ISITC EUROPE CIC

TORI
Experience. The difference.

Creating a Superior Compliance Operation Roundtable Report

ISITC Europe CIC

ISITC Europe Roundtable – Creating A Superior Compliance Operation

Date: September 17th, 2025

Kindly hosted by: TORI
Experience. The difference.

Introduction & Context

- **Chatham House Rule:** The roundtable was conducted under Chatham House rules, allowing confidential, honest knowledge sharing.
- **Purpose:** To bridge the knowledge gap between compliance and operations functions in financial services, particularly in light of rapid regulatory and technological changes.
- **Attendees:** Senior compliance officers, market heads, operations leaders from major financial institutions and technology service providers.

Main Topics Discussed

1. The Compliance–Operations Knowledge Gap

- **Persistent Themes:**
    - Ongoing lack of clarity from the FCA about compliance expectations.
    - Insufficient understanding among compliance officers about operations and IT developments, despite the direct downstream impact.
    - Compliance teams often operate with influence but without budgetary or direct operational control, leading to difficulties in proactive oversight.

2. Leadership, Vision, and Regulatory Direction

- **Concerns Over FCA Leadership:**
    - General call for the FCA to provide more prescriptive, structured direction, particularly in emerging areas like AI and digital assets.
    - Absence of a coherent industry vision; debate over who should lead (regulator, government, exchanges, or banks).
    - Political motivations sometimes driving regulatory change faster than operational capacity can adapt (e.g., T+1 settlements).
    - Lack of joined-up thinking and strategic direction highlighted as a risk, especially given international fragmentation.

3. AI and Compliance: Regulation, Risks, and Adoption

Regulatory Landscape

- **UK vs. EU:**
    - EU's AI Act (in force 2026): Highly prescriptive, risk-based categorization of AI applications.
    - UK: Principles-based and less specific; requires institutions to self-define boundaries.
    - Practical impact: UK/global firms must comply with both sets, often driving them to adopt the strictest standards by default.

Key Compliance Risks Associated with AI

- Regulatory ambiguity on acceptable AI use-cases, especially for customer-facing and critical decision-making processes.
- Explainability: Strong regulatory and internal requirements for a human-in-the-loop and transparent, auditable decision paths, especially where customer outcomes or creditworthiness are involved.
- Risk of data leakage, privacy issues (GDPR/criminal investigations), and the challenge of validating outputs, particularly when using external AI tools.
- Legal and compliance liability when incorrect or "hallucinated" AI-derived advice circulates within the business.
- Data sovereignty issues, particularly around cloud-based AI services and off-site data processing.

In-House AI Tooling and Adoption

- Many firms developing or piloting proprietary AI models trained exclusively on internal policy/procedure data to mitigate regulatory and privacy risks.
- Significant costs and resources devoted to preparing and reformatting legacy data/policies for AI ingestion.
- Expanded use of tools such as Microsoft Copilot, with varying degrees of compliance-specific configuration and training.
- Awareness gap: frontline non-compliance staff often perceive AI as a replacement for compliance/legal consultation, presenting risk that incorrect, uncontextualized advice will drive business decisions.

Controls, Governance, and Best Practice

- Movement towards formal governance structures: dedicated AI oversight committees, horizontal controls across all functions, use-case tracking, check-and-challenge processes.
- Tension between policy ownership (compliance vs. operational teams) and clear three-lines-of-defence structures.
- Call for regulator-provided clear, non-negotiable "red lines" for AI usage, especially relating to data sensitivity and consumer protection.

4. Legacy Technology & Accelerated Settlements (T+1, T+0)

- General agreement that legacy technical infrastructure is brittle and a rate-limiting factor on innovation (e.g., T+1 settlements).

- **Critical issues highlighted:**
    - Fragmentation and inconsistency across European CSDs (23+), each operating on their own local rule sets.
    - Batch processing and "evergreening" of mainframes/software, with high operational and resiliency risk.
    - Onboarding and KYC/AML processes often manual, slow, and seen as the primary bottleneck for faster settlements.
    - Use of AI for pattern recognition and process automation (e.g., SAR reporting) seen as valuable but not a panacea.
- **Risks with Accelerated Settlement:**
    - Increased risk of fraud, error, and criminal exploitation as assets move more quickly and irreversibly.
    - Compliance and controls may not keep pace, increasing operational and reputational risk.
    - Debate on balance between operational/compliance responsibilities during settlement fails or fraud.

5. Tokenized Assets and Digital Markets

- Significant growth in tokenized asset platforms (banks, stock exchanges entering), but regulatory clarity lags far behind pure technology development.
- **Noted Compliance Challenges:**
    - Complex, ambiguous mapping of roles—issuer, custodian (hot/cold wallets), and legal ownership—across jurisdictions.
    - Overlaying traditional controls on tokenized assets remains default practice in absence of specific guidelines.
    - Security/custody challenges: cold/hot wallet management, real-time vs. batch access.
    - Need for truly international standards to prevent piecemeal, reactive regulation in the wake of future crises.
    - Contrast between EU approach (first mover, often over-prescriptive and stifling) and the UK's more reactive stance.
- **Retail and Institutional Adoption:**
    - General hesitance from major banks to offer retail crypto products; reputational risk cited for custody of crypto in legal settlements.
    - Noted regulator U-turns (allowing retail access to crypto but restricting CFDs) criticized as confused and risky.

