AML Regulation 21 Audits Webinar

Does Your Firm Need One and What Does the SRA Expect?

DGLEGAL
Services for Lawyers

Presenters

Raquel Britton | Compliance Officer | DG Legal

Raquel works closely with firms to design, implement and strengthen financial crime frameworks tailored to their specific risk profiles and leads the development and maintenance of AML/CTF policies, procedures and firm-wide risk assessments, helping firms respond to evolving regulatory requirements and enhance organisational resilience.

View Raquel's Full Bio

Femi Ngele | Compliance Officer | DG Legal

Femi has experience supporting firms with SRA AML investigations, desk-based reviews and the development and implementation of robust compliance frameworks tailored to firm-specific risks. Her work includes assisting with Firm Wide Risk Assessments, AML and compliance policies and procedures, Regulation 21 audits, CQS audits and file reviews.

View Femi's Full Bio

Agenda

- What does Regulation 21(1)(c) actually say?
- Does your firm need an independent audit?
- What does the SRA expect to see?
- Common failings identified in AML reviews
- Strengthening your compliance framework

The Legal Obligation

The Statutory Text

Regulation 21(1)(c) MLRs 2017: A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to "the independent audit function to test compliance with [AML] policies and procedures."

"Appropriate and risk-sensitive"

The obligation is not absolute. Whether an independent audit is required — and what form it takes — depends on the nature, size and complexity of the firm's business. A sole practitioner doing low-risk work is not expected to commission a full third-party audit.

"Independent" means genuinely independent

The audit function must be independent of the area it is testing. This does not always mean an external auditor — internal audit can satisfy the requirement where the auditor has no involvement in the work being reviewed and reports directly to senior management.

Three limbs — all connected

Reg 21(1)(c) sits alongside the MLRO (21(1)(a)) and MLCO (21(1)(b)) obligations. The audit function tests whether those roles and the firm's wider AML controls are working in practice — it is the assurance layer over the whole framework.

The Proportionality Test

Factors to Consider

There is no single answer. The obligation is risk-sensitive. Firms must assess their position against the following factors and document their reasoning.

Size and complexity

Larger firms with multiple offices, practice areas or jurisdictions face greater ML/TF risk and are more likely to require formal independent audit. Sole practitioners and small firms may conclude it is not proportionate.

Volume and nature of regulated work

Firms handling high volumes of client money, conveyancing, corporate transactions or trust work carry higher inherent risk. The greater the exposure, the stronger the case for independent testing.

Customer and jurisdiction risk

Firms with PEP clients, international clients, or exposure to high-risk jurisdictions should reflect this in their audit decision. The firm-wide risk assessment is the starting point.

Previous compliance issues

Firms that have received SRA feedback, had SAR failures, or identified control weaknesses should treat this as a strong indicator that independent testing is required — regardless of size.

Time since last audit or review

Even where a firm has concluded an audit is not required, this should be revisited periodically. A decision made in 2019 may not reflect the firm's current risk profile or the regulatory environment.

Availability of internal audit resource

Some firms have internal compliance or risk functions capable of conducting independent testing. This may satisfy the requirement — provided the reviewer is genuinely independent of the work being tested.

Evidential Standard

Whether you need one or not – you must evidence it

We have concluded an audit *is* required

- Document the factors that led to this conclusion (risk assessment, firm size, practice areas, prior issues)
- Define the scope, frequency, and format of the audit
- Confirm the independence of the reviewer — internal or external
- Ensure findings are reported to the MLCO and senior management
- Record any remediation actions taken as a result
- Review and update the audit scope after material changes to the business

We have concluded an audit *is not* required

- Document the specific factors that support this conclusion — don't just assert it
- Cross-reference to the firm-wide risk assessment and relevant risk ratings
- Confirm what alternative assurance mechanisms are in place (eg file reviews, COLP/COFA oversight)
- Record who made the decision and when — MLCO sign-off as minimum
- Set a review date — the decision should not be left to stand indefinitely
- Revisit immediately if the firm's risk profile, structure, or regulatory position changes

SRA Expectations

The Inspection Standard

1. **A documented, reasoned decision on the audit obligation**
   The SRA expects to see evidence that the firm has actively considered Regulation 21(1)(c) and reached a documented conclusion. An undocumented assumption — in either direction — is not sufficient.

