 5. Communication 6. Monitoring	The new corporate criminal offence of Failure to Prevent Fraud under ECCTA, which exposes companies to the risk of investigation and prosecution if they benefit (directly or indirectly) from fraud committed by their employees, agents, subsidiaries or providers of services where the organisation did not have "reasonable fraud prevention procedures" in place to prevent the misconduct.	➢ Assess the adequacy of the Governance and Oversight arrangements that are in place and assessing to what extent there is a "tone from the top" approach regarding the Firm's commitment to preventing fraud ➢ Evaluate the design of the Fraud Policies and Procedures, and the alignment within the group. Where applicable we will also assess these against Regulator's expectations, industry guidance and best practice ➢ Review of the Fraud Risk Assessment to determine its suitability in identifying and assessing fraud risk within the Firm ➢ Review the Fraud Response plan to determine the adequacy of coverage and alignment with industry expectations in relation to fraud detection, investigation, and reporting ➢ Review the approach to training relevant staff regarding fraud prevention, detection, and reporting, including the format and frequency of the fraud awareness training delivered to relevant staff ➢ Assess the monitoring frameworks and tools in place, including any relevant policies & procedures ➢ Assess the suitability and proportionality of any monitoring methodologies, rules, and parameters the Firm has in place. **Indicative number of days required - 15**

Economic Crime

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative Scope Areas
Fraud risk management - App fraud	In May 2022, Treasury announced its intention to legislate and allow the PSR to require victim reimbursement for APP scams and in June 2023, this legislation came into effect. With effect from 7 October 2024 all directed payment firms will be required to operate to new rules, with multiple operational changes including both sending and receiving firms splitting the costs of reimbursement to customers equally on a 50:50 basis. This reimbursement process has been designed by Pay.UK and will require all firms to use their case management system. Most APP fraud victims should be reimbursed within five business days and there are additional protections offered for vulnerable customers. There will be an extension available in cases where the bank has suspicion of the validity of the claim.	APP scams happen when someone is tricked into sending money to a fraudster posing as a genuine payee. Every year thousands of individuals and businesses fall victim to APP scams, which can have a devastating impact on people's lives. The latest figures show £459.7 million was lost to APP scams in 2023. **The new rules have consumer protection, ensuring fair treatment and reducing the risk of fraud.** **Adhering to the rule is critical to avoid penalties and ensures regulatory standards.** **There may be some operational and financial efficiencies gained long term by streamlining processes and preventing / detecting more fraud.**	➢ Operational processes – examine the efficiency and effectiveness of processes related to the prevention, detection and response to APP transactions, including customer interaction, investigations and evidence gathering and relevant MI in relation to complaints referred to the FOS ➢ Risk management – full framework review providing a broader, high level review of the governance structure, policies and training provided to staff ➢ Compliance review – assessing adherence to new APP rules and Consumer Duty requirements. **Indicative number of days required - 10-25 depending on depth and breadth of review, size of organisation and complexity of detection solutions involved.**

Economic Crime

Other emerging topics

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
AML – Transaction monitoring	Firms must conduct ongoing monitoring of the business relationship with their customers. Monitoring arrangements should be risk based, driven by the nature, size and complexity of a firm's business and form part of its financial crime control framework. Ongoing monitoring of a business relationship includes scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with a firm's knowledge of the customer, its business and risk profile.	➢ Effective Transaction Monitoring is a key control for all firms subject to FCA regulation and / or supervision ➢ Deficiencies in firms' approaches to transaction monitoring are present in the vast majority of FCA supervisory and enforcement action ➢ In April 2024, the FCA launched a consultation aimed at making enhancements to its Financial Crime Guide, including proposals to provide more guidance to help firms in adopting and maintaining automated Transaction Monitoring systems. Whilst the results of the consultation have not yet been published, firms' approaches to Transaction Monitoring are clearly a key agenda item for the FCA ➢ In July 2024, the Wolfsberg Group, a prominent association of global banks dedicated to enhancing financial crime compliance standards, released a statement on effective monitoring for suspicious activity. The Group's statement is a call to action for firms to enhance their monitoring systems. This means that firms must assess their own risk profiles and tailor their monitoring systems accordingly, rather than adopting a one-size-fits-all approach.	**Design effectiveness** ➢ Assess the appropriateness of alert rules / scenarios / typologies / thresholds including how these are tailored according to the inherent risks, expected nature and frequency of activity of the Firm and its customers ➢ Assess and evidence a transaction risk assessment in order to support the Firm's decision-making process in implementing appropriate thresholds for rules and scenarios ➢ Assess the adequacy and appropriateness of the Firm's procedures in providing guidance and expectations on the level of investigation undertaken to discount/escalate alerted activity and to evidence risk-based judgement and rationale for decision-making where appropriate ➢ Assess the adequacy and appropriateness of the Firm's transaction monitoring procedure in providing staff operational guidance on how to work and navigate the Firm's transaction monitoring tool. **Indicative number of days required** – **10** **Operational effectiveness** ➢ Assess the quality of investigations conducted into Transaction Monitoring alerts. **Indicative number of hours required – 0.75 hours per Transaction Monitoring alert + 0.25 hours of QA**

