INTERNAL AUDIT SUPPORT

BANKING & BUILDING SOCIETIES UPDATE

October 2022

IDEAS | PEOPLE | TRUST

BDO

BDO FS INTERNAL AUDIT CONTACT POINTS

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 (i.e. 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

RICHARD WEIGHELL
PARTNER

+44 (0) 7773 392 799
richard.weighell@bdo.co.uk

CHRIS BELLAIRS
PARTNER

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

BRUK WOLDEGABREIL
ASSOCIATE DIRECTOR

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

CONTENTS

Click on a section below to take you straight there

COST OF LIVING CRISIS: REMUNERATION AND INCENTIVE ARRANGEMENTS FOR FIRMS

GEORGIA JONES
ASSISTANT MANAGER

44 (0) 782 389 8655
georgia.jones@bdo.co.uk

SHRENIK PAREKH
DIRECTOR

+44 (0) 758 301 8535
shrenik.parekh@bdo.co.uk

▶ FCA Letter to Remuneration Committee Chairs

The Regulator has recently reiterated the importance of firms' duties to their consumers and reinforced that any alterations to remuneration should not be made at the expense of customer good outcomes.

It will be paramount for firms to ensure the funds available for remuneration are adequately distributed and remain in line with the firms' business strategy, values as well as its financial performance and ongoing financial viability.

Firms will now have to strike a balance between ensuring employees are adequately remunerated, and thereby motivated, to generate financial performance and good consumer outcomes.

This puts the strength of a firm's culture and control environment to the test.

▶ What the Cost of Living Crisis means for firms: Culture and Accountability

The FCA letter to Chairs of Remuneration Committees (August 2022) highlighted that "*individuals should be held accountable for their conduct, competence with a clear, strong, and evidenced link between behaviours and remuneration outcomes*". Particularly for senior management, firms will need to demonstrate and evidence that any remuneration increases have been made in line with the firm's cultural practices and employee conduct expectations.

Some of the important steps in creating and maintaining a strong culture include:

- Creating an environment of trust where employees can speak up;
- Creating an accountability framework where performance across a range of factors is measured and rewarded – the positive and negative;
- Ensuring diversity from a range of perspectives;
- Monitoring and measuring outcomes to ensure these align with firm values.

▶ What the Cost of Living Crisis means for firms: Consumer Obligations

The New Consumer Duty outlines the FCA's new and higher expectations on the level of care and customer service provided to consumers throughout the product lifecycle. As such, firms will need to have a greater consideration for supporting customers through the current crisis as well as being alert for vulnerability characteristics. Key questions Remuneration Committees and senior management should ask themselves include:

- What controls are in place to ensure that incentive arrangements or KPIs are not encouraging non-compliance with procedure or poor consumer outcomes? For example, could employees be pressuring consumers into buying a product or service to take advantage of commission or incentive structures?
- Do our employees fully understand their regulatory obligations to consumers? For example, can all employees clearly articulate these when questioned?
- Does our Vulnerable Consumer Policy and wider policies and procedures clearly outline the classifications for vulnerability and the different options available to help these consumers?
- Have we considered the key impacts of the current cost of living crisis on our customer base and come up with realistic and appropriate means to offer support to customers who have indicated they are struggling?
- Are our complaints handling procedures robust enough to clearly identify root causes of discontent and where improvements are needed in the customer lifecycle? In addition, are complaints handling processes fair and in line with regulatory expectations?

▶ What should Internal Audit teams be thinking about?

Key questions the Internal Audit team should have for Remuneration Committees and senior management include:

- Are current KPIs and performance reviews adequately balanced between financial metrics as well as non-financial metrics, such as conduct, adherence to regulatory requirements and internal policies and procedures, customer satisfaction ratings, communication skills, teamwork, and leadership skills?
- Has the Remuneration "Pot" been appropriately and proportionally allocated amongst employees that have met or exceeded performance targets? Are there any individuals who are currently disproportionally remunerated in comparison to their colleagues?
- Are there any conflicts of interests in the performance review or remuneration arrangements? For example, could individuals be recommending lower ratings to boost their own performance? Are there C-Suite individuals that are party to their own remuneration discussions and decisions?
- What message and tone will Remuneration allocations send to employees and the wider market? For example, will there be an implication that the bulk of rewards are solely given to "rainmakers" or senior individuals?
- What MI is in place to demonstrate good consumer outcomes have been achieved alongside a strong financial performance?

