

# *CASS Audits 2022*

Brought to you by the Financial Services Faculty

# Presenters



- **Philippa Kelly**  
• Director, Financial Services  
• **ICAEW**



**Shermeen Kazmi**  
Partner, Financial Services  
Audit  
**Grant Thornton**



**Edward Westrip**  
Insurance Audit &  
Regulatory Practices  
**Mazars**



**Dennis Cheng**  
FSI Regulation Client  
Assets  
**Deloitte**



**Jim Feasby**  
Interim Head of Resolution  
Strategy, Operations & CASS  
**FCA**

# **Client Assets Reports – FCA View**

## **ICAEW CASS Webinar 18 January 2022**

**Jim Feasby**

Interim Head of Resolution Strategy,  
Operations & Client Assets Department

# Agenda

## CASS Supervision

- COVID-19
- Our approach

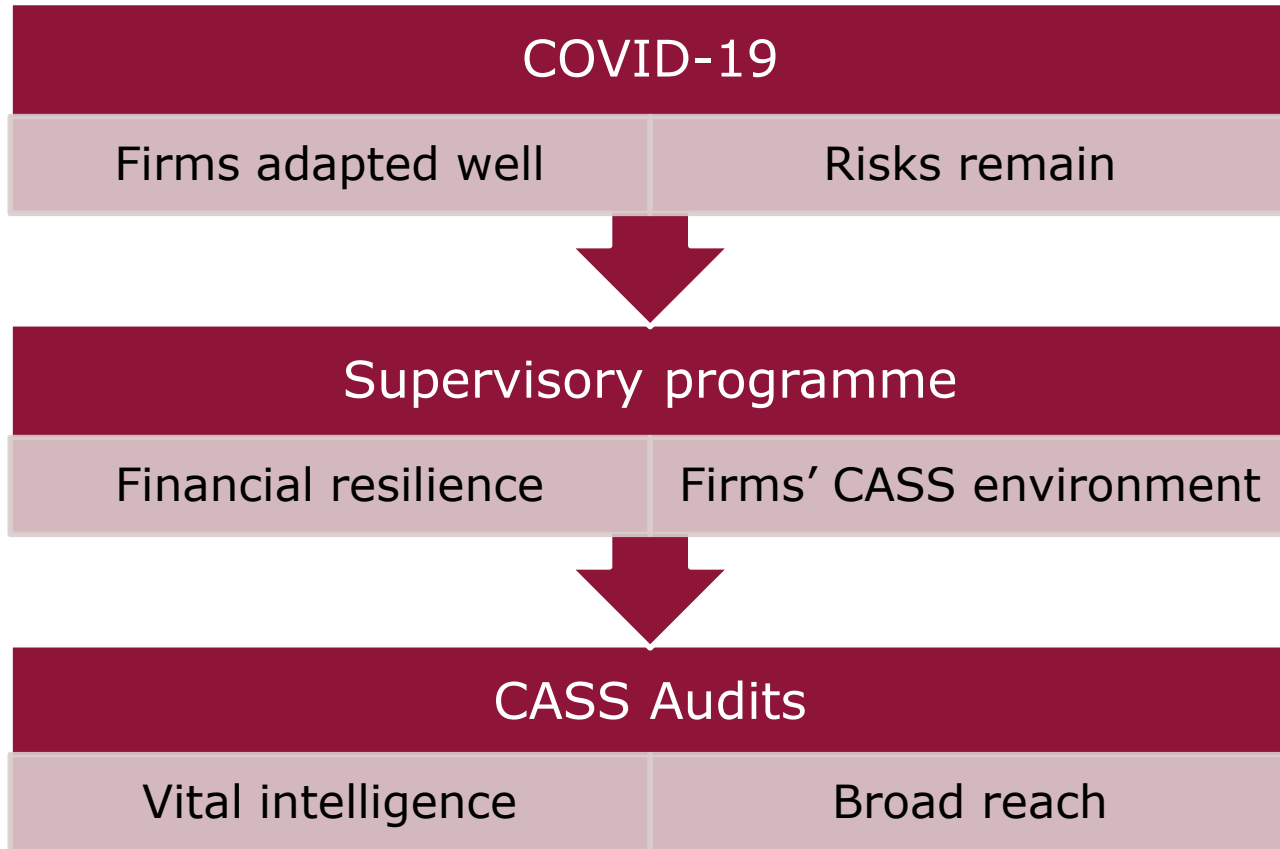
## Client Asset Reports

- How we use CASS audits
- Volumes and trends

## Audit Quality

- Breach narrative
- Undetected issues
- Work programs

# CASS Supervision



# Client Assets Reports

## Volumes

- c3,200 received each year (reasonable & limited assurance)