Economic Crime

Other emerging topics

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
AML – Politically exposed persons (PEPs)	➢ The UK is one of more than 200 countries and jurisdictions committed to international standards that require additional checks on individuals who hold significant public functions - PEPs ➢ The UK Parliament has written those standards into domestic law through the Money Laundering Regulations 2017 (as amended) ➢ The AML requirements for PEPs also extend to their relatives and close associates ('RCAs') ➢ The reason for these global standards is the increased risk that PEPs, and those connected to them, may be at risk of being targeted for bribery and corruption ➢ However, controls must also be balanced with the need for good customer treatment.	➢ In September 2023, in the wake of the Nigel Farage 'debanking scandal', the FCA launched a review to look carefully at firms' arrangements for dealing with PEPs based in the UK ➢ On 10 January 2024 the Money Laundering and Terrorist Financing (Amendment) Regulations 2023 ("Amending Regulations") came into force. The Amending Regulations provided changes to the Enhanced Due Diligence requirements in relation to domestic (i.e. UK) PEPs ➢ On 18th July 2024, the FCA issued its much-awaited update to its September 2023 review of firms' treatment of PEPs. As part of its initial review, the FCA contacted over 1,000 UK PEPs and received 65 responses. Based on the feedback received and its observations, the FCA has advised firms that they must enhance their efforts to ensure that individuals with political connections and their families, are treated fairly and without undue prejudice. The FCA has reviewed the current approach and found that, while most firms are not subjecting PEPs to unnecessary scrutiny or denying them services based on their status, there is room for improvement.	**Design effectiveness** ➢ Assess the adequacy and effectiveness of the Firm's systems and controls in establishing whether the customer, beneficial owner, or key individual(s) is a PEP ➢ Assess and provide evidence that the materiality and level of risk associated with identified PEP and associated PEP relationships has been adequately assessed and informs ongoing EDD measures ➢ Assess the adequacy and effectiveness of the Firm's approach to conducting EDD for PEPs and other high-risk customers ➢ Evaluate the adequacy and appropriateness of the Firm's ongoing monitoring arrangements for PEPs and high-risk customers. **Indicative number of days required** – 10 **Operational effectiveness** ▶ Assess the adequacy of the Due Diligence conducted on customers with PEP exposure **Indicative number of hours required** – 2.5 - 3 hours per customer file + 1 hour of QA

Economic Crime

Other emerging topics

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Market abuse	The objective of this review is to assess and provide assurance over the design and operating effectiveness of the policies and procedures implemented by the Group in order to comply with the provisions of MAR which came into force on 3 July 2016.	1 of the FCA's 13 public commitments, outlined in their 2024 / 25 Business Plan includes taking assertive action on market abuse. In particular, the FCA will significantly increase capability to tackle market abuse which will include: ▪ Increasing the ability to detect and pursue cross-asset class market abuse ▪ Build on analytics capabilities such as network analysis and cross-asset class visualisations ▪ Develop improved market monitoring and intervention in Fixed Income and Commodities, covering both market abuse and market integrity.	➢ Review and assess the design effectiveness of the governance and oversight arrangements around market abuse, management information 'MI' produced and escalation of matters, minutes of relevant Committee meetings ➢ Assess the sufficiency of the Firm's market abuse risk assessment by reference to the scale and nature of the Firm's activity, regulatory expectations and industry best practice ➢ Assess the design effectiveness of the Firm's market abuse monitoring arrangements, including: the systems and processes used for surveillance of the Firm's (and its clients') trading activity; the appropriateness of the system rules and alerts to identify potential market abuse; and second line monitoring and oversight ➢ Assess the design and operating effectiveness of the personal account dealing policies and procedures currently in place, with a focus on the processes for approval, monitoring, and reporting of employees' personal trades. **Indicative number of days required – 15**

