White Label Consultancy

DIFC Regulation 10 Readiness Checklist

A practical guide to preparing evidence for certification under the DIFC Regulation 10 Accreditation & Certification Framework. Prepared by White Label Consultancy

Prepared by White Label Consultancy

Introduction

This checklist is designed for compliance leads, Autonomous Systems Officers (ASOs), IT directors, and in-house legal/privacy teams responsible for preparing AI Systems for certification under DIFC Regulation 10. It provides a structured way to assess readiness and ensure that the evidence required by Accredited Conformity Assessment Bodies (ACABs) is organised, complete, and auditable.

It is not intended as legal advice. Instead, it distils the key obligations into practical checkpoints to help organisations move from planning to documented compliance.

1) Scope & Applicability

- ☐ Confirm operations in/through the DIFC; verify that Systems process personal data and generate outputs.
- ☐ Classify each System for High-Risk Processing (HRP) and document rationale.
- ☐ Define roles clearly (Deployer, Operator, Provider) and assign responsibilities.

2) Governance & Accountability

- ☐ Approve an AI governance policy embedding fairness, transparency, accountability, security, data quality, necessity and proportionality, risk assessment and ethics.
- ☐ Complete an AI-DPIA (or AI-specific DPIA) to justify HRP, assess necessity/proportionality and record mitigations.
- ☐ Appoint an ASO; ensure competence, independence and resourcing; no gap longer than one month.
- ☐ Establish an operating model with owners, approvals, escalation, and role-based training.

3) Transparency & Data Subject Rights

- ☐ Provide a System-specific privacy notice covering purposes, limits, outputs, storage, third-party sharing, safeguards, and codes/certifications.
- ☐ Where rights are restricted, explain scope and impact in clear language; retain justification.
- ☐ If consent is used, ensure it is specific, granular, recorded, and easy to withdraw.
- ☐ Maintain a publicly accessible Autonomous Systems Register (unless exceptions apply) detailing use cases, lawful bases, decisions, roles, transfers, and safeguards.

4) Data Quality, Fairness & Security

- ☐ Enforce data minimisation and purpose limitation; define and apply retention.
- ☐ Validate dataset quality, relevance and currency pre-deployment; monitor post-deployment.
- ☐ Assess and document bias/fairness risks with metrics, remediation and re-testing.
- ☐ Develop a security threat model addressing AI-specific risks (poisoning, model extraction, prompt injection); implement and test controls.
- ☐ Operate monitoring for performance and drift; define retraining cadence, rollback, and feedback loops.

5) Third Parties & Procurement

- ☐ Conduct enhanced due diligence on Providers/Processors (security posture, certifications, adverse news).

- ☐ Include roles, audit rights, and AI-specific safeguards in contracts.
- ☐ Put in place and periodically review cross-border transfer safeguards (adequacy, SCCs, TIAs).
- ☐ Enforce human-defined purposes; maintain purpose logs, reviews and guardrails to prevent scope creep; test resilience.

6) Complaints & Dispute Resolution

- ☐ Publish a public, accessible complaints channel for System impacts; acknowledge and update within ~1 month.
- ☐ Maintain and review a complaints register; report trends to leadership.
- ☐ Document a dispute resolution mechanism (internal or contracted); prepare anonymised case notes/statistics where appropriate.

7) Communications with the Commissioner

- ☐ Establish a procedure to notify suspensions/revocations within 30 days, with reasons and corrective actions; define reinstatement workflow.
- ☐ Report substantial organisational/System changes (ownership, key personnel, resources, design/use) promptly.

8) Certification: Process & Evidence

- ☐ Engage with an ACAB; complete initial assessment; track remediation plan within the allowed window.
- ☐ Maintain a comprehensive evidence pack (policies, DPIAs, registers, tests, training, contracts, logs).
- ☐ Track certification term (3 years); schedule ≥1 periodic audit; perform annual attestation; trigger reviews upon material change.
- ☐ Use certification marks/seals correctly; avoid unfair or misleading claims.

9) Conflicts of Interest (where relevant)

- ☐ Where ACAB affiliation exists, implement independence safeguards; disclose and, if required, obtain Commissioner approval.
- ☐ Define and follow withdrawal/exception processes.

Closing Note

This checklist summarises the practical evidence expectations under DIFC Regulation 10. It is designed to help accountable officers, compliance leads and ASOs structure their certification preparation and maintain a state of readiness for assessment, audit, and renewal.

For tailored guidance on Reg 10 compliance, or support in closing gaps and assembling your evidence pack, please contact:

White Label Consultancy
hello@whitelabelconsultancy.com
www.whitelabelconsultancy.com