## How we use CASS Audits

- All reports are reviewed
- FCA follows up on intelligence received

## Trends

- Increase in "qualified" opinions
- Reduction in "adverse" opinions

# Audit Quality

Breach reporting

Undetected issues

Work programs

# Key messages

- CASS Audits are a vital resource for the FCA
- Detail is vital in breach reporting
- We will escalate poor quality reporting
- Be mindful of organisational arrangements  
breaches





---

FCA Head Office  
12 Endeavour Square  
London  
E20 1JN

[www.fca.org.uk](http://www.fca.org.uk)

**Deloitte.**



## ICAEW Client Assets

Getting the scoping of CASS audits right

18 January 2022

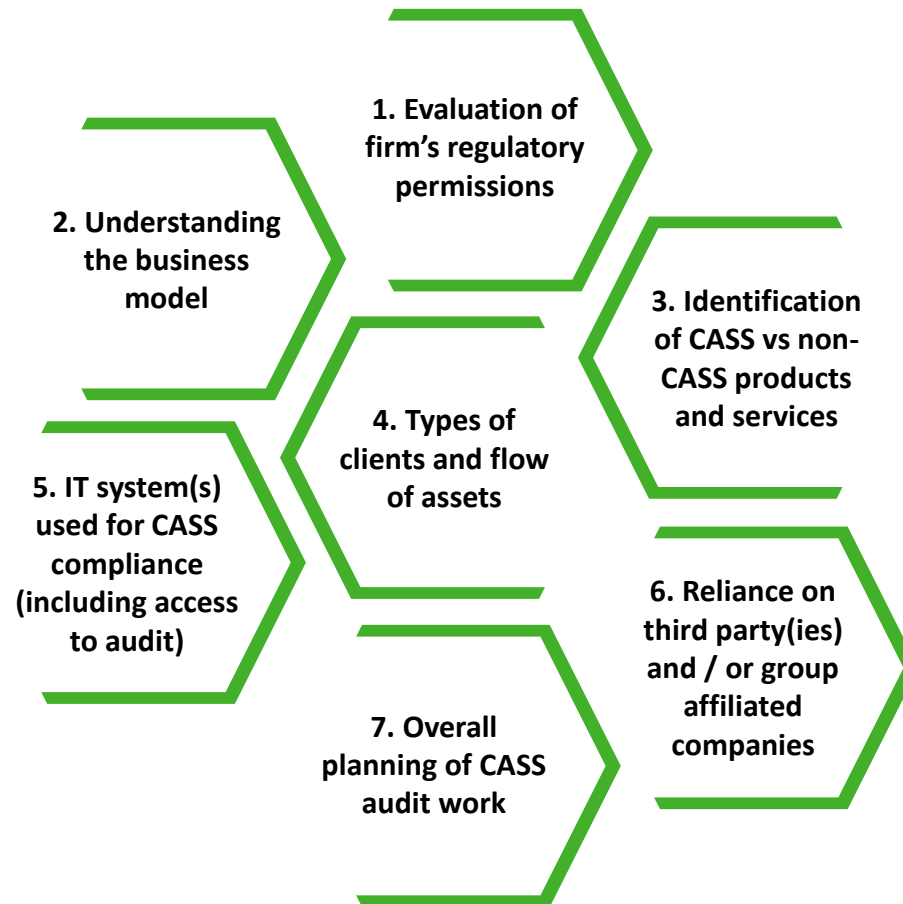
# CASS audit overview

## High level basis of the CASS audit

- a) **CASS rules in-scope (reasonable assurance opinion) –**
  - 1. **Investment firms:** CASS 3 (collateral), CASS 6 (custody assets), CASS 7 (client money) and CASS 8 (mandates)
  - 2. **Insurance Broking:** CASS 5 (insurance distribution) and CASS 8 (mandates)
  - 3. **Debt and Claims Management firms:** CASS 11 and CASS 13
- b) **Audit evaluation** – controls evaluation *during* the period, and compliance *as at the period end date*
- c) **Risk assessment** – evaluation of firm’s CASS rules, risks and controls documentation
- d) **Entity level controls** – evaluation of governance, training, etc. as well as CASS culture
- e) **Insolvency mind-set** – evaluate firm with an “insolvency mind-set”
- f) **Materiality** – none applied in the context of CASS breach reporting in the auditor’s opinion
- g) **Nature, timing and extent of audit work** – supported by appropriate and relevant audit evidence

