waystone

What FSRA Firms Should Put in Their Internal Audit Scope

A practical guide for ADGM firms that want internal audit to drive value, not just produce reports

Internal audit should not feel like an annual compliance exercise. It should not be a long meeting, a polite sample review and a final report that says “broadly satisfactory” while everyone quietly knows the customer files still need work.

For firms registered in the Abu Dhabi Global Market (‘ADGM’) and regulated by the Financial Services Regulatory Authority (‘FSRA’), internal audit needs to be sharper than that. Recent outcomes from the FSRA demonstrate a consistent message: firms are expected to understand their obligations, operate their controls, evidence what they did, and fix issues properly. Recent findings have covered multiple areas including anti-money laundering (‘AML’), sanctions and targeted financial sanctions (‘TFS’), CRS/FATCA, regulatory reporting, prudential resources, client money, outsourcing, governance, permissions and remediation discipline.

The lesson is simple: policies are useful, but evidence wins.

If your firm is planning its internal audit, whether it is refreshing the internal audit plan or considering a new provider, the scope needs to be practical, firm-specific and grounded in real regulatory risk.

1. Start with the Firm’s Actual Business Model

A strong internal audit scope should begin with the firm itself, not a template.

The audit should consider:

- what permissions the firm holds
- what restrictions or conditions apply
- what products and services are offered
- who the clients are
- which jurisdictions are involved
- whether client money or client assets are touched
- what areas are outsourced
- what systems, portals and spreadsheets are relied on
- what recurring filings are due
- whether compliance depends on one person, one provider or one process

This matters because several regulatory issues arise when firms use policies that are too generic, compliance monitoring plans that are too standard, or procedures copied from another business or jurisdiction. Outcomes

from the FSRA have identified weaknesses where procedures existed but were not sufficiently tailored or evidenced in practice.

Practical internal audit question:
Would this audit scope still make sense if the firm changed business model, client type or permission? If yes, it may be too generic.

2. Governance: Can Senior Management See What Really Matters?

Good governance is not about having more meetings. It is about whether the right people see the right issues early enough to act.

Internal audit should review whether the board and senior management receive meaningful information on:

- regulatory breaches and near misses
- overdue filings
- AML and sanctions exceptions
- high-risk clients
- CRS/FATCA filing status
- prudential or capital issues
- outsourcing problems
- unresolved audit or compliance findings
- repeat issues

Recently published outcomes from the FSRA show that weak governance often appears as unclear ownership, limited challenge, poor escalation or delayed remediation.

What internal audit should test:

- board and committee packs
- compliance and Money Laundering Reporting Officer ('MLRO') reports
- breach logs
- regulatory correspondence trackers
- open action logs
- evidence of challenge and follow-up

What good looks like:
Senior management can see issues clearly, understand the consequences, and track whether action has actually been taken.

3. Compliance Monitoring: Useful Control or Annual Theatre?

A compliance monitoring programme should be one of the firm's best early-warning tools. It should test whether the firm's controls are working before a regulator, client, auditor or incident proves that they are not.

The problem is that many compliance monitoring programmes still look too neat. They test familiar topics, but not always the firm's real risk points.

For an FSRA firm, the compliance monitoring programme should be tailored to:

- Its permissions and restrictions

- AML and sanctions risk
- client onboarding
- CRS/FATCA obligations
- prudential reporting
- outsourcing
- regulatory filings
- client money or assets
- product approval
- financial promotions
- previous findings and complaints

Findings from the FSRA have shown that firms may have policies and monitoring plans but still miss unresolved screening alerts, weak customer risk assessments ('CRA'), incomplete customer due diligence ('CDD'), reporting failures and poor outsourcing oversight.

Practical internal audit question:
Is the compliance monitoring programme testing the things most likely to go wrong in this firm?

If not, it is probably a calendar, not a control.

4. AML: The File Must Tell the Story

AML should be a core part of most FSRA internal audit scopes. The review should not simply check that forms exist. It should test whether the file explains the risk decision.

A good AML file should answer:

- Who is the customer?
- Who owns or controls the customer?
- Why was the risk rating assigned?
- What screening was performed?
- Were alerts reviewed properly?
- Is there PEP, sanctions, adverse media or high-risk country exposure?
- Was source of funds or source of wealth required?
- Was EDD completed where needed?
- Has the file been updated when circumstances changed?

Outcomes from the FSRA have identified issues including weak business risk assessments ('BRA'), repetitive customer risk assessment wording, unresolved screening matches, incomplete beneficial ownership work, missing certified ID evidence, inadequate PEP handling and weak enhanced due diligence ('EDD').

What internal audit should test:

- business risk assessment
- customer risk assessments
- CDD files
- beneficial ownership evidence

- PEP and adverse media checks
- screening alerts and closure rationale
- SOF/SOW evidence
- EDD approvals
- periodic reviews and trigger-event reviews

Practical takeaway:
If the file cannot explain the decision, the control is not strong enough. “The relationship manager knows the client” is not an audit trail. It is a sentence looking for evidence.