04

Prudential Regulation Hot Topics

Oivind Andresen
Principal

oivind.andresen@bdo.co.uk

Giovanni Giro
Associate Director

giovanni.giro@bdo.co.uk

Prudential regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Basel 3.1	Basel 3.1 will come in force on 1 July 2025 (although a short delay is likely). Basel 3.1 is the PRA's take on the final steps of the Basel 3 rules. Focus is on new risk weights for credit risk under the standardised approaches and the introduction of a capital floor for internal models based exposures. Smaller firms can elect to opt into the PRA Small and Simple Regime.	Firms must consider the Basel 3.1 impact given that it is likely to have a material impact on capital (ICAAP) and regulatory reporting.	▶ Assess the design and operating effectiveness of Basel 3.1 calculations ▶ Assess the Risk Management Framework that supports the B3.1 outcomes and ensure that the Firm is fully compliant with the new UK CRR B3.1 requirements. **Indicative number of days required – 12-15**
Solvent wind-down	The PRA expects all regulated firms to have solvent wind-down plans in place and prescribes a specific structure and content. This is a requirement from 2025 onwards. Firms must maintain processes and adequate financial resources to enable an orderly wind-down without causing undue economic harm to consumers or to the market.	The increasing regulatory scrutiny over wind-down planning is apparent from the PRA's new PS5/24 and their recommendations to firms undergoing a SREP review. Firms are required to produce wind-down plans as part of the recovery planning process. UK CRR firms are often required to provide evidence of assurance reports to the PRA, to demonstrate that the wind-down planning processes are effective to execute an orderly exit. The PRA has also published multiple papers over the past 2-3 years focusing on their concerns with the impact of firm's failure and their high expectations of firms managing orderly wind-down processes.	▶ Assess that wind down planning and how it meets regulatory requirements ▶ Assess that wind-down planning is undertaken in line with the structure recommended by the FCA in the WDPG sourcebook and FCA's finalised guidelines in FG20/1 and the feedback from the thematic review TR22/1 ▶ Assess the adequacy of wind-down planning assumptions, the granular calculation of wind-down costs and the assessment of the capital and liquid assets required in wind-down ▶ For MIFIDPRU investment firms, assess the integration of wind-down plans in the ICARA process and the calculation of the own funds threshold requirements (OFTR) and liquid assets threshold requirements (LATR) ▶ Where group relationships are significant, assess how a firm manages the intra-group dependencies in a wind-down scenario in terms of financial, operational, and governance arrangement and has assessed group-wide impact ▶ Test the credibility, effectiveness, proportionality and operability of wind-down plans. **Indicative number of days required – 8-10 (20-25 if combined with a recovery plan review)**

