



AI-FIRST AUDIT, RECOVERY & COMPLIANCE PLATFORM

Integra AuditIQ 360

DETECT · RECOVER · PROVE

A continuous audit platform for mid-market companies in India and the GCC. It scores every transaction for risk, runs 132 coded leakage, fraud and statutory checks over the whole population, drafts investigations with an AI agent that can only cite real records, and tracks every rupee and dirham recovered in one ledger — with an audit trail and evidence packs that verify.



India / UAE / KSA

GST · TDS · MSME · PINT AE · ZATCA ·
Transfer pricing · EN / AR RTL

AI Under Control

Grounded citations · PII redaction ·
governance gate · ISO 42001

Open & Self-Hosted

8 ERP connectors · CSV · MCP server ·
your region, your AI key

Integra IT Solutions FZE LLC

Integra IT Solutions — formerly Edocs Solutions & Computer Consultants — has spent two decades building ERP, WMS, EDMS, CRM and BPM platforms for organisations that live and die by the clock.

Headquartered in Sharjah, UAE, our systems run inside top-tier courier, logistics and trading enterprises across the GCC, India, Africa and Southeast Asia. We build purpose-built platforms — not generic software bent out of shape — and we own the compliance burden so our customers don't have to.

Integra AuditIQ 360 is the audit, recovery and compliance layer of the Integra platform suite. It reads from Integra Finance, Integra Ontrack ERP and eight third-party ERPs, and runs standalone on your own servers.

Company at a glance

ORIGIN

Sharjah Publishing City Free Zone, UAE

EXPERIENCE

20+ years · 100+ global clients

REACH

Live deployments across GCC, India, Africa & Southeast Asia

PRODUCT LINES

Courier ERP · Cargo & Logistics · Warehouse WMS · Integra Finance · Integra AuditIQ 360 · Integra AI · EDMS · CRM

DELIVERY

Self-hosted on your VPS or data centre · UAE / India data residency · 24/7 support

THE PRODUCT

What is Integra AuditIQ 360?

A continuous audit system that sits beside your ERP. It pulls AP, AR, GL, procurement, inventory, vendor and contract data, tests every record against coded leakage, fraud, journal-entry and statutory rules, explains the risk it finds, and carries each finding through investigation to cash recovered — with evidence an auditor can re-verify.



Detect

Duplicates, over- and under-billing, GL anomalies, three-way-match exceptions, inventory leakage, intercompany mismatches, contract breaches, 20 JE tests, 14 vendor fraud tests and sanctions — over the whole population, nightly.



Recover

An explainable 0–100 risk score, an AI investigation agent that can only cite real records, separation of duties on approval, and one recovery ledger from detected to cash confirmed that feeds ROI and gain-share.



Prove

115 sourced statutory rules for India, the UAE and KSA; an append-only, hash-chained audit trail; evidence packs with a SHA-256 manifest; board narratives in which every number drills to its query.

132

CODED CHECKS
LEAKAGE · FRAUD · JE ·
STATUTORY

69

SCREENS ACROSS
9 NAVIGATION GROUPS

7

EXECUTIVE KPI ENGINES
160+ KPIS

2

LANGUAGES
ENGLISH · ARABIC RTL

Benefits at a Glance

**Explainable, Not Black-Box**

Every risk score lists its factors and points; every rule its source, date and confidence; every KPI its formula.

**Whole Population, Nightly**

Detectors, JE tests, vendor fraud tests and statutory rules run over every record — not a sample once a year.

**Regional Rules Coded**

GST 2B / IMS / 37A / 16(4), TDS under both Acts, MSME 43B(h), UAE PINT AE and transfer pricing, KSA ZATCA.

**AI an Auditor Can Accept**

Citations must resolve to real records or are dropped. PII is redacted first. The starter of an investigation cannot approve it.

**One Number for Recovered**

One ledger — detected, validated, claimed, cash confirmed — read by dashboard, reports, narratives, ROI and gain-share.

**Evidence That Verifies**

Append-only hash-chained audit trail verified in one call; evidence packs with per-file SHA-256 and the chain head.

