

MEKORMA

Why Vendor Validation is Now a Critical AP Strategy

Not Just a Compliance Checkbox

Table of Contents

Introduction	3
The Rising Risk Landscape	4
The Hidden Cost of Non-Compliance	4
AP's Expanding Role in Risk Management	5
The Compliance-First Framework for Vendor Validation	6
How Mekorma Supports AP Teams to Stay Compliant & Reduce Risk	9
Appendix: Self-Audit Checklist for AP Vendor Compliance	11
References	12



Introduction

Accounts Payable (AP) is no longer just about invoices. With shifting global trade dynamics and increased regulatory scrutiny, AP teams face growing responsibilities and an opportunity to positively impact organizational well-being.

The current enforcement landscape is seeing an increase in penalties, while no longer requiring proof of intent. This means that even minor oversights can lead to serious financial consequences for organizations. Ensuring accurate vendor data and compliance has become essential, making AP a central player in risk management.

In this guide, we'll explore why vendor validation is now central to AP operations, outline key risks, and present a practical framework for safeguarding your organization through smart automation with Mekorma Vendor Validation.

The Rising Risk Landscape

In the United States, the last five years have seen an increase in government oversight of trade, vendor relationships, and compliance. Agencies like the Office of Foreign Assets Control (OFAC) have broadened their enforcement reach, increasing penalties.

In early 2025, OFAC updated or expanded sanctions involving multiple countries, including Iran, Venezuela, and China.

It has become vital for business wellbeing to rigorously screen all vendors prior to engagement to avoid partnering with restricted entities. Even if an organization works solely with local vendors, regular screening is important to ensure compliance and avoid penalties.

Under strict liability regulations, “we didn’t know” is no longer a defense. AP teams must stay informed and take every precaution to avoid working with sanctioned vendors.

This means AP teams are liable for who they pay and staying informed about any regulatory or sanctions changes.



The importance of implementing and maintaining risk-based sanctions compliance programs for companies of all sizes and operations cannot be overstated.

MORRISON FOERSTER

The Hidden Cost of Non-Compliance

Consistent, well-documented compliance practices aren't just a nice-to-have, they're essential to protecting your organization. Gaps in compliance can lead to financial, operational, and reputational risks.



Fines & Penalties

OFAC civil penalties can exceed \$300,000 per violation.



Audits Risks

Inadequate controls can trigger red flags during financial or tax audits.



Reputational Damage

Vendor payment errors or compliance issues can erode stakeholder trust.



Operational Disruptions

Invalid vendor data may lead to payment delays, procurement issues, or duplicate payments.

Even if your team believes they're following the rules, a lack of clear documentation or gaps in automation practices can still put your company at risk.





AP's Expanding Role in Risk Management

As the gatekeepers of outbound payments and vendor relationships, AP teams are uniquely positioned to identify vulnerabilities and mitigate risks before they escalate.

Today's AP departments have evolved far beyond their traditional function as data entry, check printers, or simple transaction processors. Today, AP plays a pivotal role in financial control, regulatory compliance, and enterprise risk management.

This expanded role means AP is now responsible for:

- ✓ **Monitoring Third-Party Risk:** Vendors are extensions of your supply chain and financial ecosystem. AP teams must regularly assess and validate vendor legitimacy, data accuracy, and compliance.
- ✓ **Detecting Fraud and Irregularities:** Because AP teams manage invoice processing and payment disbursements, they are on the front line and often the first to spot unusual patterns such as duplicate invoices, falsified data, or mismatched records.
- ✓ **Supporting Audit Readiness:** From maintaining vendor files to documenting validation procedures, AP must ensure traceability and transparency in all actions taken.
- ✓ **Strengthening Internal Controls:** AP teams can help prioritize regulatory compliance by collaborating with Finance, Procurement, and IT to help enforce segregation of duties, build approval workflows, and prevent policy overrides. This will help strengthen internal controls, ensure clear documentation, and show due diligence.

By embracing these responsibilities, AP professionals can drive strategic value and become proactive stewards of enterprise resilience. However, this can only happen with the right tools and systems in place.

AP is no longer just about cutting checks or paying invoices. The core of AP is about preventing the next big mistake before it hits your bottom line.

The Compliance-First Framework for Vendor Validation

Compliance shouldn't be a scramble when an audit hits or a regulation changes. By designing a proactive framework, AP teams can turn vendor validation into a strategic advantage, not just a checklist task.

Here's how to build a robust, repeatable process:

Step 1: Lay a Solid Foundation with Accurate Onboarding

Onboarding should never be just about payment details. Set the tone for compliance by getting vendor data right from the start. A key part of onboarding any new vendor should always be data verification and compliance.

