ICAEW KNOW-HOW
FINANCIAL SERVICES FACULTY

CASS Audits 2023

17 January 2023

This webinar will begin shortly...

© ICAEW 2023

Agenda and presenters

A:
FCA focus areas

Jim Feasby
FCA

B:
How to scope a CASS audit

Mduduzi Mswabuki
EY

C:
IT and third parties

Nicola Geraghty
PWC

D:
Breaches and reporting

Edward Westrip
Mazars

© ICAEW 2023

Client Assets Reports
FCA View

ICAEW CASS Webinar
17 January 2023

Jim Feasby
Head of Client Assets, FCA

Agenda

FCA Strategy	• Topline outcomes • Reducing and preventing serious harm • Role of client assets regime
Our approach	• How we use CASS audits • Volumes and trends • Discrepancies
Audit Quality	• Breach schedule narrative • Undetected issues • Our approach

CASS Scoping

Mduduzi Mswabuki
EY
Partner

Building a better working world

CASS Scoping

CASS Scoping is the first thing we need to consider at the beginning of an engagement:

One of the most challenging aspects of the CASS scoping stage is determining whether a regulated firm is within the scope of CASS audit and then if it is, what type of report is required to be issued.

For all firms that are regulated by the FCA, the audit teams are required to document their considerations and conclusions in respect of whether a firm is within the scope of CASS audit.

Since the considerations and the level of work involved to determine whether a firm is within the scope of CASS audit will be different depending on the relevant facts and circumstances for each firm, audit teams will need to exercise their professional judgement in determining the amount of work required to validate their considerations and conclusions. Audit teams should not be relying solely on management representation to determine the scope of CASS audit, although this should be one of the procedures performed.