6. Compliance Talent, Budget, and the "Compliance Squeeze"

- **Talent Shortages & Retention:**
    - Compliance increasingly seen as high-liability but low-reward; budget constraints and recruitment challenges are endemic.
    - Good talent often poached or lost due to stress/burnout and higher pay elsewhere.
    - Personal liability (e.g., SMCR) has made the role less attractive, despite increased importance.
    - Training, onboarding, and retaining good compliance professionals recognized as key to raising standards system-wide.
- **Budget & Resource Tensions:**
    - Compliance viewed as a cost centre; struggle to secure adequate resourcing amid business-driven priorities and legacy cost structures.
    - Delayed or underfunded technology/infrastructure upgrades seen as contributing directly to ongoing compliance failures and fines.

7. Practical Tools, Technology, and Current Challenges

- Reliance on outdated tools (Excel, ad-hoc databases), patchwork solutions for horizon scanning and workflow management.
- Lack of robust, integrated compliance systems across most institutions; technology stacks often lag far behind lighter fintech competitors.
- Ongoing internal battle for IT investment, with front office and revenue-facing projects consistently prioritized over back/middle office, ops, and compliance upgrades.
- Examples of persistent "evergreening" of core systems due to complexity and fear of operational disruption on migration.
- Risk that without early compliance involvement in technology projects, costs and risks compound over time.

8. Regulatory Fines, Enforcement Trends, and Perceptions

- Regulator (FCA/SCA) seen as increasingly stretched; focus moves from sector to sector in cycles, sometimes missing root causes.
- Fines often treated as cost of doing business, especially if costs are low for larger institutions.
- UK seen as lagging behind US in compliance investment/enforcement but changing due to rising fine sizes and new risks.
- Frustration over lack of operational, regulatory, and compliance experience among many regulators (especially FCA).
- Perception that fines often hit risk/compliance functions after the fact, rather than operations or business units where issues originated.

Action Items

1. **Review and Strengthen AI Governance:**
    - Assign AI oversight committees and clarify reporting lines for compliance involvement in AI policies and deployments.
    - Map all current AI use-cases and ensure robust controls for data protection, explainability, and documentation.
    - Educate both compliance and broader business functions on required human-in-the-loop and disclosure requirements for AI-generated content.
2. **Enhance Policy Management Processes:**
    - Centralize and standardize all compliance and operational policies, ensuring traceability and accessibility for AI and human users.
    - Accelerate migration of legacy policy documentation into structured, machine-readable formats.
3. **Clarify Operational vs. Compliance Responsibilities:**
    - Conduct reviews to define and map perimeters of responsibility, ensuring clear hand offs and documentation between compliance, operations, and legal.
4. **Audit Technology and Systemic Risk:**
    - Evaluate robustness of current compliance and operational systems; prioritize upgrades based on identified risks and future regulatory changes.
    - Push for early-stage compliance involvement in all significant operational/technology projects.
5. **Foster Continuous Internal Dialogue:**
    - Establish or expand internal compliance and operations forums to promote ongoing discussion of emerging risks, technology adoption, and regulatory changes.
6. **Advocate for Regulatory Clarity and Industry Leadership:**
    - Engage with regulators to advocate for more prescriptive, forward-looking guidance, especially on AI and digital assets.
    - Support cross-industry efforts to drive best practices in ambiguous areas (e.g., KYC utilities, custody of digital assets).
7. **Strengthen Talent Pipelines:**
    - Promote, resource, and support graduate and professional training programs in compliance.
    - Develop and retain talent through internal training, mentorship, and career development initiatives.

Follow-up Points & Next Steps

- **Further Meetings:**
    - Continued roundtables on specific topics: AI governance, tokenized asset compliance, and accelerated settlements.
    - Suggest establishment of sub-groups for sharing experiences on internal AI adoption, policy management, and compliance technology upgrades.
- **Potential Industry Coordination:**
    - Explore coordinated approaches for utility development in KYC/onboarding.
    - Engage in ongoing dialogue with regulators regarding the need for more proactive, prescriptive guidance.
- **Ongoing Knowledge Sharing:**
    - Circulation of anonymized roundtable write-up for all attendees.
    - Promote networking and peer support—both informally and via formal forums.

Closing Reflections

- **Shared Sentiment:** Attendees found comfort, inspiration, and challenge in the realization that their struggles—spanning regulatory ambiguity, the relentless pace of change, and the complexity of technology—are universal across the sector.
- **Universal Need:** Universal call for better tools, clearer guidance, and more robust, forward-thinking compliance structures.
- **Critical Role of People:** The value of experienced compliance professionals was repeatedly emphasized.
- **Industry at a Crossroads:** Tech is moving fast; compliance must move just as fast, if not faster, to keep institutions and clients safe in a transforming landscape.

Session ended with informal networking and appreciation for the open, collaborative discussion.

About ISITC Europe CIC

ISITC Europe CIC is a not-for-profit industry body promoting education, innovation and collaboration throughout the global capital markets.