Internal Audit in a Faster Regulatory Environment: Can Your Firm Demonstrate It?

Regulated firms today are not short of regulatory updates. Dear SEO letters, thematic reviews, cyber alerts, AML guidance, enforcement actions and rulebook amendments continue to flow across the UAE's regulatory landscape.

The challenge is no longer identifying regulatory change. Most firms have processes in place to do that.

The more important question is whether they can demonstrate what happened next.

Across the DFSA, FSRA, VARA, CBUAE, and the UAE capital markets framework, including the CMA, regulatory expectations are becoming increasingly aligned. Firms are expected not only to understand their risks and maintain effective controls, but also to evidence that those controls operate effectively in practice.

Expectations continue to rise across governance, AML/CFT, sanctions compliance, cyber resilience, outsourcing, operational resilience, digital assets, client asset protection, regulatory reporting, and Board oversight.

For Boards and senior management, the question is straightforward:

> ***If a regulator requested evidence tomorrow, could we confidently demonstrate that our control environment is keeping pace with regulatory expectations?***

Updating a policy is not enough. Recording an action in a tracker is not enough. Discussing an issue at committee level is not enough.

> ***Has the underlying process changed? Were appropriate individuals trained? Was accountability clearly assigned? Did management and the Board receive meaningful reporting? Were controls independently tested? Can implementation be evidenced quickly and clearly?***

This is where internal audit has evolved beyond a periodic review function. At its best, it provides Boards and senior management with an independent assessment of whether the organisation is truly managing risk and maintaining control, rather than simply documenting actions as completed.

The Difference Between "Updated" and "Embedded"

Most firms invest significant effort in responding to regulatory developments. The challenge is rarely one of commitment. More often, it is one of demonstrating effectiveness.

A regulatory update is logged. A policy is revised. A communication is issued. The action is marked as complete.

Months later, however, a different question arises:

> ***Can we show that the change is working in practice?***

This is often where weaknesses emerge.

Effective regulatory change management should extend beyond policy updates. It should include impact assessments, clearly assigned ownership, control enhancements, staff communication, testing, governance reporting, and documented evidence of implementation.

Internal audit plays a critical role in validating this process. It assesses whether regulatory change has truly been embedded into day-to-day operations rather than merely recorded as completed.

Regulatory Change Is a Business-Wide Responsibility

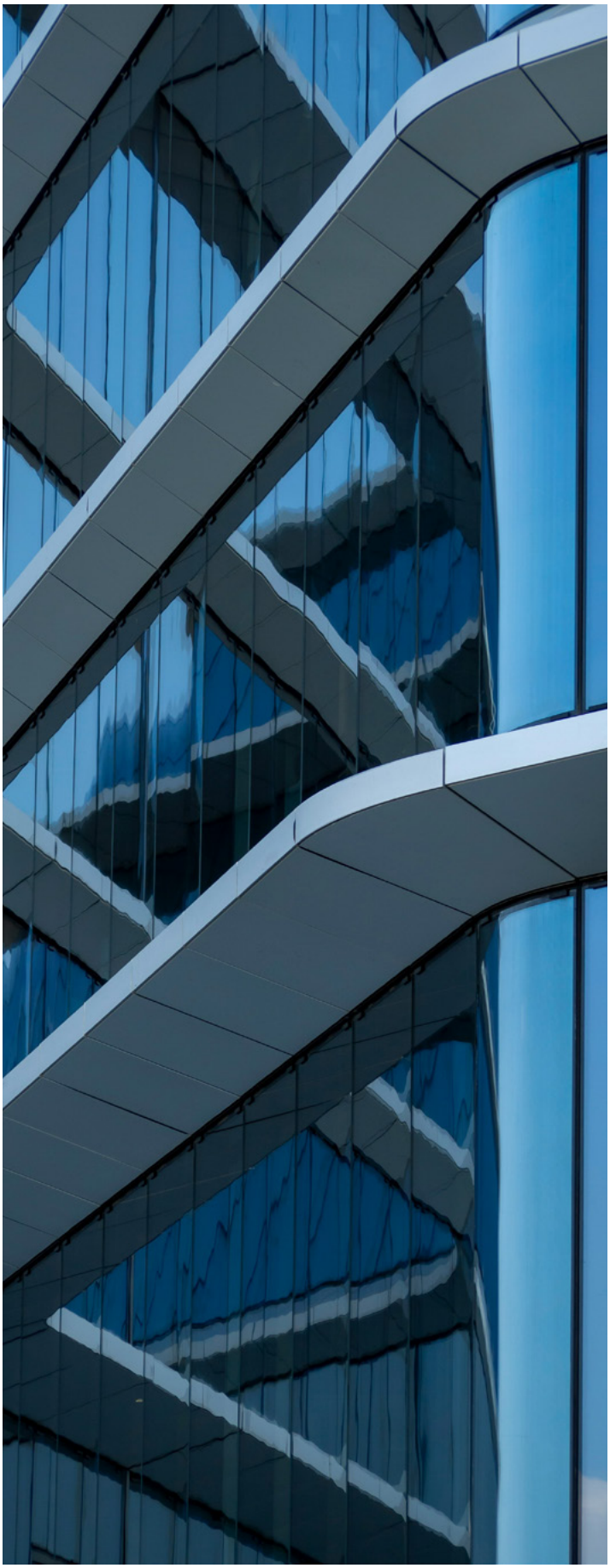
One of the most common misconceptions is that regulatory change is solely a Compliance function responsibility.