2. **AML policies that address the audit function**
   The firm's AML policy should explicitly reference the independent audit obligation, describe the firm's approach, and explain how the decision was reached. Generic templates that omit this section are a common inspection finding.

3. **Evidence of independent testing where required**
   Where the firm has determined that an audit is required, the SRA will expect to see audit reports, findings, and evidence of follow-up action. The audit must be genuinely independent — not a self-review by the person whose work is being tested.

4. **Integration with the firm-wide risk assessment**
   The audit decision should flow from the firm's risk assessment. The SRA will look for a clear link between the risk profile identified and the level of independent assurance applied. Risk assessment and audit policy should be consistent.

5. **Reporting to senior management**
   Audit findings — or confirmation that no audit has been conducted and why — should reach the MLCO and senior management. The MLRO's annual report is an appropriate vehicle. The SRA expects audit to feed into governance, not sit in isolation.

What Goes Wrong

Recurring Issues Identified by the SRA and OPBAS

No documented decision on Reg 21(1)(c)

The most common finding. Firms have simply not considered whether an independent audit is required. There is no policy provision, no documented reasoning, and no audit or explanation of why one was not conducted.

AML policy omits the audit obligation entirely

Many firms use standard template policies that predate the current regulatory focus on audit. The independent audit function is either absent from the policy or described in vague, uncommitted terms with no firm-specific content.

Audit conducted but not genuinely independent

Where firms do conduct a review, the reviewer is often the MLRO reviewing their own work, a fee-earner in the same team, or a compliance officer with day-to-day responsibility for the controls being tested.

Findings not followed up or escalated

Firms that do commission audits sometimes fail to act on the findings. Where issues are identified and not remediated, this compounds the original control weakness and demonstrates that the audit function is not embedded in governance.

Decision treated as a one-off exercise

The audit decision is made once and never revisited. As the firm grows, takes on new practice areas, or faces regulatory developments, the original analysis becomes stale — but no one reviews it.

Risk assessment and audit decision inconsistent

A firm's risk assessment identifies high inherent risk in its client base but has concluded no audit is required with no explanation of how these are reconciled. The SRA will identify this inconsistency on inspection.

Practical Steps

The Inspection Standard

1. **Conduct a Reg 21(1)(c) gap analysis** Review your current AML policy against the independent audit obligation. Does it address the requirement? Is there a documented decision? If not, this is your immediate action.
2. **Cross-reference your firm-wide risk assessment** Your audit decision must be consistent with your risk assessment findings. If your risk assessment shows elevated risk in any area, your audit policy should address how that risk is independently tested.
3. **Define what 'independent' means for your firm** If using internal resource, document why that person is independent of the work being reviewed. If using an external firm, retain evidence of their scope, findings, and your firm's response.
4. **Build the audit cycle into your compliance calendar** Whether you audit annually, every two years, or have concluded no formal audit is required, record this in your compliance schedule and make the decision visible at governance level.
5. **Ensure findings feed into governance** Audit reports should be reviewed by the MLCO and summarised in the MLRO's annual report. Actions arising must be tracked to completion — not filed away.
6. **Review the decision annually and after material changes** The proportionality analysis is not a one-off exercise. Set a fixed annual review date. Trigger an unscheduled review if the firm expands, takes on new practice areas, or receives SRA feedback.

Contact Details

DGLEGAL
Services for Lawyers

T: 01509 214 999
E: admin@dglegal.co.uk
W. https://dglegal.co.uk