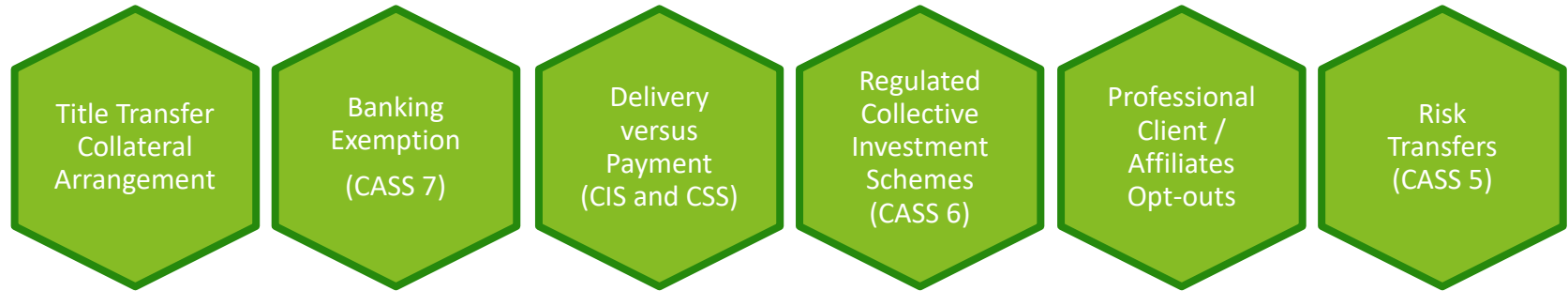
# CASS footprint and business model

Identifying in-scope products and services, systems and service providers

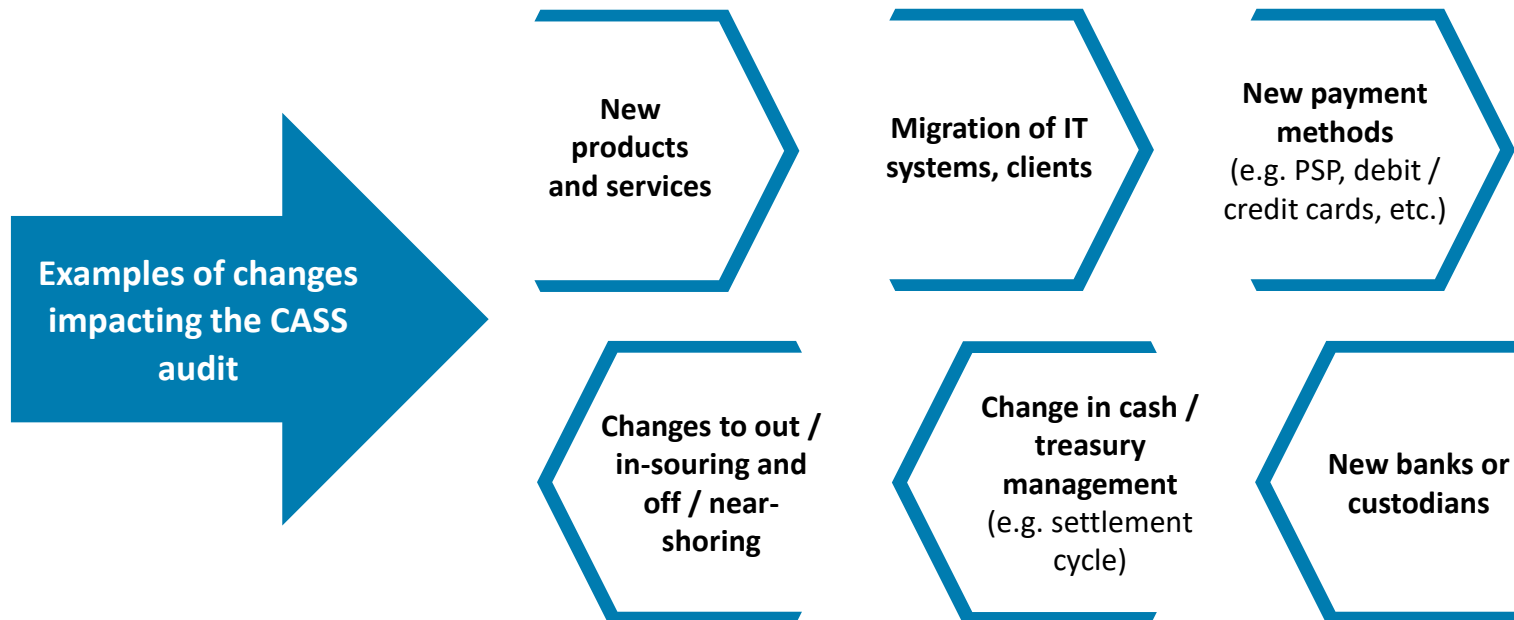


# CASS footprint and business model

CASS “exemptions” and changes at the firm which impacts the CASS audit



CASS conditions for using the “exemptions” must be met!



# Limited assurance engagements

## **Matters to consider in a limited assurance engagement:**

- a) Why does client money / custody assets not arise from the business?
- b) Who is responsible for clients' monies and assets?
- c) Why are regulatory permissions not used (if this is the reason for client assets not arising)
- d) How is the firm remunerated for its services provided to clients?
- e) "Model A" vs. "Model B" vs. "White Label" vs. "Give-up" arrangements – what do they all mean and are they consistent between client T&Cs, legal agreements and operational arrangements?



