cleartax

SECURITY & TRUST KIT

UAE E-INVOICING MANDATE · GO-LIVE JAN 2027

Vendor Discovery, Done Properly.

The 4 Proofs to Demand Before You Sign.

The evidence you must demand from every e-invoicing vendor — **before your invoice data becomes the government's source of truth.**



WHAT "VERIFIED" LOOKS LIKE — IN FOUR DOCUMENTS

DOC 01

The SER Walkthrough

Penetration-test evidence + a signed data-handling commitment.

DOC 02

Certifications & Audits

SOC 2, ISO 27001, encryption — on paper, not on a slide.

DOC 03

Data-Residency Note

Where data lives, where it fails over — proof it never leaves the UAE.

DOC 04

The SLA Sheet

Uptime, response & resolution — with contractual teeth.

WHY IT'S URGENT

Every slide says "enterprise-grade security." Almost none of them sign it.

The market has moved past feature comparisons. Every approved ASP claims the same scale, the same security, the same connectors. What actually separates vendors is no longer what they **claim** — it is what they can **evidence**, and what they will put in writing.

From 1 January 2027, your e-invoices flow through your ASP to the FTA in real time. That makes your ASP the custodian of your most sensitive commercial data: every customer, every price, every margin, every dispute.

THE RULE OF VENDOR DISCOVERY

If a security claim exists only in a demo or a slide, treat it as unverified. Every claim here maps to a document you can hold, an audit you can read, or an SLA you can enforce. Ask every vendor for all four — then ask for them signed.

Jan 2027

Real-time flow of every invoice to the FTA begins. Your ASP becomes your regulator-facing single source of truth.

THE REAL STAKE

A vendor security failure is not an IT incident. It is a business exposure event — visible to the regulator.

Why this favours specialists

For a global software giant, your security questionnaire is a ticket in a queue. For ClearTax, compliance is the entire company — so security evidence is not assembled on request; **it is the product.** Everything here is available today, in full, under NDA.

01 The SER Walkthrough

A Security Engagement Review is where claims meet evidence: an independent penetration test, plus a signed commitment on exactly how your data is handled.

DEMAND THIS EVIDENCE

- An **independent VAPT** on the platform, with a walkthrough of the latest report — what was found, and fixed.
- Testing that **recurs** — annual or better, plus after major releases — not a one-time accreditation exercise.
- A **signed data-handling commitment**: who can access your data, under what roles, with what logging, and how access is revoked.
- Access governed by **RBAC**, every API call token-authenticated — not blanket "admin access."
- Willingness to complete your questionnaire and **sit with your infosec team** — not a redirect to a generic trust page.

RED FLAG TO WATCH

A vendor who shares a certificate but refuses to walk through the underlying report. Certificates say testing happened. The walkthrough tells you whether they understood the findings.



THE CLEARTAX ANSWER

We run a structured SER with every enterprise prospect — a walkthrough of our latest independent VAPT report, our SOC 2 Type II findings, and our security architecture, **with your infosec team in the room.** Data access is governed by RBAC with granular permissions; every API call is token-authenticated; and we sign a data-handling commitment covering access, logging, retention and revocation — aligned with UAE PDPL privacy-by-design. Nothing is "available on request." It is available in the first meeting, under NDA.

02 Certifications & Independent Audits

Certifications are table stakes — but only if they are current, independently audited, and cover the actual production platform. Ask for scope and dates, **not logos.**

SOC 2 Type II

Security controls audited over time by an independent firm — not a point-in-time snapshot. The gold standard for operational security discipline.

ISO 27001:2022

Certified ISMS covering people, process and platform — on the current 2022 standard, not the retired 2013 one.

ISO 22301:2019

Business-continuity certification: proof that failover, recovery and continuity plans are documented, tested and audited.

Independent VAPT

Regular third-party penetration testing and hardening — with reports you can review, not a self-assessment.

AES-256 · SSL/TLS

Strong encryption at rest, and encrypted transmission for every invoice in motion — across every hop.

RBAC + Token APIs

Granular, role-based access, with an authenticated token on every API call. No shared credentials, no blanket admin.