EY

Decision Tree

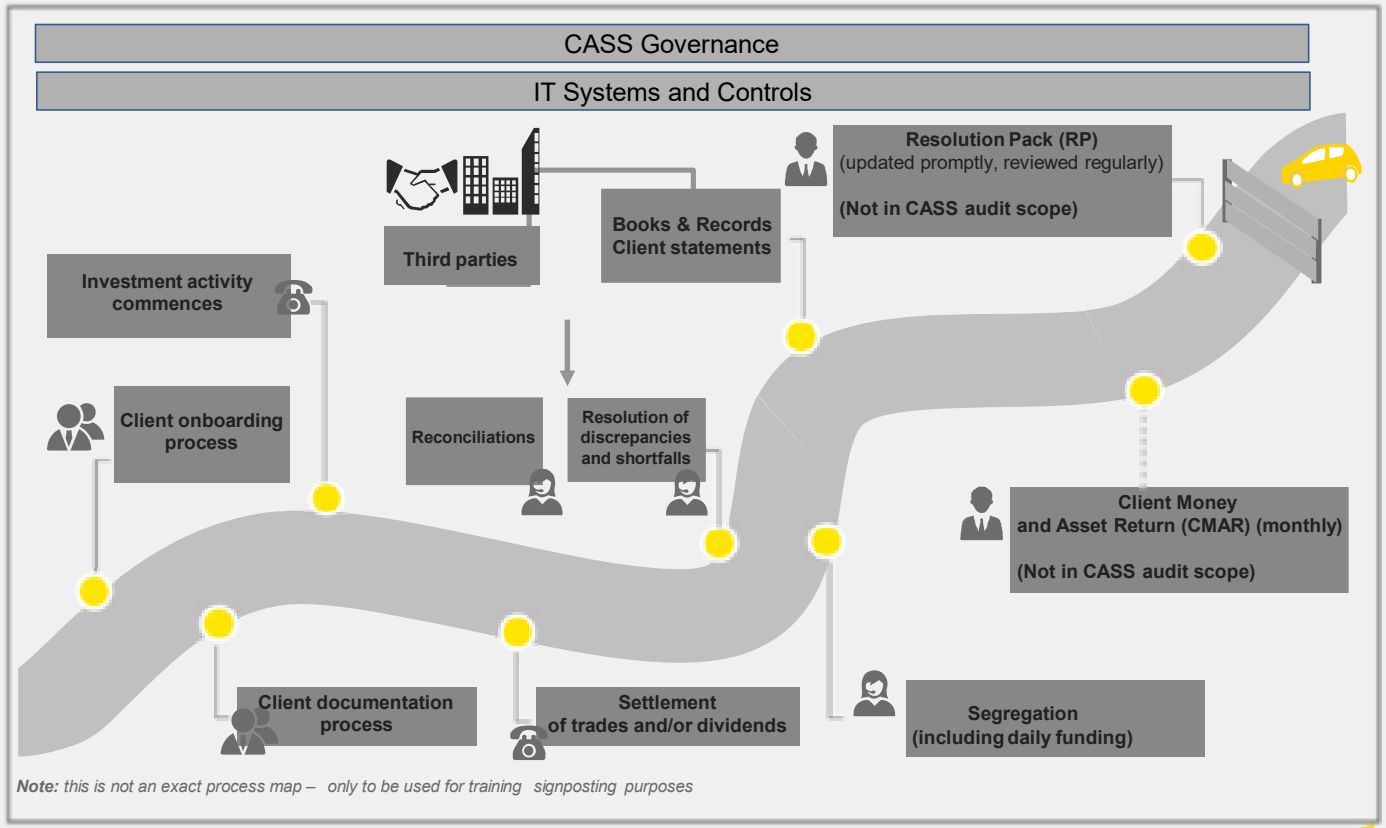
Limited Assurance

Type	Procedures
Firm that does not conduct investment business	• Review management's assessment of Applicability • Auditor to exercise professional scepticism
Firm that conducts investment business but is not permitted to hold	• Determine whether the firm is relying on exemptions e.g. ❑ TTCA ❑ DVP ❑ Banking Exemptions • Determine if the firm is relying on it's Business Model. • Review the firm's Applicability assessment. Perform detailed walkthrough and follow-through/confirm. • Auditor to exercise professional scepticism
Firm that conducts investment business, has permission to hold, but claims not hold	

Reasonable Assurance

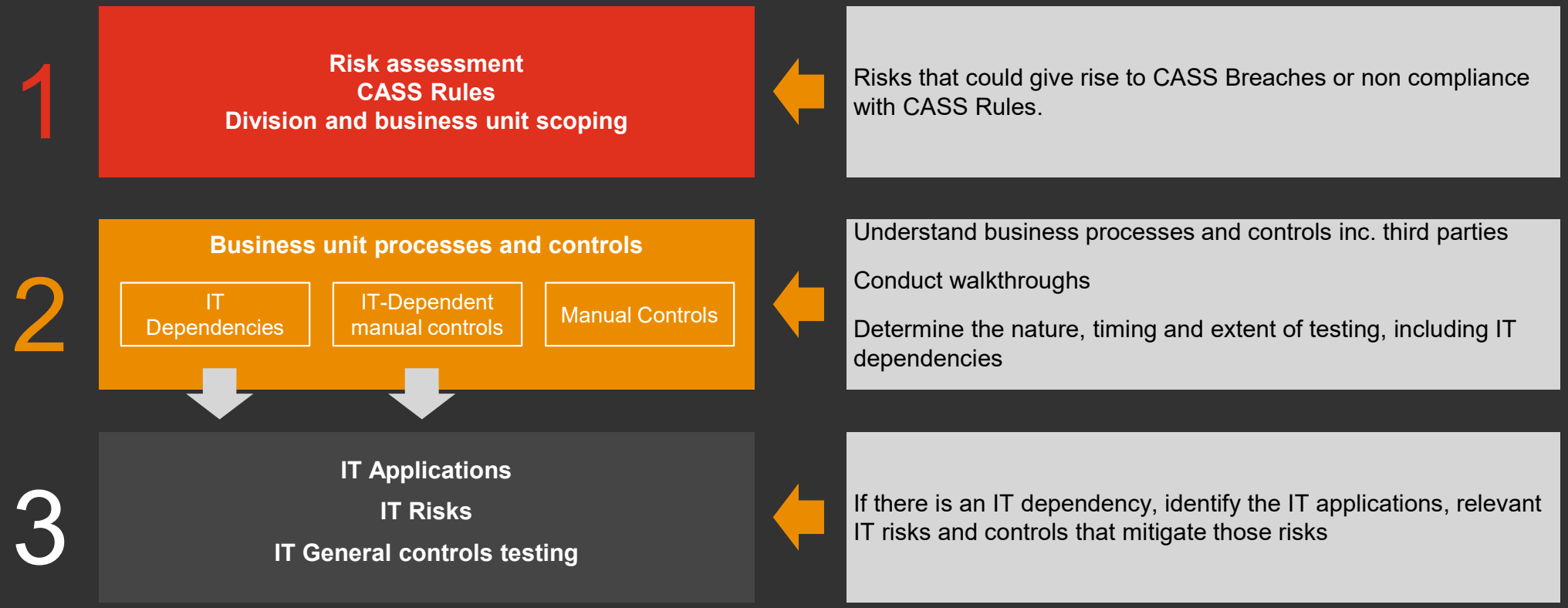
	Procedures
1	Determine which CASS Rules Apply: • CASS 6 • CASS 7 • CASS 8 • CASS 3 This can be done through: • Reviewing client's own CASS applicability assessment • Obtaining an understanding of each product, service or business line via walkthroughs, enquiries of management and determine which CASS Rules • Reviewing CMAR to validate your understanding
2	Obtain an understanding of CASS Governance and controls
3	Obtain an understanding of the firm's systems and IT controls that supports the firm's adherence to CASS requirements
4	Determine whether the firm uses TPAs (Third Party Administrator)

