

# ONE COMPASS

YOUR COMPLIANCE SURVIVAL GUIDE | THE SEPTEMBER 2026 REVIEW

## AM I AT RISK?

### HIGH:

Significant impact – Immediate action required.

#### ● Luxembourg register deficiencies can now escalate

##### WHY IT MATTERS?

LBR has introduced an enhanced compliance process for incomplete or outdated RCS and RBE data, with enforcement beginning from 21 September 2026. For funds and managed entities, a filing inconsistency can become a visible governance weakness and may escalate if the 30-day remediation window is missed.

##### KEY ACTION

Run a targeted RCS/RBE reconciliation across relevant Luxembourg entities, allocate an owner for every discrepancy and retain evidence of correction and sign-off.

#### ● DORA incident reporting becomes a quality test

##### WHY IT MATTERS?

CSSF supplementary instructions sharpen expectations for complete, consistent and efficient DORA major ICT-incident reports. They do not create a new obligation, but they show how Luxembourg supervisors expect existing reporting duties to operate in practice.

##### KEY ACTION

Benchmark the incident playbook and reporting templates against the CSSF and ESA instructions, then test ownership, escalation, data capture and submission quality

### MEDIUM:

Moderate impact – May require adjustments.

#### ● Digital innovation becomes a supervisory priority

##### WHY IT MATTERS?

From 2027, ESMA's new Union Strategic Supervisory Priority will focus initially on AI and tokenisation alongside the existing cyber and operational resilience priority. Firms using AI tools, automated workflows or tokenised structures should expect more consistent supervisory questions about inventory, accountability, controls and investor safeguards.

##### KEY ACTION

Create or refresh the inventory of AI and tokenisation use cases, map accountable owners and third parties, and ensure boards receive decision-useful reporting.

#### ● Cyber product reporting is now live

##### WHY IT MATTERS?

From 11 September 2026, CRA manufacturers must report actively exploited vulnerabilities and severe incidents through the Single Reporting Platform. Most ManCos and AIFMs will be users rather than manufacturers, but scope, contractual notification and supplier readiness still need to be tested.

##### KEY ACTION

Confirm whether any group entity is a manufacturer, importer or distributor, and add CRA readiness to critical ICT-provider assurance and incident playbooks.

### LOW:

Minimal operational impact – Monitor.

#### ● UK AIF data signals where scrutiny may go next

##### WHY IT MATTERS?

The FCA's first market-wide analysis reports £1.8 trillion in UK-managed AIF assets in 2025, rapid private credit growth and concentrated leverage and liquidity risk. It is research, not a new rule, but it provides a baseline for UK AIFM reform and supervisory dialogue.

##### KEY ACTION

Use the findings to challenge product, liquidity and leverage assumptions, and monitor the FCA's modernisation of the UK AIFM regime.

#### ● Tokenised settlement moves closer to production

##### WHY IT MATTERS?

The ECB launched Pontes for settlement of tokenised wholesale transactions in central bank money and plans limited own-funds investment in tokenised securities. There is no immediate compliance project, but operating-model questions are becoming more practical.

##### KEY ACTION

For planned DLT products, assess custody, settlement finality, valuation, asset servicing, controls and governance before treating tokenisation as a distribution feature.



MY SURVIVAL TOOLS

The practical shortlist for the month. Prioritise evidence, ownership and decision-making rather than creating parallel compliance projects.

| TOPIC                            | ACTION REQUIRED                                                                                                                            | DEADLINE/URGENCY                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Luxembourg RCS/RBE data          | Reconcile entity, beneficial ownership, registered-office and outstanding filing data. Evidence corrections and accountable approval.      | Now; act within 30 days of any LBR notice                   |
| AI and tokenisation governance   | Inventory use cases, map accountable owners and suppliers, assess investor and operational risks, and add board-level reporting.           | Build into 2027 compliance planning now                     |
| DORA incident reporting          | Align classification, escalation, data capture and reporting templates with the CSSF and ESA operational instructions.                     | Apply now                                                   |
| CRA reporting readiness          | Determine role and scope; validate incident-routing, vulnerability escalation and supplier notification clauses.                           | Reporting applies from 11 Sep 2026                          |
| Critical dependency mapping      | Map shared infrastructure and concentration beyond direct suppliers; incorporate simultaneous disruption into testing.                     | Prompt review                                               |
| Irish AIF application forms      | Use the September 2026 QIAIF application form and third-party agreement template; update filing checklists and version controls.           | Immediate for live or planned Irish filings                 |
| Integrated UCITS/AIFMD reporting | Map current data ownership, reporting controls and delegate dependencies; track ESMA technical standards without delaying current returns. | Prepare during 2027 planning; implementation will be phased |



