White Label Consultancy

DIFC Regulation 10 Documentation Requirements Guide

A comprehensive guide to preparing evidence for certification under the DIFC Regulation 10 Accreditation & Certification Framework.

Prepared by White Label Consultancy

Introduction

This guide is intended for compliance leads, Autonomous Systems Officers (ASOs), IT directors, and legal/privacy professionals tasked with preparing AI Systems for DIFC Regulation 10 certification.

It distils what an Accredited Conformity Assessment Body (ACAB) will typically ask for during the certification process. Certification is evidence-driven. The strength of your preparation lies in clear, objective, and well-documented artefacts.

This guide provides a structured overview of the documentation you will need, ensuring confidence and readiness at every stage of the certification lifecycle.

1) Company & System Profile

- Corporate details (registration, industry, authorised signatory).
- System description (function, data sources, outputs, intended use cases). Confirm whether the use case is High Risk under Regulation 10.
- Scope mapping: if using a non-standard certification scheme, provide a mapping to Regulation 10 requirements.

2) Lawful Basis, Necessity & Risk

- AI DPIA (necessity, proportionality, risks, mitigations, gap register, management plan).
- Risk Register (privacy, fairness, safety, security, explainability, misuse). Lawful basis documented; rights impacts and redress noted.
- Consider Prior Consultation with the Commissioner if high risks cannot be mitigated.

3) Transparency & Individual Rights

- System-specific privacy statement covering categories of data, purposes, sharing, retention, rights, and automated decision-making impacts.
- Autonomous Systems Register (public, unless an exception applies) covering use cases, lawful bases, decisions, limits, and transfers.
- Choice/consent artefacts: consent flows, logs, withdrawal processes.

4) Data Governance & Quality

- Data inventory and lineage (datasets, metadata, provenance).
- Quality controls (validation, deduplication, drift checks, refresh cycles).
- Privacy by design documentation (minimisation, pseudonymisation, retention schedules, access controls).

5) Fairness, Bias & Explainability

- Bias assessment plan and reports (metrics, test sets, results, remediation).
- Re-testing cadence and data quality checks tied to fairness.
- User-facing explanations: meaningful, accurate, and accessible explanations of how the system works.

6) Security & Resilience

- Security risk assessment (AI-specific threats such as poisoning, model extraction, prompt injection).
- Architecture and code controls (secure SDLC, reviews, change management, rollback plans).

- Monitoring and logging (performance, drift, retraining pipelines, access logs).
- Incident response and breach procedures aligned with recognised standards.

7) Human Oversight & Accountability

- ASO appointment letter, role description, reporting line, independence, and resources.
- No gap longer than one month before or between ASOs.
- Governance artefacts: policies defining roles, oversight forums, escalation paths, training logs.

8) Third Parties & Data Transfers

- Due diligence files (selection criteria, posture reviews, certifications). Contracts (controller–processor terms, audit rights, sub-processor approvals, AI safeguards).
- Cross-border transfer safeguards (adequacy, SCCs, TIAs).
- Operational safeguards (resilience, disposal, vulnerability/attack detection).

9) Complaints, Appeals & Dispute Resolution

- Public complaints procedure (channels, SLAs, templates, statistics reporting).
- Appeals process (independent review, timelines, tracking, cooperation with Commissioner).
- Dispute resolution mechanism (internal or contracted, confidential, anonymised notes and stats).

10) Certification Lifecycle Evidence

- Initial assessment pack (self-assessment forms, interviews, site reviews, gap report).
- Certification report (ACAB findings, remediation evidence).
- Ongoing monitoring (annual attestation, trigger-based reviews, verified complaints).
- Audit readiness: contemporaneous records, change logs, correct use of marks/seals.
- Regulatory communications (suspensions/revocations within 30 days, reinstatement steps, substantial change logs).

11) Templates & Formats

- Use official templates provided by the Commissioner (mandatory for certain submissions).
- Align evidence with the accepted structure to speed review and minimise ambiguity.

12) Submission Checklist (Quick Reference)

- ☐ Company & System profile
- ☐ AI DPIA + Risk Register
- ☐ Transparency pack (privacy notice, explanations, Autonomous Systems Register)
- ☐ Data governance set (inventory, quality, PETs)
- ☐ Bias & fairness assessments
- ☐ Security documentation (risk assessment, IR/Breach plan, logs)
- ☐ ASO appointment & governance artefacts

- ☐ Third-party pack (due diligence, contracts, cross-border safeguards) Complaints/appeals/dispute resolution procedures
- ☐ Lifecycle artefacts (gap report, remediation plan, annual attestations, Commissioner notifications)

> ***Pro Tip on Evidence Quality:***
>
> Keep artefacts objective, current, and auditable. Use version control, record approvals, and link every claim (e.g., "bias mitigated") to test results or change tickets. Where you deviate from the sample Certification Program Requirements, provide a clear mapping for the ACAB.

Closing Note

Preparing for DIFC Regulation 10 certification requires discipline, but it is achievable with the right documentation in place. This guide is designed to provide clarity on what evidence is required, helping compliance leads and ASOs maintain readiness and reduce risk of delay.

For tailored support in structuring documentation, closing evidence gaps, or preparing certification submissions, please contact:

White Label Consultancy

hello@whitelabelconsultancy.com

www.whitelabelconsultancy.com