

10 Steps to Clean, Control, and Classify ERP Data **Before AI**

A print-ready guide for governments and schools that want ERP data clean enough, controlled enough, and clear enough for trusted AI use.

Clean ERP Data

Internal Controls

Classification

Root Cause

AI Readiness

ERP AI Readiness Snapshot

Controls-First

Vendor master quality

62%

Chart of accounts classification

71%

Permissions mapped for AI

48%

Exception remediation evidence

58%

//

AI is only as strong as the data and systems supporting it.

MGO, AI adoption risks for state and local government

//

Successful AI depends on clear process understanding and clean, structured data.

UHY, AI + Data Governance for State & Local Government

//

Controls-first delivery embeds accountability into automation.

Internal control principle applied to ERP AI readiness

WHY THIS GUIDE EXISTS

AI does not fix weak controls. It scales them.

If ERP data is duplicated, misclassified, over-permissioned, or unsupported, AI can turn those issues into fast, confident, hard-to-defend answers.

- ✓ Duplicate vendors become distorted spend answers.
- ✓ Misclassified accounts weaken budget and ACFR narratives.
- ✓ Stale permissions become AI visibility risk.
- ✓ Unresolved exceptions become audit friction.

THE PRACTICAL STARTING POINT

Before you ask AI for answers, make sure your ERP data can tell the truth.

Government and school finance teams already have the data AI needs: budgets, actuals, vendors, invoices, purchase orders, contracts, grants, projects, chart of accounts, payroll, policies, reports, roles, and permissions.

The issue is not whether the data exists. The issue is whether the data is clean enough, classified enough, controlled enough, and documented enough for AI to use safely.

This guide turns AI readiness into a controls-first operating model: identify the process, clean and classify the data, define preventive and detective controls, document corrective actions, and only then apply AI on top of a controlled ERP layer.

Getting your ERP ready for AI requires an understanding of internal controls.

AI readiness is not just a data-quality project. It is an internal control project. Internal controls define what should happen, how the organization detects what actually happened, and how issues are corrected so the same problem does not keep feeding bad data into AI.



Preventive controls

Preventive controls are designed to stop bad data, unauthorized access, or noncompliant activity before it enters the AI-ready ERP layer.

- Required fields and valid account combinations
- Vendor setup rules and duplicate checks
- Approval workflows and spending thresholds
- Role-based access and segregation of duties
- Sensitive data tags before AI exposure



Detective controls

Detective controls find issues that slipped through or emerged after the fact. This is where AI readiness begins to become visible.

- Duplicate invoice and vendor tests
- Budget variance and miscoding analytics
- Policy exception flags and risk scores
- Access changes and permission drift
- Monitoring queues for review and escalation

3

Corrective controls

Corrective controls close the loop. They document what happened, find the root cause, remediate it, and improve the process.

- Reviewer disposition and evidence trail
- Root-cause classification
- ERP cleanup or staging-layer correction
- Policy, training, or workflow update
- Follow-up monitoring to confirm the fix worked

The ERP-to-AI control loop

The first job is not to automate the answer. The first job is to detect the issue. Once detected, the organization must understand the root cause, remediate the underlying problem, and update the control so AI does not keep learning from or repeating bad ERP patterns.

Detect

Analytics, flags, risk scores, access alerts, and variance tests identify the issue.

Diagnose

Finance, IT, or audit determines why the issue occurred.

Remediate

Correct the data, permission, policy, workflow, vendor record, or accounting code.

Prevent

Update rules, approvals, required fields, training, or validation logic.

Monitor

Confirm the fix holds and use the improved data layer for AI.

What the ERP control layer looks like in practice.

ThirdLine helps teams configure analytics, link policies, monitor exceptions, assign risk, document decisions, and publish views before AI relies on the data.

Analytics library

Configure checks for AP, vendor, p-card, control, fraud, and training patterns.

DETECT

Name	Weight	Flags	Description
Holiday Invoices	10	10	Flags invoices entered on observed holidays. (5 holidays configured). Invoice date entry on holidays is unusual and may indicate fraudulent activity, unauthorized access or data entry errors.
First invoice from vendor after an address change	10	10	Identifies the first invoice received from each vendor name after their address was changed in the system. This helps detect potential fraud schemes where vendor addresses are modified to redirect payments.
First invoice from vendor after vendor payment method change	10	10	Identifies the first invoice received from each vendor name after their payment method was changed. This helps detect potential fraud involving payment method modifications that could redirect funds.
Holiday Payments	10	10	Flags check payments issued on observed holidays (5 holidays configured). Payments processed on holidays are unusual and may indicate fraudulent activity or system configuration issues.
Round Amounts	10	10	Flags invoices with round invoice amounts (no cents). Round amounts are sometimes associated with fraudulent invoices estimated amounts or improper expense submissions.
Invoices With No PO	10	10	Flags invoices that have an empty or missing PO number. This indicates a potential bypass of purchasing controls and proper procurement authorization.
Invoices Ending In 99	10	10	Flags invoices where the invoice amount ends in .99. This pricing pattern is sometimes used to circumvent approval thresholds or may indicate consumer-

Living policy layer

Upload policies, extract rules, and link those rules to analytics.

