



Three Steps to Minimizing Supplier Risk

Danny Thompson



Danny Thompson
Senior Vice President,
Market & Product Strategy
APEX Analytix

Biography

Danny Thompson is the Senior Vice President Market & Product Strategy at APEX Analytix (<https://www.apexanalytix.com/>) and is responsible for defining and leading APEX Analytix's software product strategy and roadmap.

As the world's leading provider of supplier portal software and AP recovery audit services, APEX Analytix has been at the forefront of AP technology for over 20 years, working to safeguard over \$4.6 trillion. Its SmartVM database of 20 million + proprietary, scored supplier records was revolutionary, and it continues to move towards the future.

The recent release of APEX Analytix's cognitive technology, APEX Archimedes, and its Supplier Statements module for statement recovery audit, marks the next steps in APEX Analytix's audit recovery technology.

Keywords Accounts payable, Risk, Fraud, Robotics, Vendor master, Supplier portals
Paper type Research

Abstract

Are rogue vendors lurking in your supplier base? According to APEX Analytix' latest research ([Apex Analytix](#)), almost two-thirds of Global 1,000 businesses have over 10,000 suppliers in their vendor master file. As the author of this article explains, being assured of the credentials of each and every one of those vendors is far from straightforward.

Introduction

The risks of rogue vendors are obvious. Some risk management providers monitor for business and supply chain risk rather than fraud risk, but as APEX Analytix *Financial Leaders' Benchmarking Report*¹ demonstrates – the risks of fraud remain great across the board. Is a supplier actually a front for an employee – an employee who is authorized to approve or pay fake invoices? Misconduct, for another: is an employee-owned business, or one in which an employee has a significant interest, being wrongly preferred over other, cheaper, suppliers?

Is a supplier with a legitimate-looking name actually associated with one of your genuine suppliers, or is that superficial similarity an attempt at fraud? Or might your organization be trading with one of the thousands of prohibited organizations on the various lists maintained by the United States government, the European Union, and the United Nations? The penalties for doing so can be severe.

So how, then, should organizations protect themselves from such risks? Here at APEX Analytix, we recommend a three-stage process. First, get your house in order, then guard the front door, and then guard the back door.



Technology and Innovation

The good news: new technology makes this process easier – and more powerful – than ever before.

1. Getting your existing Vendor Master house in order

Here, the focus is on consolidating and validating your existing vendor records, flagging exceptions, and filling in any blanks. It's certainly possible to do it manually, although this can be resource-intensive. But working with an expert solution provider means that you can take advantage of their investment in automation and validation technology. This means that not only are vendor records checked against external data sources in order to validate data such as addresses, tax identification numbers, and banking information, but the expert solutions provider is also able to fill in any gaps.