Whilst firms may feel an increased pressure to remunerate staff to maintain current talent, it is likely that remuneration arrangements will receive increased scrutiny from the regulator. Accordingly, firms and remuneration committees will need to be able to, now perhaps more than ever, justify decisions made around remuneration arrangements.

ESG DISCLOSURES IN 2023: WHAT INTERNAL AUDIT TEAMS SHOULD LOOK OUT FOR

GLORIA PEREZ TORRES
MANAGER

+44 (0) 7583 689 198
gloria.pereztorres@bdo.co.uk

▶ Financial sector under pressure to report on climate-related financial information

Banks and building societies' responses to the risks and opportunities posed by climate change and the transition to a low carbon economy are at the forefront of the minds of investors, regulators and the wider society.

The PRA issued its climate-related supervisory expectations for regulated firms in 2019 within its Supervisory Statement (SS/ 3/19), with a deadline for firms to have embedded it's requirements them by the end of 2021.

PRA expects firms to engage with wider initiatives on climate-related financial disclosures such as those set out by the Taskforce on Climate-related Financial Disclosures ("TCFD"). Further, the FCA in it's ESG Strategy, manifested their commitment to transparency and their policy alignment with the government's position on TCFD reporting requirements.

Therefore, TCFD has been the key initiative most UK firms have adhered to date and some firms have chosen to also to report on how they are contributing to the achievement of the UN Sustainable Development Goals by 2030, mainly from a social perspective.

▶ The FCA analysis and feedback on published TCFD disclosures

On 29 July 2022, the FCA published their first views on the quality and coverage of TCFD disclosures made by premium listed commercial companies.

This followed the publication of the FCA's 2020 Policy Statement (PS20/17) which introduced a climate-related disclosure rule for premium listed commercial companies, requiring those companies to disclosure in line with the TCFD framework, or to explain why disclosures were not made.

This analysis by the FCA represents a 'head up' for banks and building societies.

In due time, their disclosures will be under the FCA's and PRA's scrutiny. Things to watch out for include:

- Making statements that the company is making disclosures consistent with the recommended TCFD framework, but with insufficient content to substantiate them;
- Publishing insufficient quantitative elements with respect to scenario analysis data, metrics and targets, and lacking data methodologies and sufficient audit trail.

▶ Financial Reporting Council analysis of TCFD disclosures

More lessons can be learnt from the Financial Reporting Council ("FRC") analysis of disclosures by premium listed companies.

The FRC's July 2022 feedback reported some level of maturity in the information published by 'companies that were better prepared for the reporting requirement'. However, it raised concerns that the narrative and financial statements disclosures were insufficient within a number of statements.

Learning from the FRC's feedback, areas where banks and building societies need to ensure the narrative and information provided is sufficient include:

- The granularity and the level of detail in explaining the potential impact of climate change on the business, sector and geography;
- Explaining how opportunities from decarbonisation relate to dependencies on new technologies;
- The integration into other elements of the company's narrative reporting, e.g., business model and strategy, and how this has been assessed and prioritised;
- Explaining how materiality was applied to the disclosures and whether claims of alignment are appropriately substantiated.

▶ What should Internal Audit teams be thinking about?

Firms need to be aware that disclosures will be scrutinised by the public and by the regulator. The Internal Audit function can step up and report to management on whether the preparations will be sufficient and proportionate before the publications in 2023.

Considerations for the IA team include:

- **Management Information**: what is the current maturity of the firm's MI behind its climate related disclosures? Can the current disclosures reporting be vouched back to sufficient, reliable and relevant sources of information and are their reporting processes documented to evidence appropriate governance and review by the relevant senior managers?
- **Skilled resources**: are those involved in the preparation of disclosures appropriately skilled / experienced to be able to make sense of and, where required, challenge the metrics being produced? Where skills gaps have been identified, has the firm taken proactive steps to train its reporting staff or contract in the required skilled resources?
- **Documentation**: in many cases where the quality of disclosures have fallen short of expectations, its largely been driven by a lack of sufficient documentation to substantiate the claims made by the reporting firm. Documentation processes behind disclosures should be within the scope of any reviews for this activity.