Prudential regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Liquidity	The FCA's Principles for Businesses establish an overarching requirement for all regulated firms to maintain adequate financial resources. All prudential sourcebooks (MIFIDPRU, MIPRU, IPRU) establish a general solvency requirement and specific liquidity requirements. Since the pandemic, the FCA has increased its focus on liquidity, which is very high in their supervisory agenda for 2024/25.	All firms are required to meet the general solvency requirement and hold liquid assets that are sufficient to meet their liabilities as they fall due (including under financial stress) and complete an orderly wind-down. Liquidity risk can be greater in groups due to the impact of intra-group connectivity and financial dependencies. Throughout the pandemic a number of firms have faced material challenge to remain solvent and demonstrate long-term financial resilience. The FCA has provided thematic feedback and raised concerns on poor practice around liquidity risk management and the adequacy of liquid assets held. The FCA has also started issuing direct requests to larger firms to improve their liquidity risk management framework and demonstrate that they have reliable contingency funding plans.	▶ Assess the design and operating effectiveness of liquidity risk management frameworks ▶ Assess the processes for the calculation and monitoring of liquidity requirements, both for ongoing operations and to cover wind-down costs ▶ Assess the liquidity stress testing and contingency funding plans in place to ensure that firms identify severe and plausible assumptions of financial stress and viable solutions to prevent/rectify a cash shortfall ▶ Assess group-wide liquidity arrangements and how firms manage intra-group dependencies and liabilities ▶ Test the cashflow analysis and ongoing management of inflows/outflows to ensure the reliability of liquidity data sources. **Indicative number of days required - 12-18**
Regulatory reporting	The FCA expects all MIFIDPRU investment firms to report financial information via the RegData platform accurately and timely. In the FCA's business plan 2024/25 as well as standalone papers, the FCA has confirmed the importance of accurate reporting and their intention to initiate supervisory work on firms' data items and reporting processes in 2025.	The feedback provided by the FCA in their thematic reports published first in February and then in November last year, shows that some firms have submitted incorrect or inconsistent data in their MIF returns. Regulatory returns provide key financial information on capital and liquidity adequacy to the FCA, and any errors may represent a symptom of a material underlying issue with a firm's ability to apply the correct methodology or maintain sufficient financial resources to meet its requirements.	▶ Assess the effectiveness of regulatory reporting processes including governance arrangements for internal review and validation ▶ Assess the accuracy and completeness of regulatory returns submitted by investment firms in accordance with the reporting guidelines in MIFIDPRU 9 and SUP16 ▶ Test the integrity of data sources and the accuracy of reportable data according to the MIFIDPRU methodology for the calculation of financial information. **Indicative number of days required - 15-22**

05

Governance, Risk and Conduct Hot Topics

Shrenik Parekh
Director

shrenik.parekh@bdo.co.uk

Nicola Ball
Director

nicola.ball@bdo.co.uk

Governance risk and conduct regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Consumer Duty embedding (All)	Consumer Duty came into force on 31 July 2023 for products and services for retail consumers. There are four consumer outcomes: - Products and services - Price and Value - Consumer Understanding - Consumer support.	The Consumer Duty is the FCA's flagship consumer regulation to improve consumer outcomes. It overlays existing conduct of business requirements with a new principle, rules and guidance. It has been vigorously supervised by FCA over the last year. Firms should have defined good outcomes for their consumers and have systems and controls in place to assess consumer outcomes and make changes where required.	▶ Assess the embeddedness of the Consumer Duty through the active use of comprehensive MI, reporting, root cause analysis, decision making and action execution ▶ Assess the level of engagement at senior committees and the Board in overseeing decision making in line with defined Consumer outcomes ▶ Test a sample of MI reports to assess comprehensive scope, quality of MI, root cause analysis and actions taken. **Indicative number of days required - 10-20**
Consumer Duty **Closed Book implementation** **(Higher risk: Investments, Insurance, Banking, Mortgages)**	Consumer Duty implementation for closed books (products and services no longer sold after 31 July 2023) came into force on 31 July 2024. Firms are expected to take action on closed products that fail to meet regulatory expectations.	Closed products may provide poor outcomes for consumers where they are: - No longer suitable or relevant for the consumer eg customer ineligible for product benefits - Unable to demonstrate fair value eg high exit fees - Insufficient information about consumers, including where they are uncontactable. FCA expects firms to review legacy products and make changes and expects to take supervisory action.	▶ Assess the completeness of firms' closed book project implementation plan for scope of products, consumers and areas to assess such as price and value, consumer data, consumer eligibility, consumer contact efforts ▶ Assess the execution of the project within timescales, actions remaining, actions taken and whether these are complete ▶ Assess reporting to Firms' governing body, and Annual report of the Board for status reporting and completion assessment. **Indicative number of days required - 10-20**
Consumer Duty governance	Boards to appoint a Consumer Duty Champion who should be an INED.	The FCA expects the firms' governing body to take ownership of consumer outcomes as part of strategy setting and ongoing oversight of executive managements' delivery of good consumer outcomes.	▶ Consumer Duty Champion (INED) appointed to the Board ▶ Assess evidence of Board oversight through agendas and minutes ▶ Evidence of Board and Consumer Duty Champion engagement through agendas, minutes and interviews. **Indicative number of days required - 10-15**