Choosing the right tools to support your vendor validation process will not only help protect your organization today but also position you to respond quickly and confidently when regulations shift without warning.

AP's mission in onboarding new vendors should be to confirm that each vendor is legitimate and safe to work with. Your onboarding should include:

- ✓ **Collecting Verified Tax Forms**
Always require W-9s or W-8s as applicable, and ensure forms are filled out completely and correctly.
- ✓ **Validating Tax Identification Numbers (TINs)**
Use IRS TIN Matching services to verify that vendor names and TINs match government records. This is an easy way to avoid 1099 mismatches and potential fines.
- ✓ **Confirming Physical Addresses**
Run vendor addresses through USPS address validation or Google Address Validation to ensure they're real, properly formatted, and deliverable.
- ✓ **Establishing Business Legitimacy**
When possible, confirm the vendor is registered and in good standing with their local jurisdiction.
- ✓ **Checking Sanctions List**
Always check new vendors against the most recent OFAC sanctions list. This list can change quickly, so it's important to ensure you are checking regularly.





Step 2: Don't "Set It and Forget It" - Screen on an Ongoing Basis

Vendor data can become outdated faster than you think, especially in today's political climate. Anticipate regularly evolving international sanctions and business changes that could affect a vendor's status.

To stay current and compliant, Accounts Payables teams should get in the habit of conducting ongoing validation checks as part of a monthly or quarterly rhythm.

- ✓ **Sanctions Screenings**
Routinely check the OFAC Sanctions List, especially for international vendors or suppliers from high-risk regions.
- ✓ **Status Monitoring**
Keep tabs on vendors whose tax, registration, or legal standing may change over time.
- ✓ **Documentation Discipline**
Log every check your team makes and update the status with timestamps. Whether automated or manual, maintaining a full audit trail is your best defense during reviews or audits.

Step 3: What to Do When a Vendor is Flagged – Immediate Actions to Take

Even with a strong vendor compliance strategy in place, issues will arise from time to time. What matters is how your AP team responds. To stay ahead, establish a clear, consistent process for handling concerns as they come up.

If a vendor is flagged during routine screening, use the following steps to take action swiftly and responsibly:

- 1** **Verify It's Not a False Positive:** Sanctions lists often include common or similar names. Double-check that the flagged entity matches your vendor's exact name, TIN, and address. Confirm whether it's a case of mistaken identity before escalating.
- 2** **Contact the Vendor Through Verified Channels:** If the issue involves a new or suspicious address, a change in banking information or contact name, we recommend reaching out to the vendor using contact details already on file. Avoid using new contact or banking information until it can be verified. You may also consider a small test payment to check banking details.
- 3** **In the Case of New OFAC Sanctions, Proceed with Caution:** If a previously validated vendor has suddenly appeared on the OFAC sanctions list, it may be best to get legal advice.
- 4** **Pause Payments Until Cleared:** Do not proceed with any payments until the vendor is fully verified and any issues have been resolved. If in doubt, err on the side of caution and seek legal input to avoid compliance breaches.
- 5** **Document Every Action Taken:** Regardless of vendor status, it's best practice to maintain a detailed log of every validation check, including TIN and address verification, identity confirmation, phone calls, or automated vendor validation checks. A clear audit trail will protect your team and demonstrate due diligence in case of future scrutiny.

Having a well-defined response plan allows your AP team and organization to act decisively when faced with potential risks from compliance issues. By responding quickly, your team can help avoid turning a red flag into a costly mistake for your organization.

Step 4: Build Compliance into the Workflow with Automated Controls

Technology makes it possible to enforce rules without relying on memory or manual effort. With automation tools, you can ensure that as little as possible falls through the cracks, even when the workload gets busier.

Choose a tool that offers:



Real-Time Alerts

Automatically flags new or existing vendors that match restricted entities or invalid information.



Payment Holds

Prevents funds from being disbursed until flagged records are reviewed and cleared.



Policy-Based Approvals

Intelligent workflows that require additional approvals or secondary validation for high-risk vendors.

Proactive compliance is your best strategy. Catch issues early and stay informed about any changes.



How Mekorma Supports AP Teams to Stay Compliant & Reduce Risk

Now more than ever, Mekorma Vendor Validation is your key to unlocking efficient and consistent vendor validation and compliance practices.

Vendor Validation is a built-in feature within the Mekorma Payment Hub designed to ease the compliance burden while improving vendor data integrity.