THE CLEARTAX ANSWER

ClearTax holds all of the above — current and independently audited: SOC 2 Type II, ISO 27001:2022, ISO 22301:2019, recurring independent VAPT, AES-256 at rest, SSL in transit, RBAC and token-based API auth, with privacy controls aligned to UAE PDPL. **The same platform already carries these controls at scale, every day — not maintained for the audit.**

1B+
e-invoices annually

5,000+
enterprises

50+
countries

Check on any certificate: the scope (does it cover the e-invoicing platform you'll actually use?), the issue and expiry dates, and the auditing body. A logo without a scope statement is marketing, not assurance.

03 The Data-Residency Note

"Hosted in the UAE" can mean many things. The questions that matter: where is primary, where is failover — and does anything, including backups, **ever cross the border?**

🇦🇪 UAE JURISDICTION — SEALED

PRIMARY · OCI

Abu Dhabi

Oracle Cloud Infrastructure · production workloads · UAE soil

AUTO-SYNC

⇄

local ⇄ local

FAILOVER · AWS (me-central-1)

Dubai

Independent cloud vendor · 3 availability zones · auto-sync with primary

100%	<1 hr	<15 min	Zero
UAE data sovereignty, enforced at the infrastructure layer	Recovery Time Objective (same-region DR)	Recovery Point Objective	Cross-border data movement — production or backup

DEMAND THIS EVIDENCE

- ✓ Production **and** disaster-recovery both inside the UAE. A local primary with a foreign failover is not data residency.
- ✓ A **multi-cloud** architecture — so a single provider outage doesn't take your invoicing down with it.
- ✓ **Contractual RTO and RPO** — committed, not aspirational.
- ✓ Backups and replication that **stay in-country** — never quietly transiting foreign regions.

THE CLEARTAX ANSWER

100% UAE data sovereignty, enforced at the infrastructure layer. Our failover is **local-to-local — Abu Dhabi to Dubai** — across two independent cloud vendors, so a provider-level failure never becomes your compliance failure, and no production data or backup traffic ever leaves UAE jurisdiction. Delivered through a local UAE entity, aligned with UAE PDPL, and proven at scale: the same architecture processes **300M+ e-invoices annually** on OCI in KSA.

04 The SLA Sheet

An SLA without service credits is a wish. Ask every vendor to put numbers — and consequences — **on paper.**

99.9%
Contractual uptime, backed by service credits & independently verified

60 min
First response on critical issues — 24×7, in-house, not a call centre

4 hr
Critical fix / workaround, with a named owner and live tracker

AED 100 / invoice
accumulating for every hour a failure sits unresolved, under Cabinet Decision No. 106

COMMITMENT	THE NUMBER TO DEMAND	WHY IT MATTERS
Platform uptime	99.9%, contractual, backed by service credits & independently verified	Downtime means invoices don't move — and penalties compound daily under Cabinet Decision No. 106.
First response	Within 60 minutes for critical issues, 24×7, in-house	MLS gives your ASP a 10-minute response window on Peppol. A 5-day ticket queue is disqualifying.
Critical fix / workaround	Within 4 hours, with a named owner and a live observation tracker	Every hour a failure sits unresolved is AED 100 per invoice accumulating in the background.
Failed invoices	Auto-healing retries, deep validations, ASP-owned MLS resolution	Failures should be retried and resolved by the platform — not discovered by your team in a penalty notice.
Peak throughput	10,000 e-invoices/sec, 200–300 ms generation, proven at 100M+/month	Month-end and promo peaks are exactly when a weak platform fails — and when failure costs most.
Escalation	3-tier matrix agreed at kick-off — named CSM, leadership line, up to the CEO	The escalation path must exist before things go wrong — not be negotiated during the outage.

THE CLEARTAX ANSWER

Every row above is our standard commitment: a contractual 99.9% uptime SLA backed by service credits, 24×7 in-house support with a dedicated local CSM, a 3-tier escalation matrix agreed at implementation start, auto-healing retry logic with ASP-owned MLS resolution inside Peppol's 10-minute window — and, because e-invoicing is our entire business, a direct line to our CEO if you are ever unhappy. Ask any global platform to match that, in writing.

THE BOTTOM LINE FOR CFOs

Security and trust are not evaluated in a demo. They are evaluated in documents.

- A pen-test you can read
- Certifications with scope and dates
- A residency note with no asterisks
- An SLA with credits attached

ClearTax will hand you all four — signed. Ask every other vendor to do the same.

Talk to our Expert →

cleartax