End-to-end CASS journey

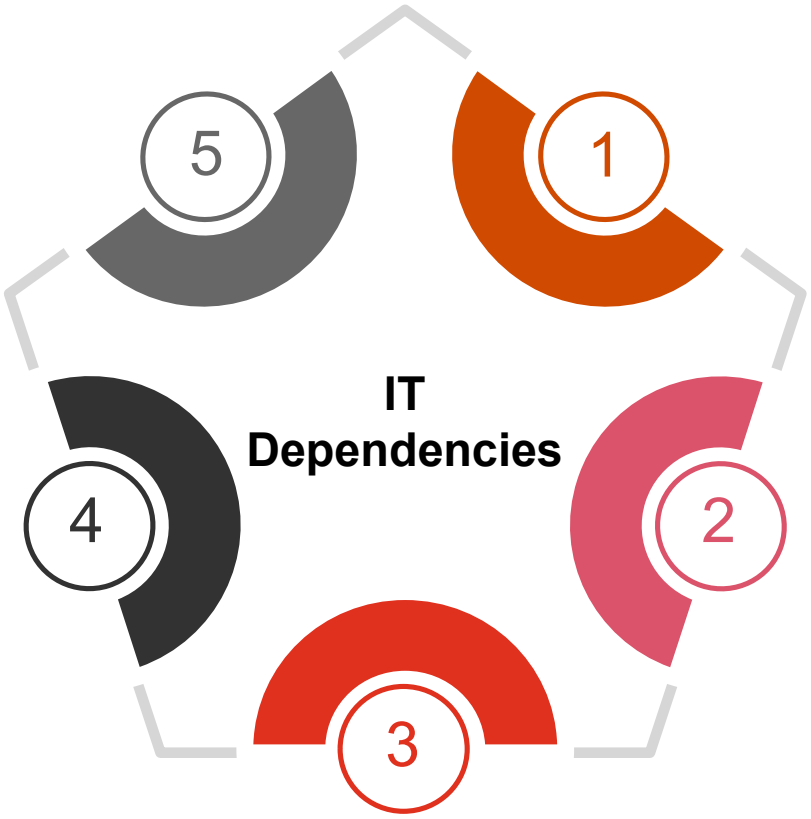


Note: *this is not an exact process map – only to be used for training signposting purposes*

Approach to scoping and testing IT controls



Five Types of IT Dependencies



1 Automated Controls

Procedures that occur without user interaction

2 System Generated Reports

Information is routinely generated by IT systems and is often used in the execution of a manual control