PREVENT

Policy Name	Policy Description
Spending Approvals	Default P-Card limits are \$5,000 per purchase and \$10,000 per month, requiring Fiscal Officer approval. Cards will be set up with \$5,000 per purchase and \$10,000 per month limits with approval from the Cardholder's Fiscal Officer.
P-Card	Split Transactions By Cardholder Same Day
Monthly Spend Outliers	Identifies months where total spending is significantly above average, specifically 10% or more standard deviations above the mean monthly spend across all months in the dataset.
Flag Split Transactions By Cardholder	Identifies potential split transactions by finding multiple purchases from the same cardholder at the same vendor name, on the same date, that together exceed the P-Card limit.
Spending Approvals	Cardholders must submit a Higher Transaction or Monthly Limit Request Form to exceed default spending limits. Higher limits may be requested by completing a Higher Transaction or Monthly Limit Request Form.

Monitoring queue

Review flagged transactions, risk scores, exceptions, and dispositions.

CORRECT

TYPE	Control Failures	High Risk	REVIEW STATUS	AI	Open	Ignored	Resolved
1 CONTROL FAILURE	Municipal Electric Ltd	Amount: \$10,555	Entered By: Richard	Invoice Entry Date: May 1, 2024	Invoice #: 424535	PO #: 18465701	INVOICE DESCRIPTION: QUARTERLY LANDSCAPING MAINTENANCE
1 CONTROL FAILURE	Atlantic Systems International	Amount: \$10,555	Entered By: Linda	Invoice Entry Date: Apr 22, 2024	Invoice #: 713922	PO #: 90169789	INVOICE DESCRIPTION: HAZARDOUS WASTE DISPOSAL

Dashboards and reports

Translate clean, classified ERP data into views leadership and auditors can understand.

CLARIFY

AP Risk	View	Export	Download Template	Filter	Share
Owner: ThirdLine Demo	Dashboard	Exports	Samples	Invoice Status	
29,966	\$ Avg Invoice Amount	\$50,281	Total Invoice Amount	\$1.51B	Average Risk Score
					0.3
Risk Over Time by Fund					

How to move from ERP complexity to AI-ready clarity.

Use these steps in sequence. The goal is not to make the ERP perfect. The goal is to create a controlled staging layer that makes ERP data safe enough and useful enough for AI.

1

Inventory systems, reports, owners, and control responsibilities.

CURRENT STATE

List the ERP modules, finance reports, policy documents, data owners, workflows, integrations, APIs, user groups, and downstream reporting obligations that AI may eventually touch.

Action

Create one inventory across finance, IT, audit, procurement, payroll, grants, and management reporting.

Control question

Who owns the data, who approves changes, and who is accountable when the output is wrong?

AI clarity

AI use cases start with known data owners, known systems, and known risk areas.

2

Map the process and identify control points.

PROCESS

Before cleaning data, understand how transactions, approvals, exceptions, reports, and corrections actually move through the organization.

Action

Map where data is created, reviewed, approved, changed, exported, reported, and archived.

Control question

Where should preventive, detective, and corrective controls exist?

AI clarity

AI can follow the process instead of summarizing disconnected fragments.

Assess ERP data quality before it becomes an AI quality problem.

DATA READINESS

Score what is complete, incomplete, duplicated, stale, inconsistent, misclassified, unmapped, or unsupported.

Action

Run checks for duplicate vendors, invalid account combinations, stale users, missing fields, miscoded activity, and unmapped reports.

Control question

Which issues are data-entry problems, process problems, training problems, or permission problems?

AI clarity

AI can distinguish clean records from records that need human review.

Analytics ThirdLine Der.