Governance risk and conduct regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Product governance **Consumer Duty supplements existing Conduct of Business requirements (e.g. PROD 3,4, CONC)**	All firms are required to have a robust product governance framework for approving new products and reviewing existing products in line with regulatory requirements for target market, distribution strategy, price and vale, and vulnerable customers or customer cohorts.	Longstanding industry failures to design and distribute products that are suitable for the customers in the target market. The Product and services outcome essentially requires firms to deliver products and services to consumers that are fit for purpose. Significant FCA focus on Product Governance.	▶ Assess the design of the Product Governance arrangements (TOR, Scope, seniority, reporting, MI frequency) ▶ Assess the execution of the Product Governance process and delivery in line with TOR, Root Cause Analysis, action taken. Should be sufficiently detailed evidence to underpin statements and decisions ▶ Assess descriptions of target markets, distribution channels for completeness and sufficient granularity. Assess accuracy of defined roles and responsibilities for product manufacture and distribution (including co manufacture) ▶ Assess communication and information sharing along the distribution chain for target markets and fees and charges information ▶ Test a sample of products and distribution channels have been reviewed under the Product Governance TOR and outcomes, decisions and actions are sufficiently detailed and supported by evidence. **Indicative number of days required – 15-25**
Price and value	Price and Value assessments are required for new and existing products to confirm they offer fair value to consumers in the target market.	Significant regulatory challenge to fees charged vs value consumer receives. - Wealth – significant supervisory action on ongoing service fees and charges (customers charged and services not delivered) - Banking – failure to pass on changes in interest rates - Credit – High Cost Short Term (HCST)/pay day lending.	▶ Assess the scope of Fair Value Analysis (FVA) which should be completed for each product and service and have sufficiently granular analysis of customer cohorts ▶ The FVA methodology should be clearly documented and consistently applied, it should cover costs, total end to end price paid by consumer, value and benefits of the product to the customer. There should be identification of customer cohorts and analysis that Fair Value is delivered to cohorts (including vulnerable consumers) ▶ For Product Manufacturers assess a Fair Value Assessment (or AoV under PROD 3 from AMs) has been produced for each product and has been sent to all distributors ▶ For Distributors assess all products distributed have a Product Manufacturers assessment of Fair Value ▶ Results should be reported to a governing body, eg through the Product Governance framework ▶ Test a sample of FVA to Assess the methodology has been followed, including cohort analysis) and has detailed evidence to support conclusions and decisions that products and services meet fair value. Test governance, decisions and actions taken. **Indicative number of days required – 15-25**

Governance risk and conduct regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Customer support (All)	Consumer Duty and requirements in PRIN 2A, DISP and COMP set out how consumers should be supported, how to handle complaints (process, timelines, FOS rights) and remediation.	Consumer Duty sets out expectations for consumer understanding and consumer support, including addressing behavioural biases in consumer processes to access information. DISP sets out requirements for handling consumer complaints, including consumer rights to refer to the FOS. FCA expects consumers to be remediated where things go wrong. Complaints are a key source of MI about consumer outcomes and FCA expects root cause analysis and actions to be taken to improve consumer outcomes as part of governance processes. Claims Management companies can target firms where they think there is an opportunity to create significant redress for consumers.	▶ Assess complaints policy, access to information about making a complaint, information to consumers who make complaints ▶ Assess processing timescales to identify any complaints processing backlogs ▶ Assess compliant levels with FOS (numbers referred and overturn rates) and Management awareness, root analysis completed and actions taken ▶ If any remediation programmes are underway, assess population scoping, redress methodology, timeliness of redress payments, project management governance and reporting, including notifications to the FCA. **Indicative number of days required - 10-15**
Appointed representatives	The Appointed representative regime new rules and guidance came into effect on 08/12/2022, including new reporting requirements to the FCA. PS 22/11	The Appointed Representative (AR) regime has been a feature of financial services legislation since 1986, giving access to the financial sector for those businesses not regulated. After some significant issues, the FCA clarified and increased standards for on boarding and oversight of ARs and Introducer Appointed representatives (IAR). The FCA now has a separate supervisory department assessing how firms are meeting the new standards. Firms with ARs are expected to: - Complete increased due diligence for onboarding - New FCA registration and notification requirements - Ongoing annual assessments of fitness and propriety, including assessment of financial interests and solvency - Increased governance and oversight arrangements - There are lesser requirements for IARs.	▶ Identify whether the firm has ARs or IARs, and if so how many. Test these are correctly registered with FCA by reviewing the FCA Register ▶ Assess onboarding processes and controls, depth of due diligence in line with regulatory requirements, concessions and approvals governance and decision making ▶ Assess contracts set out termination rights by Principal ▶ Assess ongoing monitoring and oversight including completion of annual review processes/financial assessment ▶ Test a sample of annual reviews to confirm these align to processes ▶ Assess MI (complaints, suitability advice data, competence data) and evidence of any indicators that could raise an issue about an AR. Assess action taken. **Indicative number of days required - 10-20**