3 Calculations

Calculations that are performed by an IT system

4 Security, including Segregation of Duties

IT system is used to restrict access to information or functionality

5 Interfaces/Data feed

Transfer of data between IT systems

Information Technology General Control - ITGCs

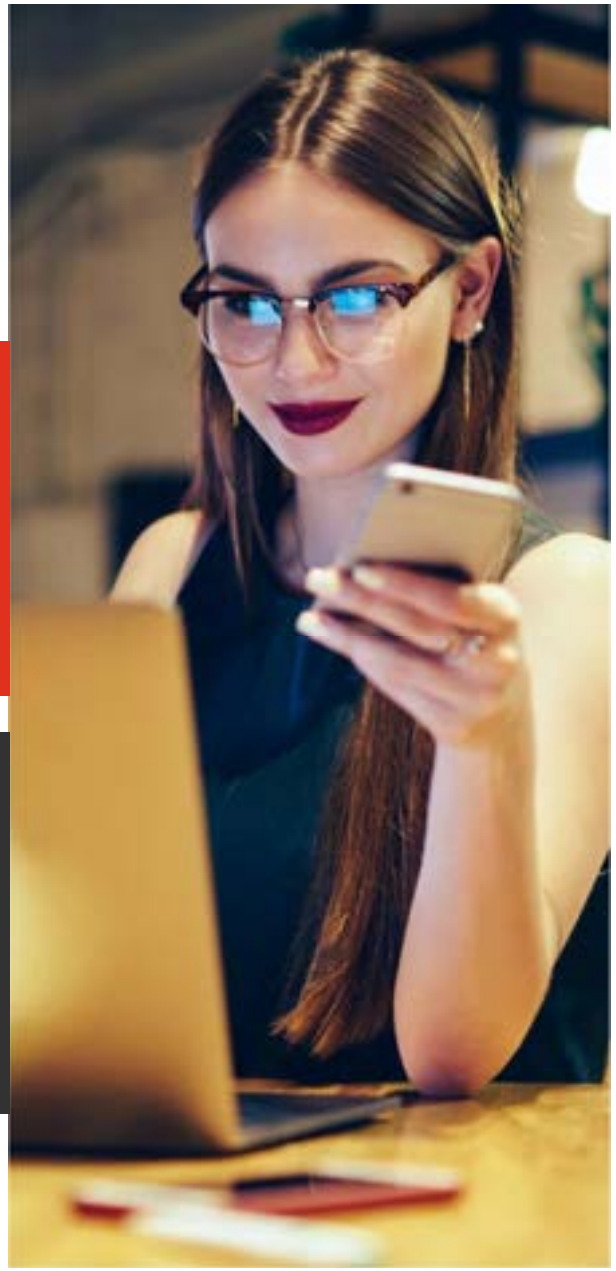
What are ITGCs?

ITGCs are controls used to manage and control the IT activities and system environment.

- **IT Control Environment**
- **Access to applications and data**
- **Program change**
- **Program development**
- **Computer operations**

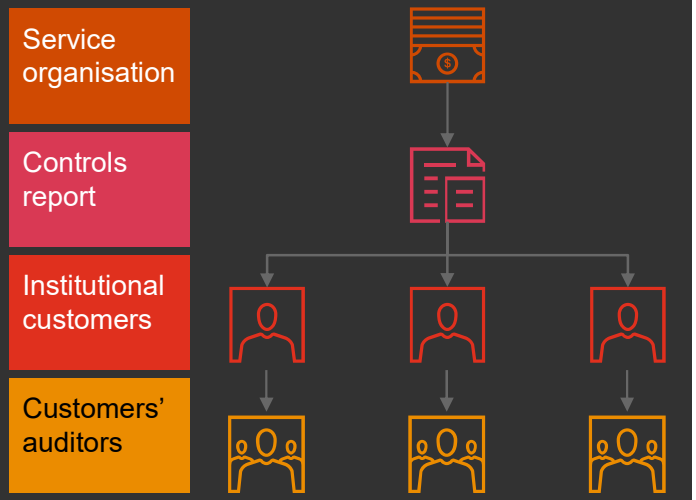
Why do we test ITGCs?

- Our planned audit strategy relies on IT Dependencies; or
- We have identified a general IT environment risk for a system that could give rise to non-compliance with the CASS rules.



Outsourcing and reliance on controls reports

ISAE 3420, AAF 01/20, SOC 1, AT-C 320



Do all of the service providers offer a controls report?

Does the firm have sufficient contracts in place with third parties?

Are ITGCs covered in the controls report I receive?

Are all of the key CASS controls and applications in scope?

Are all of the ITGCs included relevant to CASS compliance?

What about controls over complex spreadsheets & static data?

Are all of the key reports relied on tested in the controls report?

Can auditors use the controls report? Will additional testing be needed as well?

Do you understand exceptions in the controls report and how they impact the audit?

What oversight controls does the audited firm have in place? Are they sufficient?