● ESMA sets a new supervisory priority on digital innovation from 2027

**WHAT’S CHANGING:**

ESMA will introduce a Union Strategic Supervisory Priority on digital innovation from 2027. Its initial focus is the use of artificial intelligence and tokenisation by supervised entities. The priority will run alongside the cyber and operational resilience USSP.

**ACTIONS REQUIRED:**

- Maintain an inventory of AI tools, models and material automated decisions, including outsourced and embedded functionality.
- Map tokenisation initiatives and proposed digital-asset structures to legal, operational and investor-protection risks.
- Set governance standards for approval, change control, testing, data, human oversight, incidents and board reporting.

● Cyber Resilience Act reporting obligations become applicable

**WHAT’S CHANGING:**

Manufacturers of products with digital elements must now notify actively exploited vulnerabilities and severe security incidents through the CRA Single Reporting Platform. An early warning is due within 24 hours and a full notification within 72 hours, with later final reports. The obligations are product-focused and should not be presented as a general incident-reporting duty for every financial entity.

**ACTIONS REQUIRED:**

- Perform a role-based scope assessment across products, software and group activities.
- Where the firm is a user, test whether suppliers can provide timely information needed for DORA and internal incident escalation.
- Align vulnerability management, legal review, communications and incident-routing procedures where CRA scope exists.

ONE PERSPECTIVE

Supervisory readiness starts with visibility. Firms often govern named AI projects but miss AI embedded in vendor platforms, productivity tools and operational workflows. Boards should ask where outputs influence regulated decisions, investor communications or controls, how errors are detected and who can stop use. For tokenisation, digital form does not remove traditional obligations on valuation, custody, liquidity, conflicts and oversight.

The practical issue for fund governance is the interface between regimes. A supplier may have CRA duties while a regulated financial entity has DORA obligations and contractual reporting needs. The control objective is a joined-up timeline and clear decision rights, not duplicate playbooks that produce inconsistent classifications or delayed escalation.

# EXPERT INSIGHTS



● **European Commission adopts revised ESRS and a voluntary standard**

**WHAT'S CHANGING:**

The Commission adopted revised ESRS and a voluntary reporting standard intended to simplify reporting while retaining decision-useful sustainability disclosures. The official Commission material states that mandatory datapoints are reduced by more than 60% and total datapoints by more than 70%. EFRAG issued a draft revised datapoint list on 28 August and invited fatal-flaw feedback by 23 October 2026.

**ACTIONS REQUIRED:**

- Confirm whether each entity remains in CSRD scope and verify the final legal application date after scrutiny and publication.
- Map current reporting processes to the revised disclosure architecture and identify data, control and assurance impacts.
- Treat EFRAG's datapoint list as support material and track its final version and the XBRL taxonomy.

● **ESMA advances integrated UCITS and AIFMD reporting**

**WHAT'S CHANGING:**

ESMA is progressing an integrated reporting model for UCITS and AIFs, based on harmonised templates and reduced duplication between national and EU reporting. No immediate reporting change applies, but the initiative may materially affect future data, oversight and service-provider arrangements.

**ACTIONS REQUIRED:**

- Monitor the development of the technical standards and phased implementation plan.
- Map current UCITS and AIFMD reporting processes, data ownership and delegated reporting dependencies.
- Avoid delaying compliance with existing reporting requirements while simplification is developed.

## ONE PERSPECTIVE

Simplification does not remove governance risk. A smaller disclosure set can increase the importance of materiality judgements, traceability and consistency between sustainability statements, risk management and fund disclosures. Boards should focus on who approves exclusions, how estimates are controlled and whether the evidence trail can withstand assurance and supervisory review.

The opportunity is not simply fewer returns. A single template can still reproduce weak ownership if source data, definitions and delegate controls remain fragmented. Firms should use the policy window to establish authoritative data owners, reconcile recurring fields across UCITS and AIFMD returns, and define challenge and sign-off standards before technical specifications harden.