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

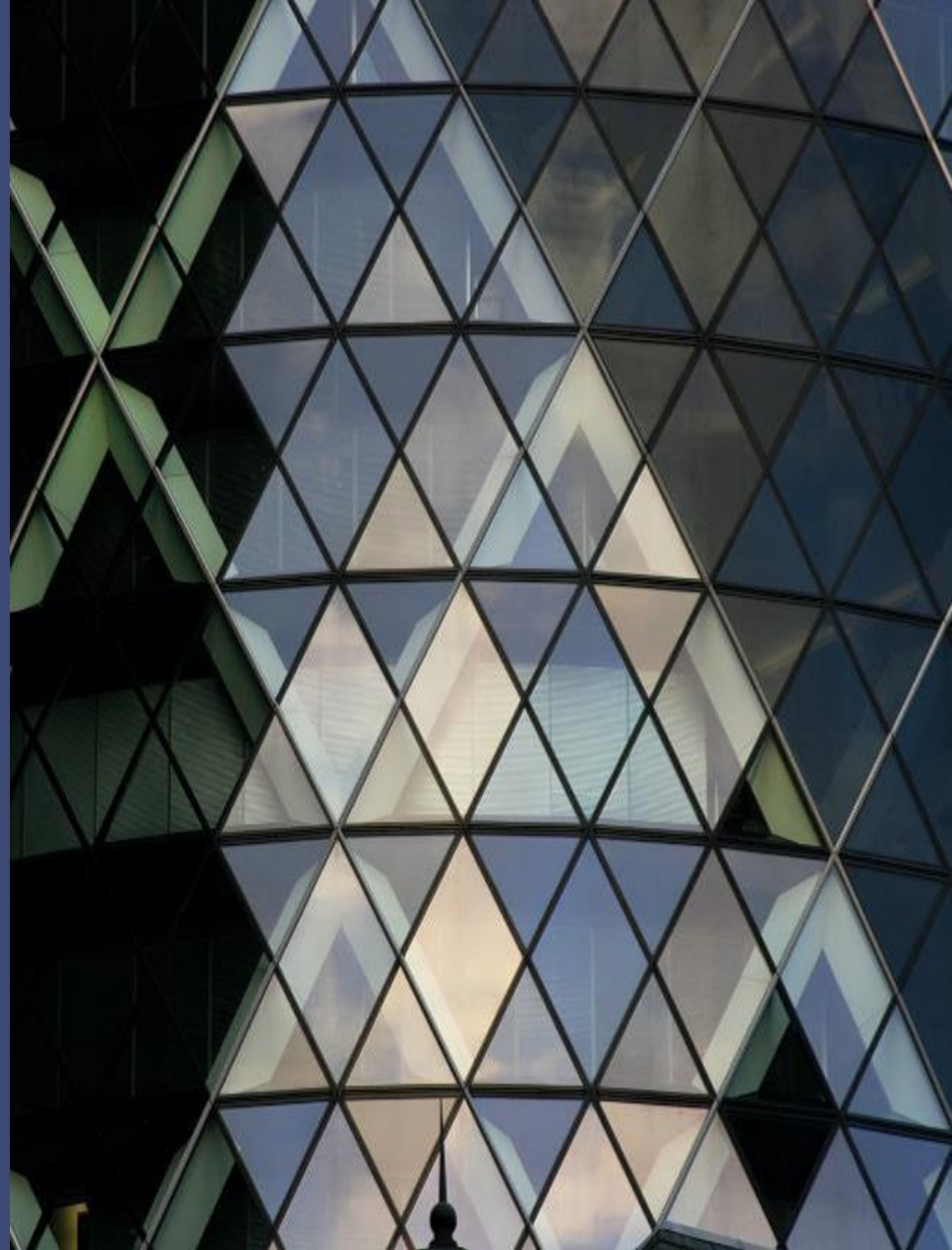
Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

# CASS Testing Approach

Edward Westrip

18 January 2022



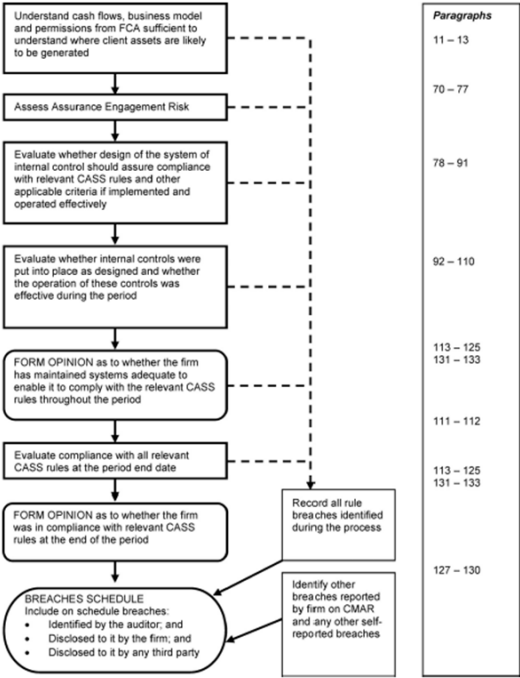


# CASS Testing Approach

## Overview

APPENDIX 1

OVERVIEW OF A REASONABLE ASSURANCE PROCESS FOR A LEGAL ENTITY



Understand cash flows, business model & permission (11-13)