MONEY MULES AND AUTHORISED PUSH PAYMENT (APP) FRAUD

SALLY FELTON
DIRECTOR

+44 (0) 7587 912 387
sally.felton@bdo.co.uk

► Background

When you consider that one of the UK's largest banks has a team of over 100 staff dealing with Authorised Push Payment (APP) fraud, you can start to get an idea of the volume of cases that banks across the UK (and globally) have to deal with on a daily basis.

APP frauds occur when a customer instructs their bank to make a payment, or bank transfer, to a recipient only to realise, some time later, that they have been scammed. Typical scenarios include:

- romance scams;
- investment scams;
- product scams.

These types of fraud are not new. Con artists have been socially engineering targets for years; the new development is the methods they deploy, especially in our digital age.

Despite the widespread press and media coverage regarding APP frauds, for example the BBC's "The One Show", some bank customers, especially vulnerable customers, will continue to fall victim to such scams and, as a result, the Financial Services industry has collectively sought to address the issue with some innovative solutions.

► Regulatory and industry efforts to prevent APP frauds

I recently attended the FCA's APP Fraud Tech Sprint, which included consultants, regulatory supervisors, technology providers and a selection of banks and payment service providers (PSPs). From the 3-day event, which included group work on current issues and assessing proposals for technology-based solutions, two key themes emerged:

- **Money mules vs. APP fraud**: some problem statements were APP related, and some were money mules, as a number of firms view the outgoing money from the mule account as an APP fraud. For example, a mule receives £1000 from a criminal gang, and is told to move £900 into another account keeping £100 for themselves as "payment" for the transfer. This outward payment of £900 is sometimes viewed as an APP fraud by some banks.
- **Challenges in Data Sharing**: banks, and other PSPs, have been seeking data sharing opportunities on fraud cases for many years. CIFAS, for example, holds millions of pieces of data on known fraud cases, but cannot share intelligence as widely as it's members would like due to apparent GDPR restrictions. Representatives from the Information Commissioner's Office were present at the event and confirmed that the "legitimate interest" rule meant that arguably data could be shared on known frauds, however data privacy challenge arise when dealing with suspicion of fraud (as opposed to known cases of fraud).

► PSR Consultation on APP scams reimbursement

The PSR's proposals for new measures to fight APP fraud, which include a requirement for almost all frauds to be refunded to the customer may have many different effects.

Banks and building societies may decide on one of two responses to the proposed measures:

- invest more money in APP fraud prevention and detection methods; or
- automate part, or as much as possible, of the APP claims process, thereby reducing the operational cost of vast numbers of staff manually processing claims which will inevitably, in most cases, be refunded to the customer.

The nature of many APP frauds are often low(er) value, high volume and generally hit retail and business customers' accounts.

Consider the volume of scam text messages sent by criminal gangs to trick people into paying £2.99 for postage, or to hand over their bank account details in order to claim their winter fuel allowance. While the initial cost to the scammer is low, the value of losses from these scams on its victims can be eye-watering, with entire life savings being transferred out by customers who genuinely believe they are investing sensibly, supporting those more vulnerable than themselves or purchasing a non-existent product.

► What should Internal Audit teams be thinking about?

- **Customer education:** IA teams should consider what controls are in place to manage customer communications on this fraud typology, how current the firm's guidance to customers is for the evolving threat landscape and how "lessons learned" from known fraud cases is being channelled back by the firm into customer support notices. Unfortunately, many customers could be too embarrassed to admit to their bank or building society they have fallen victim, and, therefore, the actual volume of fraud cases is much likely higher than currently estimated. Consider this point within the context of Consumer Duty.
- **Staff training:** awareness of the relevant parts of the FCA's guidelines around fraud should form part of the firm's training programme to ensure their front line staff are up to date with the latest requirements from the regulator. The FCA's Financial Crime Guide, Chapter 4, is a starting point.
- **Fraud culture**: Prevention of fraud, including assessing fraud risk, adopting a zero tolerance approach to fraud, etc., should be ingrained across a firm's risk management framework. Whilst prevention may come at a price, it is generally a far lower cost than responding to a fraud which will ultimately cost far more than the monetary amount of the fraud itself.

HEIGHTENED CYBER RISK: AN UPDATE ON THE LATEST NCSC GUIDANCE

BRAD DUFFELL-CANHAM
DIRECTOR

bradley.duffell-canham@bdo.co.uk

Cyber Risk has been high on the agenda of Audit Committees for a long time and it has been voted the number one risk for the last four years in the CIIA annual Risk In Focus survey. The consequences of a cyber-attack for organisations could be highly significant in terms of disruption to operations, inflicting reputational damage, theft or destruction of valuable or sensitive data, as well as the cost of fines by data regulators (and potentially ransoms paid to the hackers holding your data as hostage).