ThirdLine

Search Name Accounts Payable Fraud

Name	Weight	Flags	Description
Holiday Invoices Invoices Q Fraud	Off	0	Flags invoices entered on observed holidays 5 holidays configured . Invoice data entry on holidays is unusual and may indicate fraudulent activity unauthorized access or data entry errors.
First invoice from vendor after an address change Invoices Q Fraud	Off	5	Identifies the first invoice received from each Vendor Name after their address was changed in the system. This helps detect potential fraud schemes where vendor addresses are modified to redirect payments.
First invoice from vendor after vendor payment method change Invoices Q Fraud	Off	5	Identifies the first invoice received from each Vendor Name after their payment method was changed. This helps detect potential fraud involving payment method modifications that could redirect funds.
Holiday Payments Invoices Q Fraud	Off	17	Flags check payments issued on observed holidays 5 holidays configured . Payments processed on holidays are unusual and may indicate fraudulent activity or system configuration issues.
Round Amounts Invoices Q Fraud	Off	20	Flags invoices with round Invoice Amount s (no cents). Round amounts are sometimes associated with fraudulent invoices estimated amounts or improper expense submissions.
Invoices With No PO Invoices Control Q Fraud Training	Off	20	Flags invoices that have an empty or missing PO Number . This indicates a potential bypass of purchasing controls and proper procurement authorization.
Invoices Ending In .99 Invoices Q Fraud	Off	20	Flags invoices where the Invoice Amount ends in .99. This pricing pattern is sometimes used to circumvent approval thresholds or may indicate consumer-

25 Per Page « < 1 > » Showing 1 to 24 of 24

Software example: Configurable analytics provide a controlled way to detect ERP issues before AI-facing use cases are enabled.

4

Classify the data into a government ERP taxonomy.

CLASSIFICATION

Define the categories that turn ERP codes into plain-English structure: function, department, fund, object, program, project, grant, vendor family, report type, sensitivity level, and retention period.

Action

Create standard tags for owner, source, sensitivity, retention, report use, and AI visibility.

Control question

What does this record mean, who can see it, and which reports or decisions rely on it?

AI clarity

AI answers from the government's classification structure, not raw codes alone.

5

Clean and group master data where it matters most.

CLEAN-UP

Group duplicate vendors, normalize account mappings, connect contracts to spend, identify stale users, and classify vendor and transaction types.

Action

Clean the staged data first; export corrections back to the ERP when appropriate.

Control question

Was the root cause bad setup, bad process, missing ownership, or lack of validation?

AI clarity

AI sees the prepared version of the truth without waiting for a perfect ERP cleanup project.

6

Map permissions and sensitive data before AI sees the data.

ACCESS

Define what each role should be allowed to see, summarize, export, or act upon. AI makes permission problems visible because users can ask broader questions faster.

Action

Map access by user, role, department, fund, account, vendor, payroll field, and report category.

Control question

Would this user be allowed to see the same data in the ERP or source report?

AI clarity

AI boundaries align with ERP permissions, least privilege, and sensitive data rules.

Turn policies into living controls.

POLICY TO ANALYTICS

Policies should not live only in PDFs or binders. Connect policy rules to analytics, thresholds, exception flags, review queues, and evidence requirements.

Action

Link procurement thresholds, approval limits, travel rules, grant restrictions, close procedures, and audit requirements to testable controls.

Control question

Which policy rule is being tested, what evidence proves it, and what action is required?

AI clarity

Every flag has a reason, every answer has policy context, and every exception can be explained.

The screenshot displays the ThirdLine Policies interface. On the left is a navigation menu with options: Views & Samples, Analytics, Monitoring, Vendors, Employees, Workflow, Policies (selected), Upload, and Exports. The main content area is titled 'Policies' and shows a list of policy rules under the 'Purchasing' category (45 rules). The rules are organized into sections: 'Spending Approvals', 'PCard', and 'Split Transactions By Cardholder Same Day'. Each rule has a status indicator (e.g., 95%, 80%, 80%) and a description. The 'Spending Approvals' section includes a note about default P-Card limits. The 'PCard' section includes a note about split transactions. The 'Split Transactions By Cardholder Same Day' section includes a note about identifying potential split transactions. The interface also features a search bar for analytics to link and a button for 'Auto Link Analytics (9 unlinked)'.

Software example: Policy rules can be extracted, linked to analytics, and used as evidence for how controls are applied.

Detect issues and assign risk scores.

DETECTIVE

Not every exception deserves the same level of review. Weight exceptions using amount, sensitivity, timing, missing support, repeated behavior, policy conflict, permission risk, and audit relevance.

Action

Use analytics and risk scores to create daily or weekly worklists for finance, procurement, IT, or audit.

Control question

What did the detective control find, and is the issue isolated or part of a pattern?

AI clarity

AI can prioritize what requires human review instead of treating every data point as equally reliable.

