BRONIEC ASSOCIATES

WHITE PAPER SERIES

The Hidden Cost of What You Can't See

Researched and compiled by Arelis Romero, Marketing Manager | Reviewed for accuracy by Matt Broniec, MIS Director

Every payment, report, and automated workflow in accounts payable rests on general assumption: a supplier name matches the right entity, an address is current, a taxpayer ID belongs to the vendor being paid, two records with slightly different spellings are, in fact, two different companies, etc. These aren't facts but assumptions, and most AP organizations have never tested them.

The question of data quality is an emerging trend hiding underneath the automation, analytics, and AI investments currently reshaping AP. Every one of those tools makes an organization more dependent on the quality of its underlying data, not less. As such, clean data, once considered a housekeeping task, today functions as part of the financial control environment.

Gartner research puts the average annual cost of poor data quality at roughly $12.9 million across the large organizations surveyed, though the figure varies significantly by company size and includes factors like lost productivity, missed opportunities, and rework.1 MIT Sloan Management Review research goes further still, estimating that poor data quality costs the typical company 15 to 25% of revenue. Furthermore, Gartner found that nearly 60% of organizations do not measure the cost of poor data quality, which means they are managing the risk blind.[1]

This white paper explores how data quality shapes financial control, information reporting, and technology performance across the purchase-to-pay process, focusing on the accounts payable function, and outlines a practical approach for maintaining it over time.

The Problem Isn't Always Bad Data

Data quality issues rarely announce themselves. No supplier record flags itself as "duplicate," and no stale address identifies itself as “outdated”. These problems accumulate quietly, and they are common in nearly every supplier master:

- Duplicate records created under variations of the same name
- Multiple addresses or remittance locations for one supplier
- Inactive suppliers still marked active
- Missing or outdated tax information
- Name and taxpayer ID mismatches
- Records inherited through acquisitions or system conversions
- Inconsistent naming conventions across business units
- Unverified changes to banking, address, or contact information
- Supplier data maintained differently across ERP environments

None of these looks like a serious issue on its own, but together, they determine whether an organization actually knows who it is paying, why, and whether the numbers built on top of that data can be trusted.

Follow the Data Downstream

Poor supplier data does not stay contained to the master file, it travels. A duplicate record makes duplicate-payment detection harder. An unverified address complicates supplier validation. A wrong taxpayer ID surfaces months later, at filing time, as a problem someone else has to solve. Spend



The Hidden Cost of What You Can't See

fragmented across multiple records for the same vendor understates that supplier relationship in every report that depends on it. Legacy issues carried through an ERP migration do not disappear in the new system; they simply find a new home.

The scale of the downstream flow is easy to underestimate. Benchmarking from APQC puts duplicate or erroneous payments at 0.8 to 2% of total disbursements industry wide.[3] This means that for a company processing $50 million a year through AP, the low end of that range alone amounts to $400,000, money that no one knew was gone until someone went looking for it. The pattern tends to follow a consistent chain: poor data leads to weaker visibility, which creates control gaps, which in turn produce payment and reporting errors, adding cost and risk at every step. This is why data quality is not simply a supplier-master issue. It reaches AP operations, procurement, tax, treasury, internal audit, compliance, and finance leadership alike, usually at the moment when none of them have time to trace the problem back to its source.

1099 Reporting Makes the Risk Concrete

Information reporting is where data quality stops being theoretical. The IRS's Taxpayer Identification Number (TIN) Matching program exists specifically so authorized payers can verify payee name-and-TIN combinations against IRS records before filing, reducing backup-withholding notices and filing errors before they occur. The dollar figures make the stakes hard to ignore - for information returns due in 2026, IRS penalties range from $60 per return for corrections made within 30 days, to $340 per return for corrections made after August 1 or returns never filed. Intentional disregard carries a minimum penalty of $680 per return, with no cap. The IRS specifically lists incorrect or missing TINs among the conditions that trigger these penalties.[4]

Multiply these numbers across a master file with hundreds or thousands of reportable vendors, and a seemingly small data issue stops being small. Organizations that treat TIN validation as a year-end scramble are the ones most likely to be caught off guard by it, while organizations that treat it as an ongoing part of the supplier lifecycle rarely are.

Technology Doesn't Fix Data, It Amplifies It

ERP migrations and acquisitions carry a quiet assumption, that moving to a new system creates a clean start. It does not. A migration carries the data forward, duplicates, inconsistencies, and inactive records included, into a new environment that simply has a better interface.

Acquisitions compound this challenge. Two companies may share dozens of the same suppliers, tracked under a legal name in one system and a trade name in the other, with different supplier numbers, classifications, and payment terms attached to each. When those datasets are combined without first being reconciled, the result is not consolidation, but two sets of inconsistencies now living under one roof.