▶ The immediate threat has increased

In January 2022, the UK National Cyber Security Centre (NCSC) urged organisations to "bolster their cyber security resilience in response to the malicious cyber incidents in and around Ukraine" and published updated guidance. Reference was made to the destructive wiper malware which is being deployed against organisations in Ukraine and highlighting the risk that further attacks are likely to continue and may inadvertently spill over into organisations in other countries. This was followed by a report from the Joint Cyber Security Advisory highlighting the growing threat of ransomware attacks. There is also growing pressure on cyber insurance arrangements with "war exclusion" and "hostile act exclusion" contract language under scrutiny. This could impact claims, premiums and the ability of organisations to obtain cover. The NCSC guidance highlights the following areas:

- **Patching is an essential protection and needs to be kept up to date**. Where attackers are seeking to exploit a known security vulnerability they move fast, and it is organisations with ineffective patching programmes that are most vulnerable.
- **The organisation needs to understand its Internet-facing footprint**. Vulnerability scans / penetration testing of the whole internet footprint need to be performed regularly to ensure that everything that needs to be patched has been covered. At times of heightened risk, patching timeframes should be brought forward.
- **Access controls need to be checked carefully**. Extra focus should be applied to privileged or administrator access rights. Where possible multi-factor authentication (MFA) should be used and checked to confirm it is configured correctly. Third party access needs to be checked thoroughly, controlled and unnecessary access removed.
- **Anti-virus software and firewalls are important defences**. Antivirus should be active on all systems and updated correctly. Firewall rules must operate effectively.
- **Access to its backups is vital for an organisation to be able to recover its systems**. Backup routines must be running correctly and any backup failures addressed. The ability to restore from backups should be regularly tested.
- **Mandatory training in cyber security needs to be provided regularly**. Unless reminded, individuals can forget the level of threat, the importance of staying alert and reporting phishing or other suspected attempts at intrusion promptly.
- **Logs must be configured and monitored**, leveraging Intrusion Detection (IDS), Intrusion Prevention (IPS) and Security Information Event Management (SIEM) systems to examine, monitor and analyse the events taking place in the network - detecting potential threats and security policy violations.
- **Organisations should assume that their systems will be affected by a cyber attack at some point**. Incident response plans need to be checked and tested so that the organisation can deal with an incident effectively. Playbooks should be established detailing the response to a specific incident type including, in particular: malware/ ransomware infection; phishing email; or data breach. A test of the response plans should be performed as a priority if these scenarios have not been checked recently. The technical response should consider all key stages: Triage, Analysis, Containment/Mitigation, Remediation/Eradication, and Recovery.
- **The incident response team** also needs to be thought through carefully so that individuals with the right skills and authority to take decisions are available at very short notice, including third party dependencies and on-call arrangements with specialist suppliers in particular where they form part of the team.

▶ What should Internal Audit teams be thinking about?

With the NCSC's call to bolster cyber defences, Internal Audit should be looking at their audit plans once again to determine whether the assurance scheduled will be sufficient to meet the needs of the Audit Committee and the organisation during the current period of heightened risk.

Critical information assets ("crown jewels") need to be well protected with defensive and monitoring controls strengthened as far as possible and backups retained that cannot be rendered unusable by an attack. Incident response plans must be able to be activated rapidly with immediate availability of key individuals (including third party specialists) access to detailed information about the network and the tools necessary to respond. Competent cyber security staff are required.

Heads of Internal Audit may also wish to invest further in developing their own skills and understanding of the impact on the organisation of this important area so that they can credibility engage with colleagues in IT security and better explain the issues to the Audit Committee. Technical expertise on cyber is often sought from a co-source partner. Where this is the case, the internal audit team should look to work more closely with the partner team to build skills and maximise opportunities for knowledge sharing.

Cyber is likely to remain a key area for assurance for the foreseeable future.