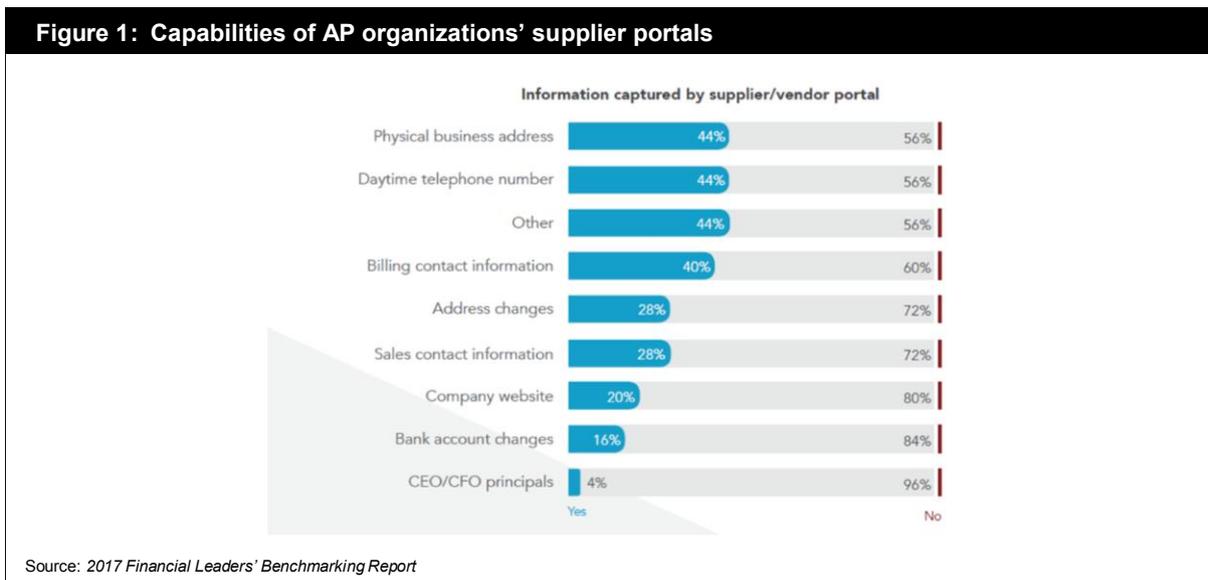
At a minimum, for instance, you will want them to enrich the basic name and address information with any missing contact names, phone numbers, email addresses, and corporate linkages, as well as add any missing Dun & Bradstreet D-U-N-S numbers, SIC/NAIC codes, and information on any applicable ownership status that might be relevant to your strategic procurement initiatives.

2. Guarding the front door

With clean Vendor Master Data, the focus moves to keeping it that way. That way any new – or changed – vendor master records are entered fully, and validated for accuracy.

Self-service supplier information portals are an excellent way of achieving this, by allowing organizations to capture vendor data at source. Suppliers are required to enter the necessary information online, with data first being captured, and then validated against third-party official records. Again, the use of an expert solution provider simplifies the process, as well as making the validation process easier and more effective, by integrating with official and third-party vendor verification data sources.

Figure 1: Capabilities of AP organizations' supplier portals





By enforcing compliance – suppliers have to satisfactorily complete the registration process through the portal to actually become suppliers – organizations gain a significant amount of control. Going forward, they know with a high level of certainty that they are minimizing supplier-related risk.

3. Guarding the back door

Finally, keep a constant eye on your vendors, and protect your back door. Best-in-class organizations deploy advanced technology solutions in the form of continuous monitoring of vendor data and vendor behaviour. Simply put, new technology enables organizations to carry out far more checking and de-risking than ever before. AP organizations can now continually monitor their suppliers for information they are not sharing. Tapping into external data sources, and matching changes in vendor data and vendor behaviour against known and emerging risk profiles, they run in the background – 24/7 – helping to keep organizations safe and secure from ongoing risk.

Figure 2: Vendor risk management practices in practice



Finding the solution

There are multiple ways to find these solutions, here at APEX Analytix we believe technologies that combine artificial intelligence software capabilities such as machine learning and robotic process automation will deliver the most impact. Leading organizations are embedding these technologies into their AP organization and employing solutions that are continuously learning and resulting in smarter recoveries, controls, analytics and working capital.

In addition, we use fraud scoring predictive analytics technology in our FirstStrike-Fraud Detect solution, our Vendor Risk Analysis service, and our Supplier Portal



Technology and Innovation

(where fraud scoring is automatically recalculated during supplier on-boarding, at any time a change is made to the supplier profile, and also on-demand).

Figure 3: The APEX Analytix Supplier Information Management Suite



In the solution, 115 separate supplier and invoice activity characteristics are combined into 21 sub-scores, and then combined into a calculated overall summary fraud score. Scoring is configurable, with suppliers who exceed a set threshold trigger then being identified for a follow up investigation.

In short, guarding against supplier-related risk has never been easier, or more effective. If your organization is serious about vendor risk, then help is at hand.

Reference

¹ <http://unbouncepages.com/apexanalytix/benchmarking-report-4/>