Risk assessment (70 - 77)

Design evaluation (78 - 91)  
 Test implemented as designed & operating effectively during period ('controls testing') (92 - 110)

Form opinion on adequacy of system to enable compliance during the period (113 - 125, 131 - 133)

Test compliance at period end ('substantive testing') (111 - 112)

Form opinion on compliance at period end (113 - 125, 131 - 133)

Breach reporting (127 - 130)

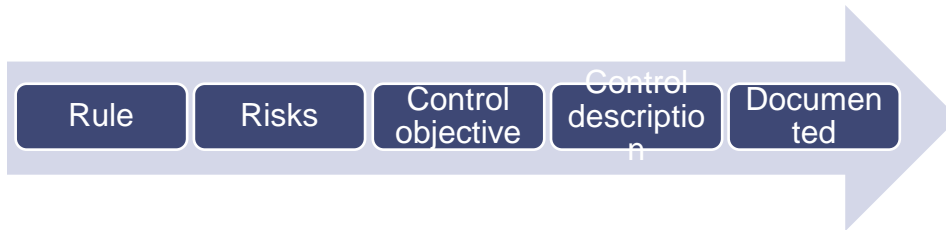
PLUS

Communication deficiencies to management & TCWG (134 – 136)

EQCR (137 – 141)

# CASS Testing Approach

## Design evaluation - creating the links - rules mapping & risk assessment



**Rules** – all CASS rules including explaining why not applicable

**Risks** – specific to the rule, consider the end to end process of client money and asset flows

**Control objective** – clear and link to the risk

**Control description** – description, manual/ automated, outsourced, frequency, dependent systems

**Documentation** – associated policy, procedure, process

### TOP TIPS

- Don't marginalise the design evaluation – it takes time. Design evaluation must cover the 4 fundamentals (identification, segregation/safeguarding, reconciliation, trust/legal title) and every rule plus segregation of duties and change management (people, process, technology)
- Link back to the work on CASS footprint and business model:
  - Variation across business
  - Exemptions and opt-outs used
- Client must do this and see a variety of formats
- Use stat audit documentation templates or extend/reuse clients documentation (NB care as we are reporting directly against the CASS rules)
- As much interested in what they ought to be doing but are not doing as much as what they are
- Document a conclusion and significant deficiency in design or a gap is a breach

# CASS Testing Approach

## Conducting walkthrough

- Checking a control is implemented as designed requires a walkthrough
- A control is a checkpoint in a process designed to prevent or detect error
- Need to select an example (e.g. a transaction or a reconciliation) and literally walkthrough a process end to end step by step with the client explaining what they do with what and when
- Need to cover upstream from each control e.g. from receipt of application and input for a transaction, or from data extraction and manipulation for a reconciliation
- Covering the transactions and identifying the controls over complete and accurate data is key to record keeping and without this compliance cannot be asserted

### TOP TIPS

- Don't marginalise the walk through – it takes time
- Bring it to life with screenshots
- Use stat audit documentation templates or extend/reuse clients documentation (NB care as we are reporting directly against the CASS rules)
- As much interested in what they ought to be doing but are not doing as much as what they are
- Document a conclusion and a significant deficiency in implementation is a breach

### Walkthrough of each control identified to mitigate risk

							Conclusion			
<b>Key control ref</b> <i>(should be the same as key control references within any separate Business Process documentation)</i>	<b>Process description</b> <i>(or summary of detailed process with cross reference to fuller process)</i>	<b>Description of risk</b> <i>(likely sources of potential misstatement or „what could go wrong“ linked to audit assertions)</i>	<b>Key control description</b> (including design factors – how these would mitigate the risk & the evidence of operation of the control, considering as applicable aspects such as: control owner; frequency of control; standardised process/ template (less risk of deviating); and criteria for thresholds/ investigation)	If the key control pertains to a significant risk, is it consistent with the key control documented against the significant risk raised? Y, N or N/A	<b>Automated, semi-automated or manual control (A, S-A or M)?</b> If automated or semi-automated, refer to the MAM Application Guidance on IT audit and comment on aspects relevant to the operation of the key control (refer guidance text)	<b>Walkthrough description</b> <i>(this should be re-performable and include specific key control identified but may include the full process for the purpose of confirming audit understanding of the critical business process as a whole)</i>	<b>Key control deficiencies</b> <i>(describe any control deficiencies noted)</i>	Is key control design appropriate to mitigate the associated risk?	Is key control implemented as designed?	If significant key control deficiencies (after considering any mitigating controls) are identified pertaining to a significant risk, confirm raised as a significant deficiency with TCWG and document audit consideration of implications (cross refer to where addressed as applicable)