The screenshot displays a monitoring dashboard for 'Accounts Payable'. On the left, a sidebar shows 'Invoices' with a 'Dataset' icon and a 'DATE RANGE' filter set to 'Feb 4 - May 30'. Below this, 'CONTROL FAILURES' are listed: 98 unresolved transactions. The main area shows a 'MONITORING REVIEW' section with 'Ignore' and 'Resolve' buttons. A table lists check details: Check Amount (\$13,197.19), Check Clear Date (05/06/2024), Check Date (04/29/2024), and Check Type (eft - register generated). Below the table, the 'Risk Score' is 0.5 and 'Analytics Flagged' is 2. A list of control failures is shown, including 'Municipal Electric Ltd' and 'Atlantic Systems International', both with amounts of \$10,555. The interface includes navigation tabs for 'Check', 'Invoice', 'Purchase Order', 'Calculated', and 'Allocations'.

Monitoring

ThirdLine

Invoices Dataset

DATE RANGE

7d 14d 30d 90d Feb 4 - May 30

CONTROL FAILURES

98 unresolved transactions

TYPE All Control Failures High Risk RE

1 CONTROL FAILURE

Municipal Electric Ltd

Amount	Entered By	Invoice Entry Date
\$10,555	Richard	May 1, 2024

Analytics Flagged: Invoice Date > Entry Date

1 CONTROL FAILURE

Atlantic Systems International

Amount	Entered By	Invoice Entry Date
\$10,555	Linda	Apr 22, 2024

Accounts Payable

Add to list

1 of 37

Document # 303564 Invoice # 424535 ThirdLine ID 30356435569

MONITORING REVIEW

Ignore Resolve

Check Invoice Purchase Order Calculated Allocations

Check Amount	Check Clear Date	Check Date	Check Type
\$13,197.19	05/06/2024	04/29/2024	eft - register generated

Check Void Amount \$0.00

Risk Score 0.5 Analytics Flagged 2

Name	Description
Invoice Date > Entry Date	Control Low
Invoice 424535 (Document 303564) has an invoice entry date (2024-04-26) prior to its invoice received date (2024-05-01).	
Duplicate Invoices	Control Off Off
Invoice 424535 (Document 303564) is duplicated on vendor number and invoice amount within 10 days with invoice(s): 713922	

Software example: Monitoring queues help teams prioritize high-risk records and identify which exceptions deserve root-cause review.

Find root cause, remediate, and document the corrective action.

CORRECTIVE

Detection is not enough. A strong AI-ready ERP program investigates why the issue occurred and fixes the underlying cause so the same problem does not keep feeding the AI layer.

Action

Classify root cause: data entry, configuration, access, policy, training, process design, vendor setup, or system integration.

Control question

What changed because of the finding: data, process, policy, permission, training, or control logic?

AI clarity

Corrected and documented data becomes safer evidence for future AI answers.

Monitoring

ThirdLine De.

ThirdLine

Invoices Dataset Configure

DATE RANGE 7d 14d 30d 90d Feb 4 – May 30

SEARCH Vendor or employee

CONTROLS All control analytics More filters

CONTROL FAILURES
98
unresolved transactions

HIGH-RISK TRANSACTIONS
14
Risk score ≥ 2.5

TOTAL INVOICES
26,993
in selected period

TOTAL DOLLARS
\$1,354,972,029
amount sum

TYPE All Control Failures High Risk **REVIEW STATUS** All Open Ignored Resolved **SORT BY** Invoice Entry Date ↓

1 CONTROL FAILURE Ignore Resolve

Municipal Electric Ltd

Amount	Entered By	Invoice Entry Date	Invoice #	PO #	Invoice Description
\$10,555	Richard	May 1, 2024	424535	18485701	QUARTERLY LANDSCAPING MAINTENANCE

Analytics Flagged: Invoice Date > Entry Date

1 CONTROL FAILURE Ignore Resolve

Atlantic Systems International

Amount	Entered By	Invoice Entry Date	Invoice #	PO #	Invoice Description
\$10,555	Linda	Apr 22, 2024	713922	90155789	HAZARDOUS WASTE DISPOSAL

Analytics Flagged: Invoice Date > Entry Date

Software example: Review fields, dispositions, and notes help convert a detected issue into documented remediation evidence.

Monitor, refresh, report, and scale AI use cases.

CONTINUOUS

ERP data changes constantly. Vendors are added, users change roles, budgets are amended, accounts are opened, grants close, and contracts expire. AI readiness is continuous.

Action

Monitor data quality, classification drift, access changes, risk scores, output quality, and refresh history.

Control question

Are controls working, and do the metrics show fewer repeat issues over time?