Governance risk and conduct regulation

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Governance and oversight	Firms should have robust governance, oversight and systems and controls to manage business in line with regulatory expectations.	The FCA and PRA have issued a number of s166 reviews over the last year all of which have an element of assessing adequacy of governance and oversight to implement new regulatory requirements, such as Consumer Duty, and assess these have embedded. The following topics have been raised and may be particularly relevant for some firms: - Operation of a 3 lines of defence model (design and separation of first and second line; effective operation e.g. understanding, risk ownership, operation of first line controls) - Adequate governance and decision making including MI, root cause analysis and actions - Conflicts of interest management, particularly within Groups of companies - Adequacy of resources in second line - Oversight of suitability of advice for investment, particularly income in retirement and high risk products (Pension transfers, Equity release) - Oversight of affordability and creditworthiness assessment processes for credit and lending products - Oversight of financial promotions for high risk products.	▶ Assess clarity of 3LOD model (design and operational effectiveness) through review of design, clarity of separation of first and second line ▶ Assess scope and coverage of Compliance function, including adequacy of monitoring plan to risks in business ▶ Assess adequacy of compliance resources, particularly if the business has changed or/and increased in scope ▶ Assess controls in place, and adequacy and competence of resources for assessing product suitability. Note testing of suitability would require specialist resource ▶ Controls in place for assessing adequacy of affordability and creditworthiness. Note testing of creditworthiness or affordability would require specialist resource ▶ Assess controls in place around high risk products (e.g., identification of 'high risk' products) ▶ Assess compliance awareness of regulatory changes and effective processes for business change implementation to meet new regulatory requirements. **Indicative number of days required - 10-20**
Vulnerable consumers	FCA thematic review report on treatment of vulnerable consumers due December 2024. Guidance on treatment of vulnerable customers published 23/02/21 FG 21/1.	Requirements set out in the FCA's vulnerable consumer guidance and Consumer Duty. Firms are required to have systems and controls in place to identify and support vulnerable consumers. The definition is wide ranging, the FCA's Financial Lives Survey (20/10/2022) found 47% of UK adults showed one or more characteristic of vulnerability. Vulnerability is considered across four key drivers: health, life events, resilience and capability. The forthcoming thematic review report could trigger additional supervisory interventions. Key risk indicators include insufficient identification of vulnerability, inadequate MI and testing, poor root cause analysis and governance.	▶ Suggest consider potential risks post Thematic Review report. **Indicative number of days required - 10-20**

FCA Horizon Scanning - CONDUCT H2 2024

View of regulatory change and FCA hot topics in H2 2024 – post election

Context - year to date and headline points

FCA three-year strategy still has a year to run with a refresh of activities due in April 2025. The strategy has three core elements:

- *reducing and preventing serious harm*
- *setting and testing higher standards*
- *promoting competition and positive change.*