# CASS Testing Approach

## Testing operational effectiveness

- Opinion in the year is not a substantive audit
- Requires control evidence
  - Identity of preparer and reviewer, both dated
  - May include process checklists
  - May include the governance & oversight committee
- Requires supporting evidence for each control activity
  - Not just 'front sheet' with signatures and dates
  - What the preparer/reviewer had in front of them
- When is a control not a control?
  - No evidence of review of due diligence on bank
  - No evidence of review and conclusion on ISEM
  - No evidence of follow up on discrepancies identified in reconciliations
- When is a control not achieving its purpose?
  - Lack of implementation of pay as pay clauses in client money calculation
  - Lack of go-live control for new bank account

### TOP TIPS

- Systems In the CASS report does mean control testing (SYSC = Senior Management Arrangements, Systems and Controls does not mean controls are something separate)
- Control sample sizes follows that for general statutory audit and extent is based on the risk assessment conducted
- Make sure you walkthrough the testing prior to completing all the items
- Control failure is a breach. May indicate a significant deficiency which may be the breach
- ITGC and application controls are included. Cannot mitigate a control failure (e.g. proving inappropriate privileged access was not misused is still a control fail)
- Reliance upon SOC reports permitted, but must be rigorously evaluated before any reliance is placed (included in paragraphs 100 to 110)

# CASS Testing Approach

## Substantive testing

- Period end statement on compliance requires substantive testing
- Two paragraphs in the standard which include 'The nature and extent of the CASS auditor's testing procedures will be a function of the conclusions it has formed on the effectiveness of internal control and the specific nature of the applicable CASS rules'

### *Examples*

- Contractual terms with third parties
- Testing period end internal and external reconciliations and evaluation of legitimacy of explanation of reconciling items
- External confirmations
- Bank acknowledgement letters

### TOP TIPS

- 4 fundamentals of protection must be in place, for example
  - Insurer terms of business agreements determine whether client monies or insurer monies arise and to whom it segregated for
  - Bank confirmations underpin completeness of segregation
- Don't leave late as nowadays when confirmations are requested they must be received to sign-off
- Never conflate substantive testing with controls testing

# CASS Testing Approach

## Robustness of evidence – information prepared by entity

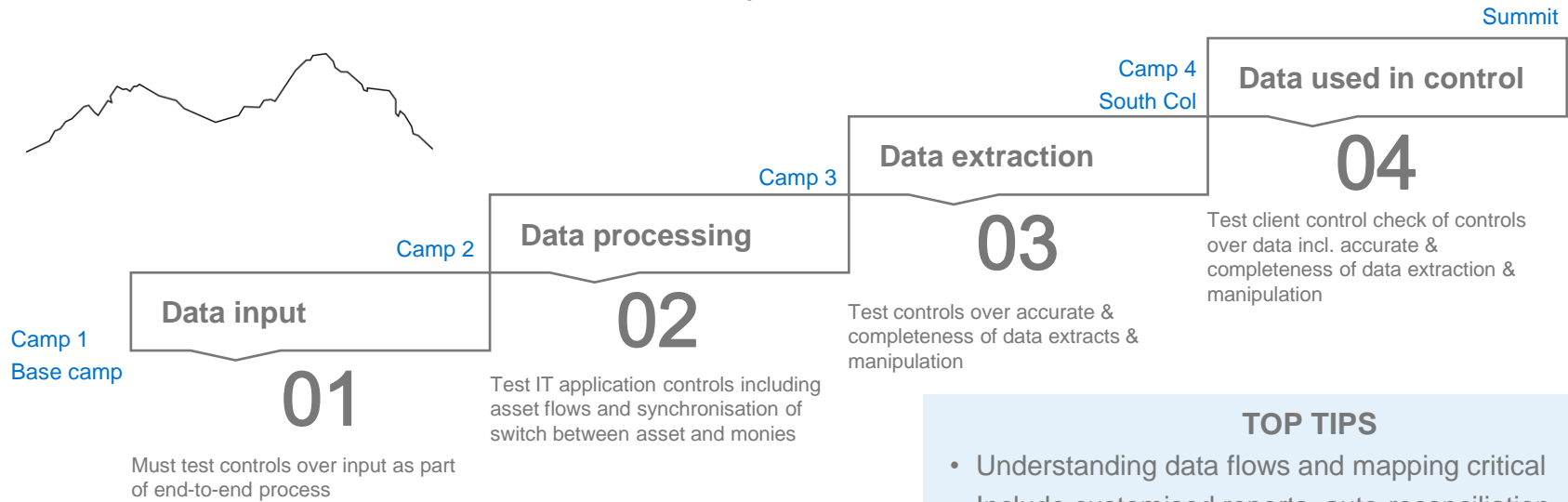
- This is relevant to control sampling during the period and substantive testing
- Can be system generated (e.g. list of transactions generated by system) or manually (e.g. log of insurer terms of business) or combination
- IPE used in an audit procedure must be proven to be complete and accurate or irrespective of how good our audit procedure is our results could be wrong
- Risks relate to the underlying data from its complete and accurate input to its correct processing and absence from modification by an end-user
  - These are covered by audit procedures such as tests of detail, sampling for attributes. tests of control or combination
- Risks relates to report generation whether parameters are inappropriate for a system query or a report logic is incorrect or the end-user manipulates it
  - Each audit firm will have its own procedures, but these are likely to cover whether the report is standard or the extent to which it is customised by the entity, whether it can be reconciled to a TB and whether it is used in performing a control
  - For CASS need to consider whether the report is a database extract breakdown or population used to select a sample or used as audit evidence when used by the entity in performing a control