How will the auditor gain sufficient understanding over the processes and controls?

Breaches

How we think about breaches & how we write them up

Edward Westrip

17 January 2023

mazars

Breaches

Feedback from the FCA

- Policy Statement 11/05 ‘Auditor’s client assets report’
- Greater consistency and transparency in reporting
- Introduced breaches schedule
- Reviewed reports in 2020 and 2021
- Significant proportion had inadequately drafted breaches
    - Severity
    - Repetition
    - Duration

Breaches

SUP 3 Annex 1R

Auditor's client assets report Part 2 – Breaches Schedule

Part 2: Identified CASS Breaches that have occurred during the period

[*Firm name*], firm reference number [*number*], for the period started [*dd/mm/yyyy*] and ended [*dd/mm/yyyy*]

In accordance with SUP 3.10.9AR, Columns A to D are to be completed by and are the responsibility of the auditor. In accordance with SUP 3.11.1G, Column E should be completed by the firm. The auditor has no responsibility for the content of Column E.

Column A	Column B	Column C	Column D	Column E
Item No.	Rule Reference(s)	Identifying party	Breach Identified	Firm's Comment
1				
…				

Instructions for Part 2:

In Columns A to D of the above schedule the auditor is to set out all the breaches of CASS by the firm occurring during the period subject to the auditor's report. These must include the breaches the auditor has identified through its work (such as in the sample testing of reconciliations) and breaches identified by the firm or any other party (such as those included in the firm's breaches register). In relation to any breach identified, the auditor must provide in Column D any information that it has as respects the severity and duration of the breach identified and, where relevant, the frequency with which that breach has occurred.

The auditor must provide a 'nil' return for this part of the report where no CASS rule breach has been identified.

In Column E the firm should set out any remedial actions taken (if any) associated with the breaches cited, together with an explanation of the circumstances that gave rise to the breach in question.

- This annex is a rule
- All the breaches of CASS by the firm occurring during the period
- All breaches identified by the auditor
- All breaches identified by the firm or any other party
- The severity and duration of the breach identified
- Where relevant, the frequency with which that breach has occurred

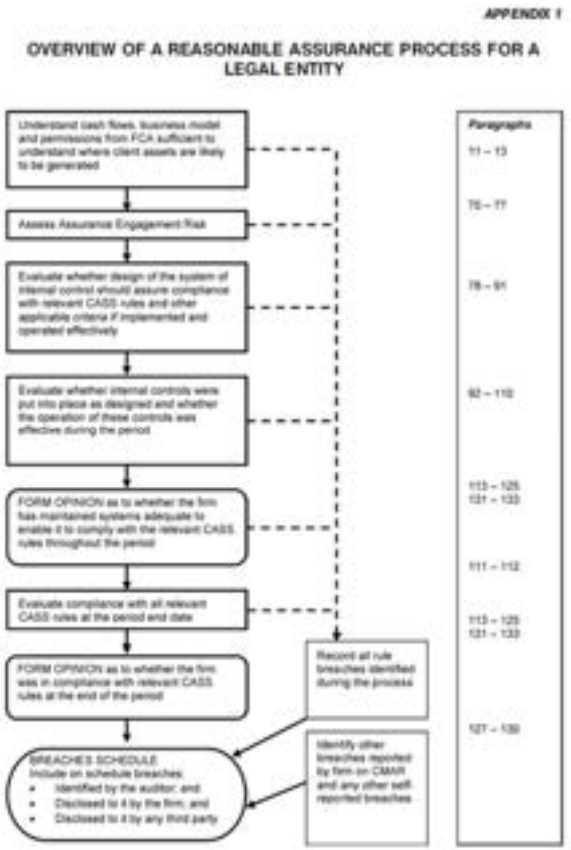
Breaches

Purpose of breaches schedule

- Supports whether opinion is qualified - expected outcome - and whether the qualification is ‘except for’ or ‘adverse’
- Detailed findings of our work (and so take pride in it!)
- Contextual information informs FCA on type of breaches experienced by firms
  - Not considering when to issue an adverse opinion but see also SUP 3.10.9C G (2) which indicates the need for the context
- Useful intelligence for regulatory focus (identified in Consultation Paper 10/20) including:
  - Baseline monitoring across firms
  - Highlight where a firm is an outlier due to type or nature of breaches
  - Identify potential thematic review where significant number of firms breach a rule
- Firms response sets out the remediation being undertaken and any mitigating factors
- The breach and the firms response supports communication with individual firms on their CASS compliance
- Means we must give sufficient time for management to consider
- And … informs risk assessment for the following periods CASS audit