The FCA's focus and hot topics - conduct

- Consumer Duty: Annual Board report; closed books; price and value particularly in GI and Wealth Management; product governance
- Vulnerable consumers – thematic review report due end 2024
- Private wealth – focus on fees and charges, adviser take on and consumer portfolio churn. Part of a larger reform of pensions to improve advice quality and value for money of DC pensions, including assessment mechanism for V4M
- Credit sector – announcement on regulation of BNPL expected. Continued fall out from BiFID project
- Motor finance mis selling investigation announcement delayed to May 2025, consumer complaints now at over 1million. FCA says more likely a question to answer
- ESG, crypto and reform of capital markets remain the biggest strategic policy areas of reform to deliver UK competitiveness agenda
- Operational Resilience final embedding deadline is March 2025
- AI was not included in the Kings speech, however growth of AI is a CMA priority with remit over financial services, and anticipated as governance challenge for FS firms
- Access to Cash reforms to maintain access for consumers, small businesses and charities. Requirements imposed for certain banks
- FCA planning strategy for financial inclusion. Unclear at present.

Economic outlook from OBR and BOE

OBR next update due October 2024. BoE expects inflation to rise temporarily to 2 ¾ % in second half of 2024 and forecasts that lower inflationary pressures will lead to inflation falling below the 2% target in 2026. Focus on inflation to ensure it stays low. Interest rates cut to 5%. (01.08.24Commons Library) The ONS estimates GDP has grown by 0.6% in the quarter April – June.

Political Outlook

- First Labour Budget due 30 October 2024 followed by Mansion House Speech will provide more detail on strategic focus
- Labour Government FS priorities for next Parliament – published in Kings Speech July 2024
  - Pensions reform – wide ranging legislation
  - Cyber resilience – new bill to increase regulator powers
  - Bank Resolution (recapitalisation) Bill – enables BoE to recapitalise small banks from FSCS funds
  - Digital Information and Smart Data bill – enable innovative uses of data to boost the economy.
- HMT expected to announce regulation of BNPL.

GEO-Political Outlook

- US presidential Election – November 2024 - Potential for instability impacting financial markets
- Middle East – escalation has a potential to destabilise recovery and cause inflation to rise.

06

Tax Governance Hot Topics

Martin Callaghan
Partner

martin.callaghan@bdo.co.uk

Tax Governance: Senior Accounting Officer

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Senior Accounting Officer (SAO) compliance	Finance Act 2009 requires 'large' UK businesses (those with annual turnover of £200m or more or balance sheet assets of £2bn or more, (the thresholds are applied on a group-wide basis) to submit to HMRC appropriate certifications that they have appropriate tax accounting arrangements in place. There are potential financial penalties (both corporate and personal) for failure to comply with the requirements of the SAO regime.	Poor tax governance can expose a business to a number of potential issues, including: • reputational risk with tax authorities, regulators and other external stakeholders • financial risk either as a result of non-compliance (with associated penalties, interest and lost management time dealing with enquiries) or a failure to access appropriate tax credits and allowances. The specific key drivers for compliance with the SAO regime are: • Compliance is a statutory obligation for large businesses • Increased emphasis by HMRC on good governance and risk management, with SAO compliance providing visible assurance to HMRC • The risk of financial penalties and adverse reputational impact with HMRC • SAO compliance additionally provides internal assurance to the Board and others as to the robust nature of a business' tax operating model.	Initially we can issue an online questionnaire focussed on tax governance and SAO compliance specifically to provide us with a snapshot of the control environment and areas of potential focus. This could include the following areas: ➢ Assessing controls and procedural documentation to ensure compliance with regulatory requirements ➢ Conducting walkthroughs and interviews with key tax and finance stakeholders and others (e.g HR function) as appropriate to gain an understanding of the control environment ➢ Benchmarking the internal SAO process to HMRC Guidance and our knowledge of HMRC's approach ➢ Identifying good practice, design control weaknesses and recommendations for improvements (where relevant) to strengthen and enhance the SAO framework. We are able to draw on our extensive experience of conducting SAO reviews to ensure all relevant lessons learned and regulatory expectations have been adequately captured. **Indicative number of days required – 15**