AI clarity

Leadership sees an AI governance process, not a one-off experiment.

AP Risk

Views

Duplicate

+ Create Template

Edit

Share

Create View

Owner: ThirdLine Demo

Data

Dashboard

Exports

Samples

Invoice Scans

Edit

Export PDF

Total Invoice Count

29,966

\$ Avg Invoice Amount

\$50,281

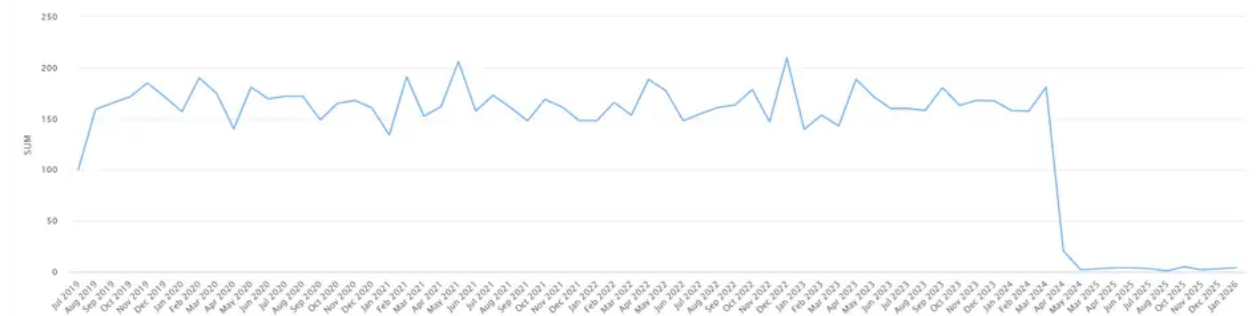
Total Invoice Amount

\$1.51B

Average Risk Score

0.3

Risk Over Time by Fund



Software example: Dashboards help management see readiness, risk, and control trends as the program scales.

Once the data is clean, controlled, classified, and remediated, AI can finally answer better questions.

Start with high-value, measurable, finance-owned use cases. Expand as the ERP control layer matures.

Budget-to-Actual

Explain variances, detect miscoding, and create leadership-ready narratives.

ACFR & Reporting

Map accounts, support reporting categories, and strengthen source evidence.

Audit Readiness

Organize evidence, track exceptions, and summarize review decisions.

AP & Vendor Risk

Identify duplicate payments, risky vendors, missing fields, and high-risk invoices.

Procurement

Connect spend to contracts, monitor thresholds, and flag unsupported purchases.

Monthly Close

Summarize open items, unusual entries, reconciliation gaps, and close blockers.

Access Controls

Define what each user can see, ask, summarize, and export.

Grants & Projects

Classify allowable costs, funding sources, match requirements, and closeout readiness.

Start small enough to monitor. Valuable enough to matter.

The best first AI pilots are narrow, measurable, finance-owned, IT-approved, and grounded in data that can be defended.

Recommended first pilot

- **Use case:** Budget-to-Actual, Compliance, and Audit Readiness.
- **Data scope:** GL, budget, chart of accounts, departments, funds, projects, vendors, permissions, policies, and exceptions.
- **Success criteria:** classified accounts, validated access, detected exceptions, remediated root causes, and source-grounded answers.
- **Owners:** finance, IT, budget, accounting, procurement, internal audit, and the AI/data champion.

90-day rollout rhythm

- **Days 1-30:** inventory systems, reports, owners, access rules, processes, and control gaps.
- **Days 31-60:** clean, classify, permission, risk-score, and create golden ERP test cases.
- **Days 61-90:** validate outputs, review root causes, document remediation, train users, and decide where to expand.

SOURCE NOTES

Research and design notes

1. ThirdLine product visuals and workflow examples are based on the AP analytics and policies demo, including configurable analytics, policy-to-analytic linking, risk score thresholds, monitoring queues, false-positive dispositions, and custom views.
2. UHY's AI + Data Governance materials frame safe public-sector AI around controls-first delivery, process understanding, clean structured data, data classification, value + risk scoring, governed automation, monitoring, auditability, and compliance.
3. MGO's AI adoption guidance for state and local government emphasizes governance, risk management, internal controls, data management, and compliance as part of responsible AI adoption.
4. ThirdLine branding uses the ThirdLine brand palette: Navy, Gold, Rust, Air, and White.

MAKE ERP DATA AI-READY

Clean. Control. Classify. Remediate. Then AI.

ThirdLine helps governments and schools stage ERP data for trusted AI use - without waiting for a perfect ERP cleanup project.



ThirdLine