Major Features

- ✓ Browser-based, self-hosted; row-level tenant security
- ✓ 40+ finding types · explainable 0–100 risk score, tunable
- ✓ JE testing JE-01..20 (ISA 240), reproducible MUS sampling
- ✓ Vendor fraud tests VF-01..14 · daily sanctions (OFAC, UN, EU, UK)
- ✓ Contract leakage CL-01..07 with AI term extraction
- ✓ AI investigation agent, 7 read-only tools, full lineage
- ✓ Ask Analytics with cited SQL · rules-written board narratives
- ✓ One recovery ledger feeding ROI and gain-share
- ✓ India GST 16 rules · TDS & MSME 27 rules
- ✓ UAE PINT AE, VAT, transfer pricing TP-01..10 · KSA ZATCA
- ✓ Append-only hash-chained audit trail · SHA-256 evidence packs
- ✓ 7 executive KPI engines, 160+ KPIs · process mining PM-01..07
- ✓ AI governance gate, ISO 42001, DPDP · MCP server, 14 tools
- ✓ 8 ERP connectors, 26 CSV types · supplier portal · EN / AR RTL

Modules & pages



Also: Transfer Pricing · Audit Committee · ML Anomaly Detection · Forecasting · Process Mining · IC Reconciliation · Supplier Portal · Connectors · Data Import · Continuous Monitoring · Job Monitor · System Status · AI Governance · API Tokens & MCP · Report Branding · Users & Access

Detection Engine & Explainable Risk Score

Eight detection modules read your AP, AR, GL, procurement, inventory, intercompany, vendor and tax data and raise typed findings. A single de-duplicated findings list feeds triage, investigation and the recovery ledger.

Finding types by module

Module	What it raises
AP Leakage	Duplicate payment · rate variance · tax variance · quantity variance
AR Leakage	Underbilling against contract or price list
GL Anomalies	Off-hours posting · journal imbalance · round numbers · duplicate entry · threshold gaming · missing documentation
Procurement	Receipt missing · qty / unit-price / price variance · maverick spend · PO splitting · supplier consolidation
Inventory	Unusual write-off · phantom inventory · shrinkage · suspicious adjustment · slow-moving
Intercompany	Timing difference · missing counterpart · currency mismatch · amount variance
Vendor Validation	Missing tax id · high-risk high-spend · missing bank details · incomplete profile · duplicate vendor · sanctions confirmed
Tax	Wrong TDS section · VAT rate mismatch · tax-invoice particulars missing · PINT AE fields missing · salary without TDS · 40(a)(ia) disallowance

Contract leakage, CL-01..07

- **CL-01** PO unit price above the contract rate · **CL-02** dated outside the contract period · **CL-03** spend above the ceiling
- **CL-04** paid earlier than contract terms · **CL-05** material spend with no contract on file · **CL-06** renewal approaching without terms
- **CL-07** volume discounts and rebates — reported as not assessable until line items are available (roadmap)
- Terms are extracted from PDF contracts by AI with a verbatim quote per term, then confirmed by a person before use

Risk score 0-100 — the factors

Additive and capped · AP, AR, GL and vendors · weights tunable per organisation · versioned and rescored nightly

Open duplicate-payment finding	+35
Overbilling / underbilling finding	+30
Three-way-match exception · GL anomaly	+25
Sanctions / PEP match on vendor	+45
Look-alike vendor · vendor's own risky transactions	+35 / +30
Recent bank change · new vendor, high-value invoice	+20
Amount outlier (robust $z \geq 3.5$)	+20
Just under approval threshold · backdated ≥ 30 d · no document	+15
Weekend · after-hours · round amount · ML anomaly	+10 / +8 / +5 / +15

Vendor signals add at most 40 points to any one invoice. Each score is shown with its factor list and on a heatmap in Risk Explorer.

Payment prevention

Pre-payment checks and payment holds stop a confirmed duplicate, a sanctions match or a vendor with an unverified bank change before it is paid. A blocked payment is recorded as **prevented** in the recovery ledger — never counted as recovered.

Unified findings & triage

Cross-module de-duplication, suppression rules with reasons, a triage queue by severity and amount, precision tracking of confirmed vs dismissed, and an explainability page per finding.

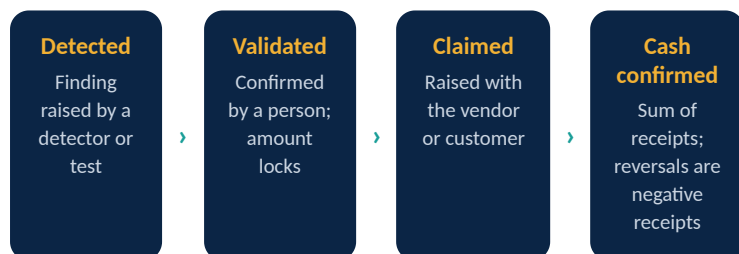
AI Investigations & the Recovery Ledger

The two capabilities finance teams ask for first — and the ones generic AI tools get wrong. In AuditIQ 360 the agent is grounded and governed, and "recovered" is one number everywhere.

