The Bulletin

Turning AP Insights into Action.

BRONIEC ASSOCIATES

Volume 2
Issue 1
February 2026

In this Issue:

- **The Human Layer in Automated AP Environments**
- **Emerging AP Risks in 2026**
- **Why Automation Risks Surface Differently in Q1**
- **Industry Notes**

The Human Layer in Automated AP Environments

Automation continues to reshape accounts payable functions across industries. Intelligent invoice capture, automated matching protocols, and workflow orchestration now process transaction volumes that once required significant manual intervention. For many organizations, automation represents not only operational efficiency, but also a heightened sense of control. Embedded approval workflows and configured tolerances create the appearance of a closed-loop system in which risk is managed systematically.

However, automation does not eliminate error; it alters where and how risk manifests. Automated systems execute rules exactly as configured. Systems depend on the integrity of vendor master data, the precision of matching tolerance, and the stability of integrations across ERP, procurement, and payment platforms. What systems do not do is reassess assumptions over time or interpret whether transactional activity remains consistent with operational intent. When configurations drift, when vendor behavior changes, or when data inputs degrade, automation continues to operate efficiently — but not necessarily accurately.

As a result, exposure in automated environments is often less visible than in manual ones. Errors are not typically procedural; they are structural. Duplicate payments may arise following ERP migrations or inconsistent vendor practices. Contract pricing discrepancies may be absorbed within expanded tolerance thresholds. Credits and rebates may be excluded from invoice-centric workflows. Use tax accruals may reflect an imprecise configuration. In each instance, the system functions as designed, yet outcomes diverge from expectations.

Automated controls are highly effective at answering binary questions: whether an invoice matches a purchase order, whether the amount falls within tolerance, or whether the proper workflow was followed. Human evaluation, by contrast, considers coherence, context, and longitudinal patterns. Experienced auditors frequently identify risk not because a rule has been violated, but because transactional behavior no longer aligns with historical patterns. A vendor's credit activity may decline sharply after a system migration. Payments may cluster just below approval thresholds. Temporary process workarounds may become embedded in system logic. These conditions rarely trigger automated alerts, yet they signal emerging exposure.

Organizational maturity does not eliminate this risk. In fact, as environments grow more complex — integrating multiple platforms, automation tools, and shared service structures - potential points of misalignment increase. AP audits in automated environments, therefore, serve a distinct purpose. Independent auditors assess whether controls operate as intended in practice, whether exceptions, and whether foundational assumptions remain aligned with policy.

Independent reviews also provide necessary objectivity.

THE HUMAN LAYER *cont*

Internal teams, deeply familiar with their systems, may rationalize anomalies as acceptable variance or overlook gradual pattern shifts. External auditors are positioned to evaluate outcomes without inherited assumptions, reinforcing governance through objectivity and perspective.

The future of accounts payable is not defined by reduced automation, but by disciplined oversight. Automation accelerates processing and enhances consistency; human judgment validates that results remain coherent, compliant, and economically sound. Organizations that deliberately pair automated efficiency with periodic independent AP reviews strengthen not only control environments, but long-term financial assurance.

Key Takeaways:

- **Automation executes precisely as configured.**
- **It does not reassess whether configuration still reflects intent.**
- **In mature AP environments, risk shifts from visible transaction errors to structural misalignment. Periodic independent review validates that controls operate as designed and remain aligned with policy and contractual expectations.**



AUTOMATION & THE HUMAN EXPERIENCE

MARCH 10, 2026 | 1:00 PM EST

Join us for our upcoming webinar, Automation and the Human Experience, designed for finance, AP, and audit professionals who want to strengthen oversight in increasingly automated environments. Automation delivers speed and efficiency, but where does human judgment still matter most? This session explores the balance between system performance and human insight, helping you identify where risk can persist even in well-controlled environments.

What You'll Learn:

- Where automation performs exceptionally well and where limitations quietly emerge
- How human review identifies risks that automation wasn't designed to see
- Practical strategies to strengthen oversight, reduce exposure, and improve long-term process integrity

REGISTER NOW

Emerging AP Risks in 2026

Accounts payable environments are more automated and integrated than ever before. Yet the dominant risks are no longer manual errors or isolated breakdowns. Instead, exposure increasingly stems from structural misalignment within otherwise stable systems. We've identified these areas as most pressing and actionable risks for organizations seeking to protect financial integrity in 2026:

1. Configuration Drift After ERP Migrations
Organizations that completed ERP conversions or upgrades within the past several years are now operating beyond the stabilization phase. Over time, tolerance thresholds are adjusted, approval hierarchies modified, and exception handling practices normalized. These incremental changes rarely trigger alerts, yet they gradually weaken control precision and create opportunities for overpayments to gradually increase without oversight. Audit focus in 2026 is less about implementation accuracy and more about whether current configurations still reflect policy intent and contractual obligations.

2. Duplicate Payments in Automated Environments
Automation reduces keying errors, but system integrations, vendor consolidations, and master file merges introduce new pathways for errors. Variations in vendor IDs, payment timing, differences across payment methods, and incomplete vendor terms create conditions where duplicate payments occur without obvious exception flags. In highly automated environments, duplicate exposure often scales quietly.

3. Vendor Master File Integrity
Vendor master governance remains foundational. Consolidation initiatives, shared service expansions, and remote onboarding processes increase the likelihood of incomplete documentation, duplicate vendor records, or unauthorized banking changes embedded within otherwise compliant workflows. Because automated systems depend on master data accuracy, upstream weakness translates directly into downstream financial risk.