● AMLA ongoing monitoring guidelines move beyond consultation

**WHAT'S CHANGING:**

AMLA’s consultation on draft guidelines under Article 26(5) AMLR closed on 3 September 2026. The draft addresses keeping customer information current and transaction and activity monitoring on a risk-based and proportionate basis. Industry responses, including the EBF submission, are stakeholder positions and should not be described as AMLA requirements.

**ACTIONS REQUIRED:**

- Track the final guidelines and implementation timing.
- Review whether customer refresh, event-driven review, transaction monitoring and documentation operate as one risk-based framework.
- Avoid redesigning controls solely around industry requests that AMLA has not accepted.

● EDPB consults on when GDPR administrative fines should be imposedJurisdiction Source

**WHAT'S CHANGING:**

The EDPB adopted draft Guidelines 04/2026 for public consultation. They provide a five-step methodology for determining whether an administrative fine should be imposed in addition to, or instead of, other corrective measures. They complement the existing guidance on calculating fine amounts.

**ACTIONS REQUIRED:**

- Review breach investigation records for evidence of accountability, intent or negligence, mitigation and remediation.
- Ensure incident committees document why decisions and corrective actions are appropriate and proportionate.
- Track the final guidelines after consultation closes on 13 November 2026.

ONE PERSPECTIVE

The hidden governance challenge is coherence. Periodic KYC, trigger events and transaction monitoring are often owned by different teams and systems. Firms should be able to show how new information changes risk ratings, monitoring intensity and escalation, while documenting proportionate departures from standard review cycles.

Fine exposure is influenced by the quality of decisions made before and after an incident. Clear ownership, timely containment, transparent escalation and a credible evidence trail can matter as much as the technical event. Boards should be able to demonstrate active oversight without prejudging legal liability.

# EXPERT INSIGHTS



● **ESMA Data Day 2026 focuses on integrated fund reporting and simplification**

**WHAT'S CHANGING:**

ESMA's Data Day 2026 will cover supervisory technology, simplification, integrated fund reporting, ESAP and crypto monitoring. The agenda signals continued work on reporting efficiency but does not itself change reporting obligations.

**ACTIONS REQUIRED:**

- Monitor outputs relevant to integrated fund reporting and regulatory-data quality.
- Identify reporting pain points caused by duplication, inconsistent data definitions and manual reconciliation.
- Avoid deferring current compliance in anticipation of future simplification.

## ONE PERSPECTIVE

Reporting simplification will reward firms with strong data lineage. If the same exposure, counterparty or fund attribute is defined differently across returns, a new reporting architecture will not automatically solve the problem. Firms should use the policy window to standardise ownership, definitions and controls.



● ECB launches Pontes and prepares own-funds investment in tokenised securities

**WHAT’S CHANGING:**

The Eurosystem launched Pontes to settle wholesale tokenised-asset transactions in central bank money. The ECB also began preparatory work to invest a small portion of its own funds in tokenised securities, initially focusing on euro-denominated public-sector and supranational issuance.

**ACTIONS REQUIRED:**

- No immediate action for firms without a tokenisation initiative.
- For live projects, map settlement, custody, asset servicing, cash-leg, legal finality and operational resilience arrangements.
- Monitor market access, eligible assets and the phased development of Pontes.

ONE PERSPECTIVE

Institutional infrastructure is reducing one barrier to tokenised markets, but product governance remains decisive. A tokenised security still needs clear rights, reliable valuation, robust custody and servicing, and controls around smart contracts and venue or platform dependency. Boards should approve the operating model, not just the product concept.

# EXPERT INSIGHTS



● **Central Bank of Ireland updates AIF application forms**

**WHAT'S CHANGING:**

The Central Bank of Ireland updated AIF application forms and supporting templates for certain fund types, including the QIAIF application form and agreements with third parties. The update affects documentation used for relevant Irish fund authorisations and filings.

**ACTIONS REQUIRED:**

- Confirm that current and future Irish AIF submissions use the latest forms.
- Update internal filing checklists and notify teams supporting Irish fund launches or amendments.