Investigation agent

- ✓ **Seven read-only tools** — `get_finding`, `related_transactions`, `vendor_profile`, `matching_documents`, `contract_terms`, `prior_cases`, `risk_score`. The model can look, never write.
- ✓ **Grounded by construction** — every evidence reference must point to a record a tool actually returned; anything else is dropped before the draft is shown.
- ✓ **Bounded** — 8 steps, 20 tool calls, 60k tokens, 120 seconds per run. A live demo investigation finished in 10 seconds over 8 steps, cited its records, caught a contradiction in the data and left the recoverable amount blank rather than guess.
- ✓ **Private** — personal data is redacted before it reaches the provider, including inside tool results. Every prompt, tool call and output is stored as lineage.
- ✓ **Separation of duties** — the person who started an investigation cannot approve it. Approval creates a case and can open a recovery-ledger entry.
- ✓ **Degrades honestly** — with no AI provider configured it produces a "facts-only evidence bundle, not AI-generated".

Recovery lifecycle



Terminal states: **written off** and **prevented** (a blocked payment). Each stage's amount locks once the entry moves past it, every change is audited, and a finding can only be marked "recovered" once cash is confirmed. **ROI** = cash confirmed ÷ subscription cost, null when cost is unknown. **Gain-share** defaults to 10 % of cash confirmed by receipt date with an optional floor or cap; invoicing a period locks it.

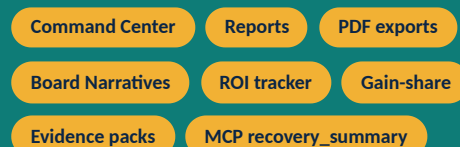
Board narratives with a why-tree

Narratives are written by rules, not by a model. Every number is a cited fact (F1, F2, ...) with a reproducing query; a fact that cannot reproduce to the cent is dropped and flagged. Approval freezes the narrative and drill-through shows whether it still matches live data. The why-tree splits any change exactly into volume and average-size effects.

What this means for you

- ✓ No more "AI said so" — every claim in an investigation points to a record you can open
- ✓ The dashboard, the board deck, the ROI figure and the gain-share invoice show the same recovered number
- ✓ Prevented and recovered are never mixed
- ✓ Auditors see who started, who approved and what the model was shown
- ✓ Your ledger never trains anyone's model; prompts are not retained in the usage log
- ✓ Works with Gemini, Claude, OpenAI or any OpenAI-compatible endpoint — your key

EVERYTHING THAT READS THE LEDGER



SUPPLIER PORTAL

Suppliers sign in on their own login to answer disputes and confirm or dispute statements. Bank-detail changes are deliberately not offered there.

Journal-Entry Testing, Vendor Fraud & Tamper-Evident Trail

Journal-entry testing JE-01..20

ISA 240 • AS 2401

Tests	Coverage
JE-01 • 02 • 03	Unbalanced journals • number-sequence gaps • duplicate entries
JE-04 • 05	Benford first digit and first-two digits — Nigrini MAD bands, per-digit z-scores; run only with ≥ 300 / 1,000 amounts
JE-06 • 07	Round amounts • just below the approval limit
JE-08 • 09 • 10	Weekend • holiday • after-hours postings
JE-11 • 12 • 13	Period-end entries • backdated / late • high-value manual
JE-14 • 15 • 16	Infrequent posters • descriptions ("plug", "override") • missing support
JE-17 • 18 • 19	Reversals • suspense / clearing accounts • seldom-used accounts
JE-20	Segregation of duties — poster equals approver

Every test reports passed / exceptions / not assessable / not suitable. Parameters freeze with each run. Sampling is reproducible: risk-based, monetary-unit (MUS) or seeded random. Up to 250,000 entries per run; exceptions export to CSV.

Controls frameworks

SOX / ICFR with a COSO 2013 key-control set, SOC 2, ISO 27001:2022 Annex A, ISA 240 and SAS 99 libraries as neutral templates, linked to live findings through control signals. No pre-filled results — ever.