With Mekorma, your AP team can:

- ✓ Automatically screen vendors against OFAC lists so you don't have to
- ✓ Validate Tax Identification Numbers (TINs) with the IRS and street addresses with Google Address Validation and USPS for U.S. based vendors.
- ✓ Flag high-risk vendors for follow-up before payments are processed
- ✓ Automatically hold payments when risks are detected. No manual intervention required.
- ✓ Maintain an audit trail that shows compliance checks were performed
- ✓ Schedule recurring validations to ensure ongoing accuracy

Mekorma Vendor Validation runs directly inside your ERP, making it a seamless part of your AP process for Microsoft D365 Business Central, Dynamics GP, and Acumatica.

Compliance is Essential, but it Doesn't Have to Be Complicated

Vendor validation has always been important, but in today's shifting regulatory environment, it's mission critical. Now is the time for AP teams to embrace a strategic role in supporting their organization's risk management and compliance.

Mekorma Vendor Validation helps simplify vendor validation, reduce human error, and stay ahead of quickly changing rules. With automated safeguards and audit-ready documentation, you can embrace uncertainty with confidence.

The logo for MEKORMA, featuring the word in a white, sans-serif font. The letter 'O' is replaced by a green triangle pointing upwards. A thin horizontal line is positioned below the logo.

MEKORMA

Want to learn more?

*Download our brochure, schedule a demo,
or read more on our blog.*

Find us at www.mekorma.com

Appendix

Self-Audit Checklist for AP Vendor Compliance

Use this checklist to evaluate your current processes and identify areas for improvement

Vendor Onboarding & Data Accuracy

- ☐ Do you collect and verify W-9s or equivalent tax forms during onboarding?
- ☐ Are all Tax Identification Numbers (TINs) validated against IRS records?
- ☐ Do you use USPS or Google Address Validation to confirm vendor addresses?
- ☐ Is vendor data reviewed for completeness, formatting, and consistency?

Sanctions & Compliance Screening

- ☐ Are vendors screened against the OFAC Sanctions List before payments are issued?
- ☐ Do you perform regular (e.g., monthly or quarterly) vendor rescreening?
- ☐ Is there a documented process for handling matches or potential red flags?

Automation & Risk Controls

- ☐ Have you implemented automation to flag high-risk vendors or incomplete data?
- ☐ Are payments automatically held when compliance issues are detected?
- ☐ Do your systems prevent users from bypassing review and approval workflows?

Documentation & Audit Readiness

- ☐ Can you produce an audit trail of all validation and compliance checks?
- ☐ Is your AP team trained on current compliance requirements?
- ☐ Do you maintain a written policy for vendor validation?

Score Yourself

- ☐ **12 – 15 checks:** You're on solid ground. Your team is set up for success.
- ☐ **8 – 11 checks:** Some strong practices in place. Review gaps and prioritize updates.
- ☐ **Less than 8:** Consider a system or workflow overhaul to reduce risk and improve compliance.

Resources

U.S. Department of the Treasury – Office of Foreign Assets Control (OFAC)

Sanctions Programs and Information

<https://ofac.treasury.gov/sanctions-programs-and-country-information>

U.S. Department of the Treasury – OFAC Enforcement Actions

Civil Penalties and Enforcement Information

<https://ofac.treasury.gov/reports/ofac-enforcement-actions>

Internal Revenue Service (IRS)

e-Services for Tax Professionals (TIN Matching)

<https://www.irs.gov/e-services/e-services-for-tax-professionals>

Internal Revenue Service (IRS)

Form 1099-G Instructions and Penalties

<https://www.irs.gov/instructions/i1099gi>

U.S. Customs and Border Protection (CBP)

Trade Updates, Tariffs, and Import Regulations

<https://www.cbp.gov/trade>

Morrison Foerster LLP (MoFo)

Sanctions Enforcement Trends: Preparing for 2025 and Beyond

<https://www.mofo.com/resources/insights/240103-sanctions-enforcement-trends>

Baker McKenzie

Global Sanctions Update – 2024

<https://www.bakermckenzie.com/en/insight/publications/2024/02/global-sanctions-update>

Deloitte

Third-Party Risk Management: The Compliance Imperative

<https://www2.deloitte.com/global/en/pages/risk/articles/third-party-risk.html>

Institute of Finance & Management (IOFM)

2024 Accounts Payable Benchmarks and Compliance Trends

<https://www.iofm.com>

PYMNTS.com

Why AP Automation Is a Must for Compliance and Risk Mitigation

<https://www.pymnts.com/news/b2b-payments/>

United States Postal Service (USPS)

ZIP Code Lookup and Address Verification Tools

<https://tools.usps.com/zip-code-lookup.htm>