Breaches

Can be identified at any stage in the CASS audit



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)

TOP TIPS

- Failure to mitigate a risk to compliance

- Actual instance of non compliance
- Evaluate processes on the presumption that the firm may become insolvent
- As much interested in what they ought to be doing but are not doing as much as what they are
- All breaches whoever finds with no materiality or de-minimis

Breaches

Capturing and identifying breaches

- Issues for evaluation (some may be rebutted)
- Deficiencies in internal control meriting attention of TCWG ('management letter')
- Some are significant deficiencies in internal control (very unlikely these are not a breach)
- Breaches for schedule (recommendation not required in 'management letter' if adequately addressed by breach and management response)

'Illustrative Hierarchy'

TOP TIPS

- Use an issues log with rule, description and initial evaluation as to significance
- Review with client and document their response
- Remember facts - evidence - change our view not 'special pleadings'
- Capture final judgement as to whether breach or management letter point ('MLP')
- Draft MLP too – if it reads like a breach it probably is (MLP are deficiencies which are not significant and could give rise to future breaches)
- Need to understand how firm identifies and captures issues and evaluates
- For most complex clients also use a questions log

Breaches

Drafting breaches

- Bold heading summarising can be helpful
- Describe breach with clarity and succinctly
  - Severity (including amount), duration, repetition
  - Why rule broken and link with guidance/evidential provisions
  - Consider implications for insolvency such as record keeping, monies at risk, failure in reconciliation to a significant extent
  - Whether open at year end
- Think about why the breach has occurred and whether it indicates a significant deficiency
  - Isolated (e.g. a few manual errors by people)
  - Systemic (e.g. poorly trained staff, significant deficiency in process or technology)
  - Repeated failure can indicate a systemic/pervasive issue
- Must include failures in IT general or IT application controls
- Not strictly speaking in template but can group the breaches with sub-headings of whether prior period or current period and whether open or closed at period end (exceptionally also whether closed by date of report if this aids usefulness)

TOP TIPS

- Put yourself in the position of the regulators staff – can they see clearly what went wrong, why and how serious
- Group similar breaches based upon rules and common theme
- Get the rules right and use organisational arrangements rules only when appropriate
- Make sure include all open from prior period
- Cross reference between schedule and issues log
- Check evidence of closure
- Educate clients to better write their breach logs
- Encourage clients to provide clear responses (immediate steps to rectify, action to prevent recurrence and, if possible, an indicative timescale)

Breaches

Example from Consultation Paper 10/20

- Rules are out of date and things have moved on but gives the general idea

Column A	Column B	Column C	Column D	Column E
Item no.	**Rule reference(s)**	**Identifying party**	**Breach identified**	**Firm's comment**
The auditor would provide here a row number.	The auditor would cite here the CASS rule(s) implicated.	Set out whether the firm, the auditor or other party identified the breach.	The auditor would provide here a description of the breach identified during the period with relevant contextual information.	The firm would provide here a description of the remedial actions taken (if any) and/or mitigating factors associated with the breach the Auditor has cited.
1	CASS 7.4.1	Firm	The firm has identified 12 instances during the period where it failed to promptly deposit client cheques into a client bank account in breach of CASS 7.4.1. The highest amount was for £1,475.67 and the longest period was for 3 business days.	These instances were picked-up through our regular monitoring controls, reported to compliance, and rectified on the same day they were identified. The cause of these breaches was human error. As part of their annual audit plan, our internal auditors undertook reviews of the relevant controls and assessed their adequacy. No further remedial actions were required.
2	CASS 7.8.1R(2)	Auditor	In February 2009 the firm opened a new client bank account with a UK Bank. The firm did send a notification of trust letter, but did not receive an acknowledgement from the bank and continued to place client money in the account in breach of CASS 7.8.1R(2). At period end the account held approximately £1.56 million.	Trust acknowledgement letter has now been received for this account. The account opening check list has now been updated to ensure that a new client bank account cannot be used without first receiving an acknowledgement of trust letter from a bank.

© ICAEW 2023