● **Ireland publishes roadmap for retail investment taxation**

**WHAT'S CHANGING:**

Ireland's Department of Finance published a roadmap to simplify retail investment taxation and outlined a new Investment Account for Irish tax-resident individuals. Eligible assets are expected to include listed securities and suitable retail funds, including ETFs. Key tax parameters are to be announced with Budget 2027 and legislation is expected through the Finance Bill.

**ACTIONS REQUIRED:**

- Monitor Budget 2027 and the Finance Bill before changing products or communications.
- Assess which UCITS, ETFs and distribution models may be eligible once final criteria are available.
- Prepare tax, operations, disclosure and distributor workstreams for a possible 2027 launch.

## ONE PERSPECTIVE

The regulatory change is narrow, but the control lesson is broader: filing failures often arise from weak document governance rather than legal interpretation. Firms with Irish launches or amendments should maintain a controlled template library, retire superseded versions and require a final form check immediately before submission.

The commercial opportunity will depend on implementation detail and operational usability, not the policy headline alone. Product manufacturers and distributors should test account eligibility, tax calculation, reporting, portability and consumer communications together. Early coordination can prevent a tax wrapper from being treated as a late-stage distribution overlay.



CSSF sharpens DORA major ICT–incident reporting expectations

WHAT’S CHANGING:

The CSSF published supplementary operational instructions for DORA major ICT-related incident reporting, alongside ESA guidance, to improve report quality, consistency and processing efficiency. Financial entities are expected to take the practical instructions into account.

ACTIONS REQUIRED:

- Compare internal incident procedures and reporting templates with the CSSF and ESA instructions.
- Test roles, escalation paths, data ownership and submission controls through a practical incident scenario.
- Brief ICT, operational resilience, risk and compliance teams on the updated supervisory expectations.

LBR Circular 26/02: compliance procedure for maintaining RCS and RBE data

WHAT’S CHANGING:

LBR has operated automated monitoring since January 2026 to identify missing, inaccurate or outdated RCS and RBE information. Circular LBR 26/02 confirms a progressive enforcement process from 21 September 2026. Following a registered notice, an entity has 30 days to regularise before escalating administrative measures and sanctions may apply.

ACTIONS REQUIRED:

- Review RCS and RBE data for all in-scope Luxembourg entities and managed structures.
- Reconcile beneficial ownership, registered office, governance appointments and outstanding statutory filings.
- Create an escalation workflow for notices, with named owners, evidence retention and board or governing-body visibility.

ONE PERSPECTIVE

This is a supervisory quality signal, not a new reporting regime. A technically correct incident classification can still produce supervisory friction if ownership, timestamps, impact data and narrative consistency break down under pressure. Scenario testing should therefore assess the full evidence chain from detection to approval and submission, including how later reports reconcile with the initial notice.

The key risk is not simply a late filing. Inconsistent register data can reveal weak entity governance, fragmented ownership of corporate records and poor change-management between administrators, boards and compliance. A controlled reconciliation should use one authoritative data set, document exceptions and ensure future changes trigger coordinated updates rather than periodic clean-ups.

# EXPERT INSIGHTS



● **FCA resilience exercise highlights systemic dependency risk**

**WHAT’S CHANGING:**

The FCA’s cross-sector exercise covered satellite disruption, damaged subsea cables and a cyberattack on a cable landing station. Firms were less confident about shared and international dependencies than about their own vulnerabilities. The FCA highlights communications networks, satellite systems, subsea cables, public databases and common technology providers.

**ACTIONS REQUIRED:**

- Extend service maps to common infrastructure and indirect dependencies.
- Assess geographic, provider and technology concentration across funds, delegates and key administrators.
- Use severe but plausible scenarios to test impact tolerances, communications and decision-making.

● **FCA publishes its first market-wide analysis of UK AIFs**

**WHAT’S CHANGING:**

FCA research based on regulatory reporting states that UK-managed AIF assets reached approximately £1.8 trillion in 2025, private credit is among the fastest-growing segments, and leverage and liquidity risks are concentrated in certain fund types. The paper establishes a baseline before proposed UK AIFM reforms and is not itself a rule.

**ACTIONS REQUIRED:**

- Use the findings in product, liquidity, leverage and private-credit risk discussions where relevant.
- Benchmark the quality and consistency of regulatory data used in governance reporting.
- Monitor the FCA’s proposals to modernise the UK AIFM regime.