Vendor fraud tests VF-01..14

- **VF-01** shared bank account • **VF-02** vendor bank equals an employee's • **VF-03** shared tax id • **VF-04** vendor contact matches an employee
- **VF-05** master changes out of hours or without SoD • **VF-06** payment soon after a bank-detail change • **VF-07** new vendor, large early payments
- **VF-08** dormant vendor reactivated • **VF-09** sequential invoice numbers • **VF-10** high share of round amounts • **VF-11** split invoices below a limit
- **VF-12** payee with spend but no master data • **VF-13** free-mail or PO-box contacts • **VF-14** screening coverage

Sanctions & watchlists

OFAC SDN and Consolidated, UN Security Council, EU and UK lists — about 33,600 entries at first load — refreshed daily with source, hash and fetch time, plus a custom watchlist per tenant. Matches are tiered (id / strong / potential / weak) and need a human decision; false positives are remembered; a confirmed match can place a payment hold. The platform never says "clear" on stale lists.

Vendor bank-account protection

Bank accounts and tax ids are stored encrypted, displayed as the last four digits and matched through a keyed blind index. Every change is recorded masked, and a change followed by a payment raises VF-06.

Append-only audit trail

A database trigger rejects updates. Per-organisation sequence numbers and a hash chain; one call verifies the whole chain. A before / after edit log on AP invoices, vendors, GL and payments covers Companies (Accounts) Rules 3(1).

Verifiable evidence packs

One ZIP per compliance, SOX or finding pack: JSON / CSV records, a PDF summary, a manifest with per-file SHA-256, the audit-chain head and cited rule versions. A verify endpoint re-checks any pack later; the summary PDF is byte-reproducible.

Process mining PM-01..07

Procure-to-pay map with variants, transitions and p95 cycle-time outliers: invoice with no PO, retrospective PO, PO approved after invoice, invoiced before receipt, paid before approval or invoice date, same approver on PO and invoice.

India, UAE & KSA Compliance — Coded, Sourced, Labelled

115 statutory and audit rules live in a registry: **20 verified** against primary sources, **52 secondary** and **43 indicative**. An indicative rule can only raise an advisory — it never hard-fails. Every rule shows its source and the date it was checked.

India GST & e-Invoice • 16 rules

- GSTR-2B vs books reconciliation from the portal JSON
- IMS assistant: accept / reject / pending with ITC impact
- Rule 37A — supplier 3B not filed by 30 Sep → reverse by 30 Nov
- Sec 16(4) time-bar with 60 / 30 / 7-day warnings, GSTR-9 aware
- GST 2.0 rate set and Sec 14 transition • GSTR-3B lock / 1A
- e-Invoice applicability by AATO • IRN 30-day limit • IRN, QR and GSTIN integrity

India TDS & MSME • 27 rules

- Effective-dated: Income-tax Act 1961 to 31 Mar 2026, then the Income-tax Act 2025 (Secs 392 – 398)
- Sections 192, 193, 194, 194A, 194C, 194H, 194-I, 194IA / IB / IC, 194J, 194Q, 194R, 194T, 195
- Thresholds, rate by PAN type, no-PAN 20 %, inoperative PAN, deposit by the 7th, interest 1 % / 1.5 % a month
- 40(a)(ia) disallowance and cash-exposure view
- MSME 15 / 45-day limit, 43B(h) / 37(2)(g), Sec 16 interest at 3× bank rate

UAE • 15 rules + transfer pricing

- PINT AE — 51 mandatory fields, 14-day issue window, arithmetic checks
- VAT 5 %, Art. 59 invoice particulars, TRN format, reverse charge, exempt supplies, VAT-return reconciliation to books
- Corporate Tax readiness estimate (not a tax computation)
- Transfer pricing TP-01..10: related-party totals vs AED 40m / 4m / 500k, Master File / Local File triggers (AED 200m / 3.15bn), zero-interest loans, unreconciled intercompany, benchmark ranges you supply

KSA ZATCA Phase 2 • 16 rules

- UBL 2.1 structure, UUID, gapless invoice counter (ICV)
- Previous-invoice-hash (PIH) chain and hash integrity
- QR TLV tags 1–9; ECDSA stamp when the certificate is present
- Clearance vs reporting flows, VAT 15 %
- Wave 25 readiness (> SAR 187,500 by 1 Feb 2027) • Oman information only

Regulatory timeline we are built for

30 Sep → 30 Nov

Rule 37A: ITC on invoices whose supplier has not filed GSTR-3B must be reversed by 30 November.

1 Apr 2026

Income-tax Act 2025 in force. TDS rules switch by effective date; both Acts stay available for prior periods.

1 Jan 2027

UAE e-invoicing mandatory for businesses ≥ AED 50m; government entities from 1 Oct 2027.