ECONOMIC CRIME UPDATE: MAR TRADE SURVEILLANCE REQUIREMENTS

KAREN MONKS
MANAGER

+44 (0) 7769 283 619
karen.monks@bdo.co.uk

► Background

Market Abuse Regulation (MAR) covers the offences of insider dealing, unlawful disclosure of inside information and market manipulation. Two of the key changes introduced by MAR were the requirement to monitor for, identify, and report instances of attempted market abuse and the requirement to monitor orders for the purpose of identifying potential market abuse.

► FCA fines Citigroup Global Markets Limited

FCA recently fined Citigroup Global Markets Limited (CGML) £12,553,800 for failing to properly implement it's MAR trade surveillance requirements relating to the detection of market abuse. The fine was levied on the firm for failing to properly implement the requirements to detect and report potential market abuse since July 2016, when the rules took effect.

Additionally, it took CGML 18 months to identify and assess the market abuse risks the business may have been exposed to and the key risks the business needed to detect.

► Key Findings

The FCA found that by failing to properly implement appropriate trade surveillance controls as required by MAR, CGML could not effectively monitor its trading activities for certain types of insider dealing and market manipulation. In particular, the FCA found:

- CGML's implementation of the requirements of Article 16(2) of MAR was flawed, in particular the approach taken by CGML did not take into account the delegated regulations that supplemented the requirements of the Regulation;
- CGML did not complete its initial gap analysis of the MAR requirements until October 2017 and the output did not include a risk assessment of the 900 identified surveillance gaps. As a result, the output did not provide the business with the mechanism to identify the most serious market abuse risks affecting the business. Additionally, CGML did not complete a Market Abuse Risk Assessment, as required by Article 16(2), until December 2017;
- CGML failed to accurately track the implementation of the requirements of Article 16(2). In particular, the firm's MAR Working Group failed to provide sufficient oversight of the implementation of the requirements within the business;
- Additionally, CGML failed to define the scope of the MAR implementation objective within it's 2016 EMEA Compliance Plan and, as a result, compliance with Article 16(2) was not agreed as a condition for the completion of the objection;
- Finally, the FCA found that the CGML Board were wrongly informed in late 2016 that MAR implementation was complete.

► Wider Considerations – Market Watch 69

In May 2022 the FCA published a newsletter on market conduct and transaction reporting issues. This focused on firms' arrangements for market abuse surveillance and draws on the FCA's observations from engaging with the industry in respect of the requirements of Article 16(2) of MAR.

► Market Abuse Risk Assessments:

- The FCA expects firms to complete a comprehensive, accurate and up-to-date market abuse risk assessment in order to ensure that firms have effective surveillance coverage.
- The FCA recognises that there is no prescribed methodology for firms to follow when completing a risk assessment, but through supervisory work they have observed a range of methodologies for preparing the risk assessment. The FCA have commented that, in their experience, the most effective risk assessments involve consideration of the different types of market abuse and how they apply across different areas of the business and asset classes.
- The FCA has commented that where firms do not consider different types of market abuse, the different areas of business in which they operate, how that business is undertaken, and the different asset classes and instruments traded, firms may not be able to adequately identify market abuse risks and align their monitoring programme to them to ensure effective surveillance.
- The FCA has also commented that this may also be the case where firms do not review and update their systems as necessary to ensure they remain effective in the context of risks arising from changes in their business.

► Order & Trade Surveillance:

- The FCA has observed that surveillance arrangements are improving across industry, however, there continues to be variance. Throughout their supervisory work with firms they have seen examples of comprehensive, tailored systems, accurately aligned to risk assessments, however, they also observed instances of little or no monitoring taking place.
- Overall the FCA has noted that since the introduction of MAR, third-party system functionality in areas such as tailored calibration has progressed in recent years. However, some firms are unaware of these developments and so may not be making best use of the technology.

ECONOMIC CRIME UPDATE

► Policies & Procedures

- The FCA have observed that whilst firms have created a range of policies and procedures in relation to monitoring for market abuse, the approach to this varies. Some firms have clear, detailed and up-to-date policies and procedures and it appears these may provide a helpful reference point for staff and assist with work in areas such as alert review and escalation.
- The FCA have observed that some firms continue to have vague policies and procedures with limited detail and no guidance on what information to use or consider. As a result, where there is no such guidance, the information considered in alert review may be insufficient or incorrect, and alerts may be inappropriately closed rather than escalated. We also observed that firms with vague or undetailed policies and procedures sometimes struggle to ensure a consistent approach.