5. Sanctions and TFS: Do Not Just Trust the Screening Tool

Screening systems are useful. They are not a substitute for judgement.

Internal audit should test whether screening alerts are reviewed, documented, escalated and closed properly. It should also check whether sanctions, TFS, Financial Action Task Force (‘FATF’) and high-risk jurisdiction updates are reflected in the firm’s policies, systems and risk assessments.

Recent findings have shown that unresolved alerts, weak closure rationale and inadequate TFS assessment can create real control concerns.

What internal audit should test:

- screening system configuration
- customer and beneficial owner screening
- PEP, sanctions and adverse media results
- unresolved alerts
- closure rationale
- escalation to MLRO
- ongoing screening
- FATF and sanctions update process
- TFS risk assessment

Practical takeaway:
The screening tool raises its hand. The firm still has to answer the question.

6. CRS and FATCA: Start at Onboarding, Not at Filing

CRS and FATCA issues often appear as reporting errors, but the root cause usually starts much earlier.

Common control weaknesses include:

- self-certifications collected late
- forms not signed or dated
- missing tax residence
- invalid or unsupported TINs
- inconsistent entity classifications
- missing Passive NFE/NFFE controlling persons

- nil returns without enough supporting logic
- annual returns filed but risk assessments missed
- portal evidence not retained

Outcomes from the FSRA have repeatedly focused on self-certification validity, reportable account completeness, TIN treatment, controlling person reporting and missed AEOI portal obligations.

What internal audit should test:

- self-certifications at account opening
- completeness of tax residence and TIN fields
- signature and date checks
- entity classification
- passive NFE/NFFE controlling person logic
- reportable account population
- nil return approval rationale
- annual return to client/investor register reconciliation
- CRS/FATCA risk assessment evidence
- AEOI portal screenshots

Practical takeaway:
The annual return is the output. The real control starts the day the account or investor is onboarded.

7. Regulatory Reporting: Not Admin, Actual Governance

Regulatory reporting can look administrative until it is missed. Then it becomes a governance issue.

Internal audit should review the full regulatory obligations calendar, including:

- AML Returns
- prudential returns
- auditor reports
- annual accounts
- CRS/FATCA filings
- risk assessments
- annual supervision fees
- regulatory notifications
- portal submissions

Outcomes from the FSRA show that missed or repeated filings can lead to serious consequences, particularly where the firm cannot evidence ownership, escalation or submission.

What internal audit should test:

- regulatory obligations register
- filing calendar
- owners and backup owners

- submission evidence
- portal access
- overdue items
- fee payments
- board reporting of late or missed obligations

Practical takeaway:
Every filing needs an owner, a backup owner, a deadline and proof. Hope is not a filing control.

8. Prudential Resources and Financial Reporting

Where relevant, internal audit should cover capital, liquidity and financial reporting controls. Recent actions from the FSRA have highlighted issues around capital resources, liquid assets, audited expenditure, IFRS accounts, auditor reports and unpaid fees.

What internal audit should test:

- capital calculations
- liquid asset evidence
- EBCM calculations
- audited expenditure inputs
- finance working papers
- auditor reports
- IFRS financial statement process
- annual fee payment controls
- board reporting of capital adequacy

Practical takeaway:
Capital calculations should be reviewed properly. One spreadsheet and a confident nod should not be the control.

9. Permissions and Perimeter: Are We Doing What We Are Allowed to Do?

Internal audit should test whether the firm's activities match its permissions. This is especially important where firms grow quickly, launch new products, rely on group entities, use Special Purpose Vehicles ('SPVs'), alter payment flows, or promote services across jurisdictions.

Outcomes from the FSRA have shown the seriousness of firms operating outside permission, using unregulated structures, making misleading authorisation claims, or not maintaining clear group boundaries.

What internal audit should test:

- FSP permissions and restrictions
- product approval process
- new business approvals
- marketing materials
- website wording
- client agreements
- group entity arrangements

- introducer and referral arrangements
- payment or settlement flows

Practical takeaway:
If the business has evolved but the permissions analysis has not, that is a problem waiting for a meeting invite.

10. Outsourcing: Who Is Checking the Checker?

Outsourcing can be sensible and efficient. But firms remain responsible for what is outsourced.

Internal audit should assess whether the firm has proper oversight of administrators, outsourced compliance providers, MLROs, tax advisers, group teams, IT providers and operational partners.

Findings from the FSRA have shown issues where firms relied on providers without enough challenge, evidence, escalation or understanding of what had actually been done.

What internal audit should test:

- outsourcing register
- provider due diligence
- service agreements
- responsibility matrix
- oversight meetings
- deliverable review
- issue escalation
- access to working papers
- exit plans

Practical takeaway:
If the firm cannot explain what the provider did and how it reviewed the work, oversight is weak.