### TOP TIPS

- Engage a specialist and plan early
- CASS governance and oversight should have understood how they systems work and how data feeds into the reconciliations
- For all reports we should check parameterisation of report or conduct a code review and also check mathematical accuracy
- For standardised reports used for sampling or in a control likely sufficient to walkthrough the logic and reconcile to TB or otherwise document how ensured data retrieved is complete
- For customised reports will need to go beyond reconciling to TB for example to recreation (data analytics), test of control or detail, data flow diagram and source code review
- Where customised reports are used in controls its continued use is underpinned by testing ITGC change management and others (if any)

# CASS Testing Approach

## Robustness of evidence – information used by client in a control



Must test ITGC including change management as part of a CASS audit

- TOP TIPS**
- Understanding data flows and mapping critical
  - Include customised reports, auto-reconciliation, robotics and end user computing (macros, access databases etc) in testing scope. Change management may sit outside IT.
  - Parameterisation of standard reports
  - Consistency of data
  - SOC reports at service organisations for ITGC

# CASS Testing Approach

## Concluding remarks

- Design evaluation and walkthrough determine what is tested
- Testing primarily controls and must not equate having done something as a control
- Audit firms must apply the same discerning approach to CASS over evidence of accuracy and completeness of sample populations and requiring control evidence and supporting evidence used in controls including its accuracy and completeness
- Testing of IT general controls and applicable application controls must be performed for CASS and change management covers not just reports but auto-reconciliations, end user computing and robotics
- Where the standard is silent then best practice from statutory audit especially those of PIE provides guidance



## Contact

### Mazars

#### Edward Westrip

Director, Head of CASS

Edward.Westrip@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services\*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

\*where permitted under applicable country laws.

[www.mazars.co.uk](http://www.mazars.co.uk)

## Follow us:

### LinkedIn

[linkedin.com/company/mazars-in-the-uk](https://linkedin.com/company/mazars-in-the-uk)

### Twitter

[twitter.com/mazars\\_uk](https://twitter.com/mazars_uk)

### Facebook

[facebook.com/MazarsinUK](https://facebook.com/MazarsinUK)

### Instagram

[instagram.com/mazarsinuk](https://instagram.com/mazarsinuk)



# ICAEW CASS Webinar

18 January 2022

# Breach reporting

# Reporting breaches

- **Breaches Schedule** attached to every reasonable assurance report
- FCA expects **every breach** of a rule to be reported
  - only those rules within the scope of the report
  - identified by the auditor, the firm, or a third party

## any breach => not a clean opinion

- **forget materiality**
- schedule includes a requirement for the firm to comment on each breach reported

# What makes a good report of breaches

- **only breaches of relevant CASS rules**, ie not other rules
- **clarity** – needs to be understood by the reader, and given context, for example:
  - how frequent?
  - how many transactions affected?
  - when?
  - for how long?
  - what was the amount involved or at risk?
  - how many client bank accounts involved?
  - how many client securities involved?

# Adverse/qualified – which opinion?

- SUP 3.10.9 and CASS Standard provides guidance
- systemic or pervasive as opposed to isolated incidents
- consider aggregate effect of any breaches
- **likely to be adverse opinion?**
  - extent of loss if firm had gone into administration while breach persisted
  - breach of requirement to keep proper records of client assets
  - failed to carry out or incorrectly carried out to a significant extent reconciliations

# Breaches in Limited assurance engagements

# Scope of Limited assurance engagements

## Opinions in limited assurance reports

- firm has relevant permissions but claims it does not hold client money or custody assets
- firm does not have the relevant permissions

## Why do any work?

- to support our report to the FCA (limited assurance report) on whether client money/assets were held
- client could be holding client assets/money outside permissions, which is not afforded protection
- 'negative/limited assurance'



# Modified Limited assurance opinions

## Not uncommon for a modified limited assurance opinion

- Issues leading to client money/custody assets being held:
  - Errors with scoping
  - Receipt of client assets by error
  - Overpayments
  - Incorrect invoicing
  - Operational errors