► Wider Considerations - SYSC 6.1.1R - Countering the risk of market abuse-related Financial Crime

- In December 2018, the FCA published Chapter 8 of the Financial Crime Guide which set out guidance for firms in relation to market abuse. Key to complying with these obligations is ensuring that firms have a clear understanding of the market abuse risks that are relevant to the business and the controls required to mitigate these risks.
- Through their supervisory work, the FCA have still identified firms that have yet to produce a robust framework and, as a result, these firms struggle to demonstrate a consistent and effective approach.

► What should Internal Audit teams be thinking about?

As we have seen in the past, the FCA expects all firms to take note of decision notices and relevant publications, and expects senior management to consider the impact that the findings may have on their business.

With this in mind, it is important for Internal Audit teams to provide appropriate assurance to senior management on the second line (compliance) oversight regarding market abuse risks, including coverage of the following considerations for its financial crime framework:

- Review of the firm's current approach to MAR and ensure that it considers all the requirements within primary and secondary legislation;
- Review of the firm's MAR gap analysis to ensure that it covers the requirements of all primary and secondary legislation, and ensures that all products and services that are offered to clients are appropriately considered. This should include any products and services that have been introduced by the business after the original implementation of MAR;
- Ensure that the firm's MAR Risk Assessment is reviewed on a regular basis and takes into account all key risks facing the business, and considers both the inherent and residual risks of each of these risks;
- Ensure that senior management are receiving regular and accurate Management Information on the MAR systems and controls and ensure that MAR remains as a standing agenda topic for all relevant financial crime committees;
- Review of the firm's policies and procedures to ensure that they are up-to-date and provide employees with a sufficient level of detail on the approach to be taken when monitoring transactions for possible market abuse and the established escalation process.

A ROUNDUP FROM THE REGULATORS

REGULATOR	DATE	DOCUMENT	WHAT'S NEW?
BCBS	30/09/2022	Report	Basel III Monitoring Report - helpful update which includes recent sample data on banks' cryptoasset exposures
EBA	29/09/2022	Work Programme	EBA's Work Programme for its 2023 - 2025 strategic priorities. Operational Resilience and Consumer Protection feature high on the list.
PSR	29/09/2022	CP22/4	PSR proposals regarding mandatory reimbursement and cost allocation for authorised push payment (APP) scams
FCA	29/09/2022	Speech	What firms and customers can expect from the consumer duty and other regulatory reforms
PRA	26/09/2022	PS8/22	PRA policy statement on the definition of capital. Rule changes to come into effect from 1 January 2023
BoE	26/09/2022	Notice	BoE is returning to its 2022 annual cyclical scenario stress-test framework following disruption from COVID and Ukraine-Russia conflict
PRA	23/09/2022	CP9/22	The PRA proposes to amend it's Rulebook by amending parts relating to Depositor Protection, removing the Dormant Account Scheme and making minor amendments to supervisory and policy statements in relation to depositor protection requirements

A ROUNDUP FROM THE REGULATORS

REGULATOR	DATE	DOCUMENT	WHAT'S NEW?
HMT	23/09/2022	Growth Plan 2022	The recent "mini-budget" published by the Chancellor of the Exchequer
FCA/PRA/FRC	23/09/2022	Guidance	Taskforce on Disclosures about Expected Credit Losses (DECL) published updated guidance on a complete set of high quality IFRS 9 Expected Credit Loss accounting (ECL) disclosures
FCA	22/09/2022	CP22/18	Guidance on the trading venue perimeter - consulting on new guidance on the regulatory perimeter for trading venues to clarify what the FCA means by a "multilateral system" and how this applies to different types of arrangements in financial markets
PRA	12/09/2022	DP4/22	The Discussion Paper describes how the PRA intends to approach policy-making as it takes on wider rulemaking responsibilities under the Financial Services and Markets Bill
FCA	08/09/2022	Dear CEO letter	FCA letter to CEOs regarding it's supervision strategy for benchmark administrators
FCA	05/09/2022	Dear CEO letter	Dear CEO letter to FCA 'portfolio firms' regarding trade repositories
FCA	02/09/2022	CP22/17	Quarterly Consultation Paper No. 37 - a variety of changes to the Handbook, including recent changes to the regulatory perimeter in respect of credit agreements entered into with high net worth borrowers

FOR MORE INFORMATION:

RICHARD WEIGHELL

+44 (0) 7773 392799
richard.weighell@bdo.co.uk

www.bdo.co.uk