11. Client Money and Client Assets

Where relevant, this should be high priority. Client money and client asset weaknesses can create immediate regulatory, client protection and reputational risk.

Internal audit should test whether client funds and assets are identifiable, segregated, reconciled and properly protected. Findings from the FSRA have shown the risk of unclear bank account use, weak records and third-party arrangements without sufficient safeguards.

What internal audit should test:

- client money classification
- bank account ownership
- segregation
- reconciliations
- client ledgers
- payment approvals
- third-party account usage

- formal agreements with third parties
- breach logs

Practical takeaway:
If no one can clearly explain where client money sits and why, stop and investigate.

12. Policies and Procedures: Current, Local and Usable

Policies should be practical documents that reflect how the firm actually operates. They should not be decorative.

Internal audit should review whether policies are:

- current
- approved
- version controlled
- aligned to ADGM requirements
- tailored to the firm
- communicated to staff
- consistent with actual practice

Regulatory findings have highlighted issues where firms used procedures that were outdated, incomplete, or not tailored to local requirements.

Practical takeaway:
A polished policy from another jurisdiction may look impressive. It may also be wrong.

13. Training: Make it Useful

Training should help staff make better decisions. It should not just prove attendance.

Internal audit should test whether training is role-specific and linked to the firm's actual risks.

What internal audit should test:

- AML training
- sanctions/TFS training
- CRS/FATCA training
- conduct and financial promotions training
- board training
- new joiner training
- attendance
- knowledge checks
- follow-up for non-attendance

Practical takeaway:
Good training answers the question: "What should I do differently tomorrow?"

14.Remediation: Closed Should Mean Fixed

This is one of the most important areas. Firms often close actions because they updated a policy or sent an email. That is not enough.

Internal audit should test whether the root cause was addressed and whether the new or revised control actually works.

What internal audit should test:

- issue logs
- regulatory findings
- compliance monitoring findings
- prior audit findings
- root cause analysis
- action plans
- closure evidence
- independent validation
- repeat findings

Practical takeaway:
An action is not closed when the document is uploaded. It is closed when the control works.

Questions to Ask Your Internal Audit Provider

If you are appointing a new provider or reviewing the one you already have, ask these questions.

Scope

1. How will you tailor the scope to our FSRA permissions?
2. How will you reflect our business model, clients and outsourcing?
3. Will you test evidence or mainly review policies?
4. How will you decide sample sizes?
5. How will you cover previous findings and repeat issues?

Technical coverage

1. Can you review AML, sanctions/TFS, CRS/FATCA and regulatory reporting?
2. Can you review prudential controls if relevant?
3. Can you test client money/client assets if relevant?
4. Can you assess permissions and perimeter risk?
5. Can you review outsourcing oversight?

Reporting

1. Will you explain root causes?
2. Will findings be practical and clearly graded?
3. Will actions be realistic?
4. Will you avoid vague recommendations like “enhance the process”?
5. Will you validate closure later?

Value

1. Will the report help the board ask better questions?
2. Will management learn something useful?
3. Will the work stand up if the FSRA asks for evidence?
4. Will you challenge us constructively?
5. Can you explain technical issues in plain English?

A good provider should make the firm better, not just produce a tidy report.

Simple Internal Audit Scope for FSRA Firms

At a minimum, most firms should consider covering:

Area	Why include it
Governance and board management information	To confirm issues are visible, owned and escalated
Compliance monitoring programme	To ensure testing is firm-specific and risk-based
AML, BRA, CRA, CDD and EDD	To confirm customer risk is understood and evidenced
Sanctions/TFS screening	To test alert handling, escalation and closure rationale
Regulatory reporting	To confirm filings are owned, tracked and evidenced
CRS/FATCA	To test onboarding, tax data, reporting and portal evidence
Outsourcing	To confirm providers are overseen and challenged
Prudential resources	To test capital, liquidity and financial reporting where relevant
Permissions and perimeter	To ensure activity remains within FSRA permissions
Client money/assets	To confirm safeguarding where relevant
Policies and procedures	To ensure documents are current, local and usable
Training	To confirm staff understand practical obligations.
Remediation	To ensure issues are fixed, not just closed.

How We Can Help

We support ADGM and FSRA-regulated or registered firms with practical internal audit, assurance and health check reviews.

We can help with:

- internal audit planning and delivery
- independent assurance reviews
- compliance health checks
- AML and sanctions/TFS reviews
- regulatory reporting reviews
- prudential and financial reporting reviews
- client money and client asset reviews
- FSP permissions and perimeter reviews
- outsourcing oversight reviews
- compliance monitoring programme design or refresh
- policy and procedure review or creation
- customer file testing
- board and senior management reporting improvements
- practical staff training

Our approach is simple: focus on the controls that matter, test whether they work, explain the issues clearly, and leave the management team with actions they can actually implement.

A good internal audit should not feel like a formality. It should feel like a useful mirror, occasionally uncomfortable, but far better than being surprised later.

Contact Us →