4. Tolerance Threshold Expansion
Matching PO tolerances are frequently adjusted to maintain processing speed during staffing shortages or volume spikes. Temporary adjustments often become permanent defaults. Expanded tolerances may absorb pricing discrepancies, short-ship variances, and contractual noncompliance without triggering review. While workflow metrics remain strong, financial leakage may accumulate incrementally.

5. Credits, Rebates, and Recovery Gaps
Invoice-centric automation prioritizes outbound payment accuracy but often overlooks credits, rebates, and offsets owed to the organization. When credit memos are not systematically matched or vendor statements are not periodically reconciled, recoverable funds remain unapplied. In automated environments, recovery gaps rarely appear as control failures. They appear as missed opportunities.

A Practical Perspective for 2026
The defining characteristic of emerging AP risk is not system failure, but misalignment. Controls may exist. Workflows may function. Dashboards may appear green. Yet configuration drift, data governance weakness, and tolerance expansion can quietly erode financial performance.

Organizations that combine automation with disciplined, independent AP audits are best positioned to preserve both efficiency and assurance.



ASK THE AUDITOR

Have a question about automation, AP controls, or audit risk?

Submit your question for consideration in our next issue of The Bulletin.

Selected questions will be addressed in upcoming editions.



Why Automation Risks Surface Differently in Q1

by: Frank Broniec
CEO, Broniec Associates, Inc.

As each new year begins, organizations operate with renewed clarity. From an accounts payable perspective, Q1 often appears to be a period of control and consistency. Yet, it is frequently one of the most revealing quarters of the year.

Automation has materially improved the efficiency and scalability of AP operations. Intelligent invoice capture, automated matching, and structured workflows enable substantial transaction volumes to move quickly and precisely. These systems perform exactly as configured. In contrast, in manual environments, errors were transactional and visible.

> **“In automated environments, exposure is structural.”**

Risk emerges when configuration, governance, or master data no longer align with operational intent. These conditions rarely surface during year-end, when the focus is on closing accurately and on time. They become clearer once the organization transitions from execution to evaluation.

The first quarter provides that evaluation window. Adjustments made in prior periods (modified approval hierarchies, revised tolerance parameters, vendor consolidations following ERP migrations) are now embedded in daily operations. Automation continues to execute those rules without reassessment. Temporary control changes can quietly become permanent features of the environment.

Q1 allows leadership to determine whether those shifts were intentional and appropriate.
Once activity stabilizes, payment patterns, credit utilization trends, and exception handling practices are easier to evaluate. At the start of the year, reporting is up to date, and dashboards reflect compliance. Stability can create confidence. Yet stability may also obscure embedded assumptions that have not been formally reviewed.

The first quarter should therefore serve not only as a planning period, but as a validation period. It is an appropriate time to confirm that automated controls continue to reflect policy standards, contractual obligations, and financial objectives. An independent review conducted early in the year allows organizations to address structural misalignment before operational pressure intensifies.

Automation remains essential to efficiency and scale. Our responsibility is to ensure it operates within a disciplined governance framework. Systems determine how transactions flow. Leadership determines whether those flows continue to support the organization’s goals. Q1 provides the discipline and visibility to make that determination.

Q1 Diagnostic Insight:

The first quarter is not only a planning period, but it’s also a validation window. Once year-end pressure subsides, embedded control changes become easier to evaluate. Q1 provides leadership with the visibility to confirm that automated workflows, tolerances, and vendor governance still align with financial objectives.

Industry Notes: Brief Observations Shaping AP

Mid-market public companies and PE-backed organizations are facing increased expectations around documentation of internal controls. While automation reduces manual touchpoints, regulators continue to emphasize demonstrable oversight, particularly around system configuration, vendor governance, and segregation of duties. **Automation alone is not sufficient evidence of control effectiveness.**

Industry research continues to show the highest risk period for finance transformations occurs 12–24 months after go-live. During this phase, configuration changes, staffing turnover, and workflow normalization can erode originally designed safeguards. **Stabilization does not equal optimization.**

Social engineering schemes are increasingly targeting vendor onboarding and banking update processes. In highly automated payment environments, compressed review time can amplify exposure if callback and validation controls weaken. **Vendor master governance remains foundational.**

States continue to intensify outreach and audit activity related to unclaimed property. Legacy credit balances and unapplied vendor refunds remain areas of focus. **Periodic review of dormant liabilities is increasingly prudent.**

What This Means for 2026
Across regulatory scrutiny, ERP post-implementation risk, evolving fraud tactics, and unclaimed property enforcement, one theme is consistent:

- Control environments must evolve alongside automation.
- Organizations that proactively review configuration integrity and vendor governance are better positioned to reduce exposure before it becomes operationally disruptive.

BRONIEC
ASSOCIATES

Since 1972, Broniec Associates has delivered the utmost value and benefit through the most comprehensive accounts payable audit in the industry. Our 21 offices serve clients globally across nearly every industry.

Let's Connect
Have questions or want to discuss how we can help your business?
Connect with us for industry updates and expert insights.
www.broniec.com

Stay Informed
Subscribe to The Broniec Bulletin to get insights, industry news, and event updates straight to your inbox.
🔗 https://broniec.com/subscribe