## ONE PERSPECTIVE

Conventional outsourcing registers can understate systemic concentration because the same infrastructure sits beneath several apparently independent providers. Boards should challenge whether diversification is real, whether recovery assumptions depend on the same network and whether service-provider testing results are comparable to the fund’s own impact tolerances.

The strategic signal is concentration, not an assertion that the whole sector is fragile. Governing bodies should identify which portfolio, financing and redemption features place a fund closer to the risk pockets described by the FCA. Strong data governance matters because future policy and supervision will increasingly rely on reported information to distinguish firms.



● UK publishes Anti-Money Laundering and Asset Recovery Strategy 2026-2029

**WHAT'S CHANGING:**

The UK Government's three-year strategy sets direction for targeting priority risks, improving financial intelligence, strengthening supervision and asset recovery, and investing in capability. It is a policy programme rather than a new stand-alone firm obligation.

**ACTIONS REQUIRED:**

- Brief Compliance and MLRO functions on the strategic direction and monitor implementing consultations or rule changes.
- Check that financial-crime risk assessments cover emerging risks relevant to the business model.
- Maintain evidence that controls and governance adapt when threat or supervisory information changes.

● FCA money-mule review reinforces financial-crime expectations

**WHAT'S CHANGING:**

The FCA reports that more than 230,000 suspected mule accounts were offboarded in 2025 and that cash-out activity was concentrated between the second and fifth mule accounts. The review mainly targets banks, payment institutions and e-money firms, while offering broader typology and information-sharing lessons.

**ACTIONS REQUIRED:**

- Assess relevance to the firm's business model before changing controls.
- Where exposure exists, refresh risk scenarios, onboarding indicators, transaction-monitoring logic and escalation.
- Share relevant typologies with Compliance and MLRO functions, and document why controls are proportionate.

ONE PERSPECTIVE

Strategies matter because they shape supervisory attention and information requests before every element becomes a formal rule. The proportionate response is to map stated priorities to existing risks, controls and management information, identifying genuine gaps rather than launching a generic remediation programme.

For fund businesses, the value is in connected financial-crime intelligence rather than importing retail-banking controls wholesale. Consider subscriptions, redemptions, third-party payments and investor bank-account changes as part of an integrated investor-risk view, with targeted escalation where activity is inconsistent with the customer profile.



● [CPMI-IOSCO consults on cyber resilience and third-party risk for FMIs](#)

**WHAT’S CHANGING:**

CPMI and IOSCO published a voluntary, non-binding cyber resilience toolkit for financial market infrastructures and a related discussion paper on reliance on third-party providers. The toolkit covers governance, scenario design, response, resumption, recovery and testing.

**ACTIONS REQUIRED:**

- Monitor the consultation and final materials.
- Compare relevant practices with DORA-based resilience, testing and third-party oversight frameworks.
- For firms dependent on FMIs, consider how FMI and provider disruption enters service mapping and scenario testing.

GET IN TOUCH

Need help understanding how these regulatory changes could affect you? Our specialists can help you identify key considerations and prepare for the evolving requirements.



**James Gardner**  
UK Country Lead



**Faye McCrossan**  
Compliance & Regulatory Solutions Ireland



**Tobias Ettlin**  
Group Compliance & Regulatory Services Lead



For more information, click to email us:

ONE PERSPECTIVE

Although addressed to FMIs, the ecosystem lens is directly useful to funds and managers. Resilience cannot stop at the legal perimeter of a firm. Governance should identify upstream market infrastructure dependencies, understand fallback assumptions and test whether recovery priorities align across administrators, depositaries, managers and trading counterparties.

This material is provided for information purposes only and does not constitute legal, regulatory, tax, accounting, investment or other professional advice. Certain entities within ONE group solutions are regulated by the relevant competent authorities, including ONE Fund Management S.A., authorised and supervised by the CSSF as a UCITS Management Company and Alternative Investment Fund Manager (AIFM), ONE Corporate S.à r.l., authorised and supervised by the CSSF as a Professional of the Financial Sector (PSF), OGS Corporate Governance Limited, authorised in Ireland as a Trust or Company Service Provider (TCSP), and ONE group solutions London Limited, authorised to provide TCSP services in the United Kingdom. Services are provided through the relevant Group entity and are subject to applicable laws, regulations and regulatory approvals.