VALIDERE

Environmental Compliance Software Evaluation Kit

Requirements worksheet, vendor demo brief, POC test plan, and scoring matrix. From the Validere guide: How to Choose Environmental Compliance Software.

1. Define your compliance scope

Check all that apply. Use this to build your requirements map before scheduling demos.

- [ ] EPA GHGRP / Subpart W reporting
- [ ] Methane monitoring and reconciliation
- [ ] Water / wastewater compliance
- [ ] Multi-facility / multi-jurisdiction operations
- [ ] State or provincial air reporting
- [ ] Permit-driven monitoring and recordkeeping
- [ ] Waste and hazardous materials tracking
- [ ] Field-to-office data collection workflows

2. Requirements mapping worksheet

Document one priority workflow using the chain: Requirement → Facility → Activity → Owner → Source data → Calculation → Review → Submission → Evidence.

Priority requirement or reporting program

______

Facilities and assets in scope

______

Required activities (monitoring, sampling, inspections, calculations)

______

Source systems and data owners

SCADA, historians, ERP, lab, field, spreadsheets

______

Review, approval, and evidence requirements

______

3. Vendor demo brief — send 48–72 hours before the demo

Do not accept a generic product tour. Send vendors this brief and ask them to demonstrate your scenario.

Demo brief checklist
Include one real requirement, one source system, one exception, one reporting output, and one evidence requirement.

One requirement

Example: Subpart W source category calculation, permit monitoring obligation, or recurring air report.

Your requirement: ____

One source system

Example: Production accounting export, historian tag set, lab results file, or field inspection record.

Your source system: ____

One exception

Example: Missing record, late data, duplicate entry, out-of-range value, or methodology change.

Your exception: ____

One reporting output

Example: GHGRP submission-ready output, state air report, or internal compliance summary.

Your reporting output: ____

One evidence requirement

Example: Supporting lab report, inspection photo, calculation worksheet, or approval record.

Your evidence requirement: ____

4. Demo script — run this with every vendor

Step 1: Trace a reported value backward

Start from a value in a completed report. Can the vendor reach source data, methodology, factors, and approvals?

Notes: ____

Step 2: Handle missing or late data

Show detection, assignment, escalation, and resolution — not manual work outside the system.

Notes: ____

Step 3: Modify a calculation methodology

Show versioning, impact on current and historical results, and who can approve the change.

Notes: ____

Step 4: Route review and approval

Use your actual roles. Show return-for-correction, not email-only approvals.

Notes: ____

Step 5: Make a configuration change live

Add a facility, threshold, or workflow step. Note who performs it and whether services are required.

Notes: ____

5. Proof-of-concept workflow test

Run one bounded POC using realistic data. Score whether the platform preserves context through every stage.

POC stage	What to test	Pass?	Notes
Source systems	Multiple real data inputs — not one prepared spreadsheet		
Validation	Missing, duplicate, or malformed records identified		
Calculation	Methodology applied and inspectable by authorized users		
Exception handling	Investigation routed, documented, and resolved in-system		
Review & approval	Actual roles complete their steps without parallel email process		
Reporting	Output the team genuinely uses — produced from governed data		
Evidence	Supporting documents attached and retrievable in context		
Correction	Approved value changed; history and lineage preserved		

6. Capability scoring matrix

Score each vendor 1–5 (1 = poor fit, 5 = strong fit). Weight categories based on your environment.

Evaluation area	What to assess	Score	Notes
Regulatory & workflow fit	Support for actual requirements, jurisdictions, and processes		
Data integration	Connect, validate, monitor, and trace required source data		
Compliance tracking	Ownership, deadlines, activities, evidence, approvals, history		
Calculation transparency	Methods, factors, assumptions, versions, and changes visible		
Reporting workflows	Preparation, review, output, corrections, traceability		
Exception handling	Detection, routing, investigation, escalation, closure		
Auditability & lineage	Trace outputs through calculations, sources, evidence, approvals		
Usability & adoption	Field, facility, and corporate users can complete their work		
Security & governance	Access, permissions, authentication, retention, data residency		
Configurability	Adapt to new facilities, requirements, workflows, and methods		
Implementation readiness	Migration, integration, configuration, testing, training, rollout		
Total cost of ownership	Licensing, services, internal admin, maintenance, expansion		

VENDOR COMPARISON SUMMARY

Vendor	Total score (/60)	Top strength	Top concern	Ownership model

7. Red flags — check any you observed

- [ ] Demo used only sanitized sample data
- [ ] Cannot trace a reported value to source data and methodology

- [ ] Compliance tracking disconnected from underlying data and evidence
- [ ] Calculations explained only by vendor technical staff or consultants
- [ ] Exceptions handled outside the platform (email, spreadsheets)
- [ ] Every configuration change requires a paid services engagement
- [ ] Auditability demonstrated as a user activity log only
- [ ] AI shown as a chatbot without governed access to environmental data or workflows

---