In reality, regulatory developments rarely affect just one department.

An AML-related change can impact onboarding procedures, customer risk assessments, sanctions screening, periodic reviews, suspicious activity reporting, and regulatory submissions. Cybersecurity and operational resilience requirements can affect technology teams, third-party providers, incident management processes, business continuity arrangements, and Board reporting. Governance-related developments may influence committee structures, accountability frameworks, reporting lines, conflicts management and escalation procedures.

Compliance may identify and interpret the change, but implementation requires engagement across the organisation.

This is why effective internal audit takes a cross-functional view. Reviewing policies alone is insufficient. The real measure of success is whether governance arrangements, people, systems, and controls have adapted appropriately.



What Internal Audit Commonly Identifies

Internal audit rarely discovers a complete absence of controls. More often, it identifies controls that are outdated, inconsistently applied, poorly documented, or difficult to evidence.

Several recurring themes continue to emerge.

Governance Often Appears Stronger on Paper Than in Practice

Board packs, committee charters, governance frameworks, and reporting structures may be well documented. However, meeting minutes do not always demonstrate meaningful challenge, informed decision-making, or effective follow-up.

Group governance arrangements may be referenced, while local entity responsibilities remain unclear.

Regulators are increasingly interested not simply in governance structures, but in how governance functions in practice.

Key Person Dependency Creates Hidden Risks

Many firms remain heavily dependent on individuals such as the SEO, Compliance Officer, MLRO, Deputy MLRO, Finance Officer, or Risk Officer.

While these individuals often provide valuable expertise, excessive reliance on a small number of people creates operational and regulatory vulnerabilities. Informal cover arrangements, outdated role descriptions, and unclear ownership of responsibilities can quickly become control weaknesses.

AML Weaknesses Are Usually Revealed Through File Testing

Financial crime remains a significant regulatory focus across the region.

Recent supervisory reviews and enforcement actions continue to highlight deficiencies in customer due diligence, enhanced due diligence, customer risk assessments, sanctions screening, suspicious activity escalation, AML reporting, and record retention.

An AML framework may appear robust on paper, but regulators ultimately assess whether customer files contain appropriate evidence. Risk ratings, approvals, screening outcomes, periodic reviews, and reporting data must all be supported and documented.

Cyber, Outsourcing and Data Quality Have Become Governance Matters

Cyber resilience and operational resilience are no longer purely technology concerns. They are Board-level issues.

A business continuity plan may exist, but has it been tested? A critical technology provider may be in place, but has its resilience been assessed? An outsourcing arrangement may be formally documented, but are performance expectations, reporting obligations, and escalation procedures clearly defined?

Similarly, a regulatory return may have been submitted on time, but does the underlying data reconcile to source systems?

Operational weaknesses can quickly become regulatory concerns when firms cannot demonstrate effective oversight.

Recent Regulatory Findings Reveal Familiar Patterns

Enforcement outcomes and supervisory reviews across the region continue to point to familiar underlying causes.

These include:

- missed regulatory filings
- incomplete AML documentation
- weak escalation processes
- poor governance records
- deficient client classification controls
- outsourcing oversight gaps
- prudential reporting weaknesses
- unclear accountability arrangements

Such issues rarely emerge overnight.

More commonly, they begin with relatively minor weaknesses:

- an overdue review
- a missing approval

- an unclear owner
- an outdated procedure
- a finding that was acknowledged but never fully remediated.

By the time regulators identify these deficiencies, they have often existed within the organisation for a considerable period.

This is where internal audit delivers tangible value. It provides organisations with the opportunity to identify and address issues before they develop into regulatory, operational, or reputational events.

What Boards Should Expect from Internal Audit

A robust internal audit function should help Boards and senior management answer fundamental questions about the organisation's control environment:

- are our key risks clearly understood?
- are our controls operating effectively in practice?
- have regulatory changes been properly embedded?
- are findings closed with appropriate evidence?
- are we overly reliant on specific individuals, third parties, or group processes?
- could we substantiate our position if challenged by a regulator?

Effective internal audit does more than assess past performance.

It acts as an early warning system, identifying emerging vulnerabilities before they become significant issues and providing management with the insight needed to address risks proactively.

Final Thoughts

In today's regulatory environment, success is not determined by the length of a policy manual or the sophistication of a tracker.

The firms best positioned to meet growing regulatory expectations are those that can demonstrate, with evidence, that their governance, risk management, and control frameworks are operating effectively in practice.

That requires:

- evidence
- challenge
- accountability
- follow-through
- independent assurance

When delivered effectively, internal audit provides Boards and senior management with a clear understanding of where the organisation stands, where vulnerabilities exist, and where attention is required before small issues become significant regulatory, operational, or reputational concerns.

How Waystone can help

If your firm is reviewing its internal audit arrangements, assessing regulatory readiness, or evaluating whether its assurance framework remains fit for purpose, Waystone can help.

Our team provides practical, risk-based internal audit solutions designed to give Boards and senior management greater confidence, visibility, and insight into their control environment.

To learn more about how Waystone can support your internal audit requirements, please get in touch.

Contact Us →