Automation raises the same stakes in a different form. Whether the underlying issue is unreconciled data moving forward unchecked through a migration or acquisition, or flawed data feeding an automated process, the pattern is the same: technology does not distinguish good information from bad, it simply moves faster on whatever it is given. Automation is often framed as the fix for process inconsistency, and in many respects, it is. But automation also changes what happens when the underlying data is wrong. A manual process might encounter a bad supplier record once, get flagged by a person, and be corrected. An automated process encounters that same bad record every time, at scale, often without anyone noticing.

Automation determines how quickly and consistently a process runs, while data quality determines whether that process is working from the right information in the first place. The same principle applies to AI and advanced analytics, since the value of any insight is capped by the quality, completeness, and context of the data feeding it. Better technology does not make data governance less important; it raises what is riding on it.



The Hidden Cost of What You Can't See

As Gartner research director Mei Yang Selvage puts it, "good quality data empowers business insights and starts new business models in every industry."[1] The reverse holds just as true, in that poor-quality data narrows what any of these tools can safely be trusted to do.

Maintaining Data Is a Lifecycle, Not a Project

Most organizations address supplier data through periodic cleanup initiatives, treated as projects with a defined start and end date. The trouble with this approach is that data does not stay still. Once someone adds a new supplier or updates a banking detail, the file begins drifting again. Data quality tends to hold up better as an ongoing lifecycle rather than as a one-time initiative, moving through a consistent cycle of validating, standardizing, monitoring, reconciling, and correcting information, then repeating the process.

In practice, this means a handful of specific commitments:

- Ownership should be clearly assigned, so that a role, not merely a department, is accountable for supplier data quality and has the authority to enforce standards.
- Standards should be set before problems occur, with naming conventions, required fields, and duplicate-checking rules defined at the point of supplier creation.
- Validation should happen during onboarding, confirming TIN, name, and banking details, and matching against IRS records where applicable.
- High-risk changes (particularly to banking and remittance addresses), warrant verification at the time they occur, not during the next audit.
- Existing records should be reviewed on a set cadence, not only after a merger or migration.
- Exceptions should be treated as signals rather than noise, since a cluster of similar discrepancies is often evidence of a process gap rather than a string of unrelated errors.

A third-party accounts payable review can help establish this baseline, or confirm that an internal process is holding, particularly around master file audits, TIN verification, and duplicate-payment recovery, areas where an independent set of eyes tends to catch what internal reviews, understandably, miss.

Conclusion

AP organizations will continue investing in faster systems, deeper automation, and more capable AI. However, every one of these investments rely on something far less sophisticated: the supplier names, tax IDs, addresses, and payment records an organization has been accumulating for years, often without anyone assigned to keep them straight.

> "After decades of auditing accounts payable across virtually every industry, one pattern holds true everywhere: the organizations with the fewest surprises are the ones that treat their data as seriously as they treat their financials."
>
> - Matt Broniec, MIS Director, Broniec Associates, Inc.

The right question is not simply, "Is our data clean?" It is narrower, and harder to answer comfortably: how confident are we that the data driving our AP environment can actually be trusted, and who would know if it could not? Clean data does more than make reporting easier. It is the difference between an organization that can see its own risk clearly, and one that learns about it later, from someone else.

Sources

[1] Gartner, "How to Stop Data Quality Undermining Your Business," Gartner Data Quality Market Survey.

[2] MIT Sloan Management Review, cited in "Data Quality Improvement Stats," Integrate.io (2026).

[3] American Productivity & Quality Center (APQC), Open Standards Benchmarking, Accounts Payable, cited in "Duplicate Payments: How Much Is Your Company Losing?" (2025).

[4] Internal Revenue Service, Publication 1099 (2026), General Instructions for Certain Information Returns, TIN Matching guidance; IRS TIN On-Line Matching, updated June 18, 2026; IRS Information Return Penalties, 2026 penalty schedule.



The Breaking Point: Hidden Risk in Modern Accounts Payable

About Broniec Associates

Broniec Associates helps organizations gain independent visibility into the effectiveness of their accounts payable controls, vendor management practices, and financial processes. For 54 years, organizations have relied on Broniec to identify hidden financial risk, validate operational controls, and uncover opportunities for process improvement through independent audit and review services.

Serving organizations across healthcare, higher education, manufacturing, hospitality, retail, and other industries, Broniec combines experienced professionals, proprietary technology, and proven methodologies to help clients strengthen financial oversight in increasingly complex operational environments.

Broniec Associates is a SOC 2 Type II certified, Veteran-Owned Small Business and a three-time Great Place to Work® recipient.

Learn more at *broniec.com*.