# Common CASS 5 breaches

# CASS 5 breaches

## SEGREGATION/SAFEGUARDING

### *Policies and procedures/organisational arrangements*

- Client money (CM) manuals not kept up-to-date
- Weak controls around banking of cheques leading to breach of depositing of CM within the required timeframe
- Absence of valid executed agreements with appointed representatives (AR)

### *Operational processes*

- Use of a non-statutory trust (NST) without obtaining and keeping a current confirmation from auditors

### *TOBAs*

- Entering into business without having valid terms of business agreements (TOBAs)

# CASS 5 breaches (cont'd)

## RECONCILIATION

### *Non-compliant method*

- Incorrect performance of the internal CM reconciliation
- Incorrect client money calculations due to exclusion of monies held with third parties

### *Operational errors*

- System issues leading to inability to carry out reconciliations within required timeframes
- System changes/upgrades leading to inability to prepare CM reconciliations

# CASS 5 breaches (cont'd)

## RECONCILIATION

### *Operational errors (cont'd)*

- Issues relating to system changes leading to lack of support retained for the reconciliations
- CM excess not withdrawn within prescribed time frames
- External reconciliations not performed within the prescribed time frames
- Failure to maintain accurate backup and supporting documents for CM recs

## TRUST/LEGAL TITLE

### *Acknowledgement letters*

- Operating a CM account without obtaining a valid acknowledgment letter from the bank

# Common CASS 6 breaches

# CASS 6 breaches

## SEGREGATION/SAFEGUARDING

### *Policies and procedures/organisational arrangements*

- Inadequate policies and procedures including; how is internal custody check being performed, how discrepancies can be identified and resolved, frequency of controls and processes around recs
- Inadequate CASS controls mapping – not documenting key controls and reference to processes as opposed to controls
- No policies for physical asset reconciliations. No policy or procedure for determining frequency of reconciliations

# CASS 6 breaches (cont'd)

## *Operational processes*

- Incorrect recording and registration of legal title as a result of stock transfer/withdrawal processes
- System failures leading to unsettled trades impacting on the reconciliation and CASS breaches due to timing of payments
- Transactions not covered by DvP exemption due to errors leading to incorrect use of DvP exemption
- Inaccuracy of records and accounts due to posting/processing errors, negligence etc.



# CASS 6 breaches (cont'd)

## RECONCILIATION

### *Non-compliant method & Operational errors*

- Non - compliant ISEM – Attestation vs evaluation?
- Carrying out internal custody record check using external records
- Internal custody record check not carried out within the timeframes as per the rules – “as soon as reasonably possible”
- Reconciliation discrepancies not resolved on the same day
- Internal custody recs not performed frequently enough given the business model.
- Breaks / treatment of shortfalls (whose responsibility? Leading to delays)

# Common CASS 7 breaches

# CASS 7 breaches

## SEGREGATION/SAFEGUARDING

### *Policies & procedures/organisational arrangements*

- Inadequate policies and procedures including; how client money reconciliations are being performed, how discrepancies can be identified and resolved, frequency of controls and processes around recs
- Inadequate third party providers oversight
- CASS policy and procedures manuals not updated or reviewed

### *Operational processes*

- Monies transferred to wrong client or client monies paid into incorrect CM accounts
- Duplicate cheques issued in error, cheques not banked promptly
- Client money not allocated within 10 business days following receipt
- Incorrect payments being made out of CM accounts leading to shortfalls
- Payments made/trading on uncleared funds
- Failure to withdraw monies due to firm within required timescale

# CASS 7 breaches

## RECONCILIATION

- CM resource not taken as an aggregate balance and starting position from internal records adjusted
- External records used for Internal CM rec as opposed to internal records
- Use of non-standard Internal CM rec without obtaining prior approval of FCA to adopt non-standard method
- Incorrect calculation of internal CM rec, in respect of treatment of negative balances
- Weak controls for ensuring accuracy of CM recs - lack of review and review not carried out in a timely manner
- Reconciliation discrepancies not dealt with on a timely basis.
- Surplus not withdrawn on the same day as the reconciliation
- Incorrect CM rec due to a manual processing error
- Incorrect layout and headings on internal CM rec

# CASS 7 breaches

## TRUST/LEGAL TITLE

### *Selection of and DD on banks/counterparties*

- Due diligence carried out on institutions does not meet the requirements of CASS rules.
- No review carried out/or formally documented on banks at appointment and on an ongoing basis.

### *Acknowledgement letters*

- Incorrect format used for CM acknowledgement letter
- No acknowledgement letter obtained for client transaction accounts

# Conclusions

# Conclusions

**CASS remains a regulatory priority area**

**Importance of understanding the business model**

**Controls based assurance engagement**

**CASS rules are complex – expect breaches**

**Independent engagements with an insolvency mind-set**







*Any questions?*