1 Feb / 1 Jul 2027

KSA ZATCA Wave 25 (> SAR 187,500) • UAE e-invoicing for all remaining businesses.

115

STATUTORY & AUDIT RULES
IN THE REGISTRY

43

INDIA RULES
GST • TDS • MSME

31

UAE & KSA RULES
+ 10 TRANSFER PRICING

33,600+

SANCTIONS ENTRIES
5 PUBLIC LISTS, DAILY

Transfer-pricing thresholds and some secondary-source rules are labelled indicative and should be confirmed with your tax adviser; AuditIQ 360 is a compliance aid, not tax advice. DPDP and ISO 42001 features are self-assessment and record-keeping aids, not certification.

Executive KPIs, Governed AI & an Open, Self-Hosted Platform

Seven executive modules, 160+ deterministic KPIs

Module	Measures
Finance (CFO)	Profitability, liquidity, DSO / DPO / DIO, cash-conversion cycle, leverage, cash flow, ageing, budget variance, TB and balance-sheet integrity
Inventory (COO)	Turnover, ABC, slow and dead stock, cycle-count accuracy, supplier on-time, purchase-price variance
Job Costing	Overrun, margin, labour variance, WIP over / under-billing, estimate at completion
Projects (PMO)	Earned value — PV, EV, AC, SPI, CPI, EAC, TCPI — milestones, utilisation, risk exposure
HR Analytics	Headcount, attrition, tenure, payroll, absenteeism, hiring, training; auditor-only access
Fixed Assets	NBV, recomputed vs booked depreciation, under-insurance, ghost-asset signals
Fleet	Utilisation, fuel efficiency and anomalies, cost per km, total cost of ownership

The platform computes every KPI; the AI only interprets. Missing inputs give **not computable** with the fields named — never 0 or an estimate. Each KPI carries its formula, inputs and benchmark basis.

Ask Analytics — questions with cited SQL

Plain-language questions over an allow-listed catalogue. Each query is parsed — single SELECT, no writes, forced row limit, 5-second cap — and runs read-only as a role that cannot bypass tenant isolation. The answer shows the SQL, tables and row count. On the demo tenant, "total amount at risk from duplicate payments" returned 2,434,208.44 across 26 findings in about 1.5 s.

Integrations

- ✓ **8 read-only ERP connectors** — Tally Prime / ERP 9, Zoho Books, SAP Business One, SAP S/4HANA, Dynamics 365 Business Central, Odoo 14-18, ERPNext, NetSuite — idempotent sync, watermarks, dry runs, schedules
- ✓ **26 CSV document types** plus GSTR-2B JSON, e-invoice CSV, ZATCA XML, VAT returns, TDS files, contract PDFs and watchlists — validated into a draft before publish
- ✓ **MCP server** — 14 read-only tools for Claude Desktop, Claude Code and other MCP clients; scoped tokens, every call audited, off by default

AI governance console

- ✓ Server-side gate before every model call across 6 use cases — fails closed
- ✓ No External AI Mode · data residency by region
- ✓ Provider allowlist by name, daily caps, token limits
- ✓ Model registry: risk tier, owner, human oversight, review dates
- ✓ Usage log keeps metadata only — never prompts
- ✓ ISO / IEC 42001 self-assessment: 24 controls, Annex A.2 – A.10, evidence computed from the platform
- ✓ DPDP registers: data categories, rights requests (90-day due), notices, retention
- ✓ Bring your own key: Google, Anthropic, OpenAI, Groq, Mistral, Kimi, MiMo or any OpenAI-compatible endpoint

Security & platform

RUNTIME

FastAPI · PostgreSQL 16 · Redis · Celery · React 19

ISOLATION

Row-level security on every tenant table; owner / app / read-only database roles

AUTHENTICATION

Short-lived typed tokens, httpOnly cookies + CSRF, logout, per-IP limits, SSRF guard

ENCRYPTION

Field-level for bank accounts, tax ids and all integration secrets; HTTPS, HSTS, CSP

OPERATIONS

Nightly + pre-change backups, restore drill passed, 2-minute watchdog, external uptime check

QUALITY & LANGUAGES

2,100+ backend, 500+ UI and E2E tests · English · Arabic RTL · Hijri option

See it find money in your own ledger.

Bring twelve months of AP invoices, your vendor master and a GL export — we run the detectors, JE tests and vendor screens live.

sales@integraontrack.com

+971 55 222 0975 ·
audit.integraerp.tech