Tax Governance: Corporate Criminal Offence

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers - Why should this be considered for audit plan?	Indicative scope areas
Corporate Criminal Offence (CCO)	Part 3, Criminal Finances Act 2017 means that if an "associated person" of a business criminally facilitates tax evasion, and the business is unable to demonstrate that it had reasonable procedures in place to prevent such facilitation, the business is guilty of a criminal offence. The legislation took effect in 2017 and applies to all UK businesses and any non-UK business with some UK nexus.	The legislation is broad in geographic scope, applying both to instances of UK and non-UK tax fraud and, in certain circumstances, both UK and non-UK corporates could be prosecuted. The consequences of a prosecution includes unlimited fines, reputational damage and the likelihood of regulatory sanction. The specific key drivers for compliance with the CCO legislation are: • HMRC consider the Financial Services sector generally to be 'High Risk' in relation to the CCO legislation • The potential downside of non-compliance is significant, with potential criminal prosecution, unlimited financial penalty and significant adverse reputational and regulatory impact • CCO compliance forms a part of HMRC Business Risk Review with a business being rated high risk for governance if no steps are taken to comply with the legislation • CCO compliance is a common element of M&A due diligence and can be raised by Financial Institutions as part of financing / re-financing decisions.	▶ We review key documentation relating to the area including risk assessments, policies and procedures in order to build our understanding of the procedures in place and consider the sufficiency of the documented control environment ▶ The documentation is evaluated for suitability, taking into account the sector, size and complexity of the business ▶ As a key element of the CCO defence, we review any CCO risk assessment carried out by the business and benchmark the risk assessment against our experience of leading practice and working with similar organisations ▶ Conduct interviews with key staff to establish awareness of the legislation as well as the controls and governance arrangements that are in place ▶ Specifically consider the adequacy of mandatory CCO training rolled out within the business. **Indicative number of days required - 15**

Tax Governance: Tax Control Framework and Business Risk Review

Hot Topics to be considered for the 2025 plan

Topic	Overview and key dates	Drivers – Why should this be considered for audit plan?	Indicative scope areas
Tax Control Framework and operating effectiveness	Tax governance and risk management are increasingly on the Board and Senior Management agenda, as well as front of mind for a wide range of external stakeholders including shareholders, potential investors and, of course, tax authorities and the Regulators. In addition, those large businesses with a Customer Compliance Manager ('CCM) will be subject to periodic Business Risk Review ('BRR+').	Poor tax governance can expose a business to a number of potential issues, including: • reputational risk with tax authorities, regulators and other external stakeholders • financial risk either as a result of non-compliance (with associated penalties, interest and lost management time dealing with enquiries) or a failure to access appropriate tax credits and allowances. Specific drivers for focussing on this are: • HMRC is focussing its efforts and supervisory resources on the firms most likely to provide the greatest yield – i.e., those they consider to be at highest risk of non-compliance. They are adopting a risk-based approach which moves away from time and resource-heavy enquiries and investigations. For large businesses, this will involve a periodic BRR+ (frequency based on the designated risk rating), which will involve assessing a business across all taxes against 24 low risk indicators. There has been a significant increase in the number of BRR+ taking place, as well as the level of detail and level of resource required to respond to BRR+ requests • The Environmental, Social and Governance ('ESG') agenda. Stakeholders in a firm want to know that the firm has a set of strong principles and values that extends to its approach to tax and governance framework. *Please see the ESG and Sustainability section.*	▶ We review a number of areas including: • Tax Governance and Strategy • Tax Risk Management • Tax Performance Effectiveness. ▶ Control documentation (eg Tax Strategy / Tax Policy / Tax Process) is evaluated for suitability, taking into account the sector, size and complexity of the business ▶ Walkthroughs and interviews are conducted with key tax and finance stakeholders and others (e.g HR function) as appropriate ▶ In addition, a technical review of a specified area (or type of tax, eg corporation tax / employment duties/ VAT / bank levy) can be incorporated in the scope of work in order to establish with greater certainty the effectiveness of the designed control environment. **Indicative number of days required - 15**

FOR MORE INFORMATION:

Paul Gilbert

+44 (0)7890 323 336
paul.gilbert@bdo.co.uk

www.bdo.co.uk

XXXXXXX