White Label Consultancy

DIFC Regulation 10 Compliance Roadmap

A Step-by-Step Roadmap to Achieving and Maintaining Compliance with DIFC Regulation 10

Prepared by White Label Consultancy

Introduction

This roadmap is designed for professionals responsible for preparing AI Systems for certification under DIFC Regulation 10. It is most relevant for Autonomous Systems Officers (ASOs), in-house legal/privacy teams, compliance managers, and product or risk owners tasked with aligning systems to the Accreditation & Certification Framework.

It sets out a phased journey with clear steps, suggested sequencing, and practical checkpoints. It does not replace legal advice or formal requirements from the Commissioner or an Accredited Conformity Assessment Body (ACAB). Instead, it provides structure and clarity for those leading the compliance effort.

Phase 1: Scope and Applicability

- ☐ List every "System" you plan to deploy, operate, provide, or make commercially available; confirm each meets the Framework's definition (autonomous or semi-autonomous, processes personal data, generates outputs).
    - Decide whether each System involves High Risk Processing (HRP). If yes, certification is required before commercial use.
- ☐ Nominate an executive sponsor and project lead for the certification workstream.
- ☐ If HRP applies, plan the ASO role and ensure there is no gap of more than one month before HRP operation or between ASO replacements.

> ***Tip:*** *Document the rationale for scoping decisions early, as these are often revisited during pre-assessment.*

Phase 2: Build the Governance Baseline

- ☐ Document an overarching AI governance policy addressing fairness, transparency, accountability, security, ethics, data quality, necessity, proportionality, and risk assessment principles.
- ☐ Complete an AI-focused DPIA / risk assessment; maintain a risk register and mitigation plan.
- ☐ Prepare transparency artefacts mapped to Regulation 10.2.2 (e.g., notices explaining human-defined purposes, limits, and evidentiary materials).
- ☐ Put in place mechanisms to trigger human intervention where outputs may be unfair or discriminatory; retain bias and impact assessments.
- ☐ Ensure compliance by design with the DIFC Data Protection Law and Regulations (lawful basis, authority requests, audit readiness).
- ☐ Define roles and responsibilities across the supply chain; make obligations explicit in contracts.

> ***Tip:*** *Keep the governance policy concise and evidence based. Overly complex documentation often slows down pre-assessment reviews.*

Phase 3: Security and Data Management

- ☐ Implement safeguards proportionate to the risks (training, technical/organisational controls, incident detection/response, physical security).
- ☐ Define secure data lifecycle controls, including disposal of personal data.

Phase 4: Accountability and Oversight

- ☐ Appoint an ASO with competencies comparable to a DPO; ensure independence and resources.
- ☐ Establish regular oversight of processing purposes, human-in-the-loop checks, and review cadence.
- ☐ Maintain training and feedback logs.

Phase 5: Complaints, Appeals, and Dispute Resolution

- ☐ Publish an accessible complaints process for data subjects regarding certified Systems; acknowledge and update within about one month.
- ☐ Maintain a complaints register; report trends/statistics as required.
- ☐ Document an appeals process (allowing appeals within 30 days) and, if used, identify the third-party dispute resolution provider.

Phase 6: Prepare the Certification Application Pack

- ☐ Use the official templates (Application for Certification, Confirmation Statements, etc.) from the Framework.
- ☐ Assemble evidence against the Systems Certification Program Requirements (CPRs).
- ☐ Consider an Article 20 prior consultation with the Commissioner for novel or complex use cases.

> ***Tip:*** *Start the evidence register early and keep it current. Linking requirements to specific artefacts helps avoid rework.*

Phase 7: Engage with the ACAB and Run Pre-Assessment

- ☐ Select an ACAB and agree the assessment plan.
- ☐ Undergo the ACAB's initial assessment; receive a gap report and register.
- ☐ Note: organisations have up to 12 months to remediate identified gaps without restarting the process.

Phase 8: Close Gaps and Obtain Certification

- ☐ Execute the remediation plan and submit evidence; the ACAB verifies completion.
- ☐ On approval, obtain the Certification Application Acceptance (CAA) Report — valid for three years per certified System.
- ☐ Display certification marks only while valid (not expired, revoked, or modified).

Phase 9: Operationalise Controls (Day-to-Day)

- ☐ Keep documentation current; test Systems against certification requirements regularly.
- ☐ Manage change control for architecture and processes.
- ☐ Maintain the ASO function continuously.
- ☐ Respect rules on certification marks and avoid unfair or misleading use.

Phase 10: Monitor, Report, and Audit (Years 1–3)

- ☐ Expect at least one audit during the 3-year validity; more may be scheduled based on risk.
- ☐ Notify the ACAB of any suspensions or revocations; the ACAB must inform the Commissioner within 30 days.
- ☐ Report substantial changes (e.g., organisation status, key personnel, resources, or System use/design changes) promptly to the ACAB.

Phase 11: Renewal and Continuous Improvement

- ☐ Begin re-certification planning 6–9 months before expiry.
- ☐ Close out all audit findings in advance of renewal.
- ☐ Track updates to the Framework and CPRs; adjust controls accordingly.

> ***Tip:*** *Treat the 3-year cycle as a continuous improvement, not a one-off project.*

At-a-Glance Mini-Checklist

- ☐ Confirm scope and HRP status
- ☐ Build governance baseline
- ☐ Establish security and lifecycle controls
- ☐ Appoint ASO and oversight mechanisms
- ☐ Publish complaints and appeals processes
- ☐ Assemble certification pack
- ☐ Engage with ACAB for pre-assessment
- ☐ Close gaps and obtain certification
- ☐ Operationalise day-to-day controls
- ☐ Monitor, report, and undergo audits
- ☐ Renew and continuously improve

Closing Note

This roadmap is intended as a structured guide to support compliance leads, legal teams, and ASOs in planning and executing Regulation 10 certification. It offers clarity on sequencing and expectations, while leaving room for organisations to adapt details to their own context.

For questions or tailored support, please contact:

White Label Consultancy

hello@whitelabelconsultancy.com

www.whitelabelconsultancy.com