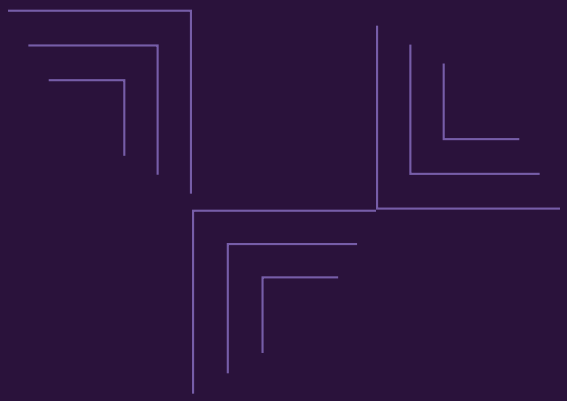
Galvanize
is now Diligent



Balancing risk control & productivity

Understand the gaps in your ERP system controls to maximize performance

Table of contents

A finance leader's guide to balancing risk & performance 3

The risk control & productivity trade-off 4

Data analysis to the rescue 5

Are your risk management controls effective? 6

Address red flags & minimize false positives 8

7 ways to improve your risk management & performance 10

- 01 The purchase-to-pay cycle 11
- 02 Payroll & expense systems 12
- 03 Order-to-cash 13
- 04 General ledger & journal entries 14
- 05 SOX compliance 15
- 06 Anti-bribery legislation 16
- 07 Using a whistleblower program to detect major fraud 17

What to look for in a solution 18

Fix the gaps in your ERP system controls 20

A finance leader's guide to balancing risk & performance

CEOs are increasingly looking to the finance function to give more insight to drive strategic risk decisions.

Finance leaders already manage financial risk, cash flow, strategic investment and compliance. So, their role is fundamentally about balancing risk with opportunities to increase performance. But how do they make sure the risks related to fraud, error and abuse are being managed well? And how do they do that without sacrificing performance objectives?

The typical approach is to rely on the controls in enterprise resource planning (ERP) systems.

But how dependable is that? In this eBook, we'll look at some natural gaps that exist in ERP systems—and specific actions you can take to better mitigate risk and focus on improving financial performance.

The risk control & productivity trade-off

Controls help reduce the risk of things going wrong and causing damage to the organization. So the more controls in place, the better, right? Not exactly.

It's a perpetual trade-off between running a high-performance organization versus implementing controls to reduce risks.

The more controls in place, the more likely that processes will become unacceptably slow and cumbersome. That often means frustrated employees come up with ways to bypass controls just to get their work done.

So, how do you know if risks are material enough to negatively impact strategic objectives? For example, how do you know if a series of payments that bypassed approval procedures aren't actually part of a bigger pattern of bribery?

To some extent, ERP systems were intended to help deal with this problem. The theory was that an integrated enterprise-wide system on a single platform would be more efficient and could also have sufficient built-in and automated controls to minimize the risks of bad things happening.

But ERP systems come with their own risks. How many of these can you spot in your organization?

+ You have more than one ERP platform; controls in standalone applications and at the point of connection to an ERP system often hide weaknesses that create additional risks
+ There are often multiple individual instances of ERP systems, spread across locations and business areas; this results in duplicate invoices and payments being processed if the same vendor is set up as both a corporate and a branch entity
+ If control settings are activated, they're often subject to workarounds—perhaps well-intended or for the sake of efficiency—as well as deliberate attempts to bypass controls
+ Your ERP control settings aren't turned on
+ The pressures of implementation deadlines cause some controls to be overlooked
+ Data entry errors as simple as misspellings are very common and virtually impossible to eliminate
+ It's difficult to get insight into what's actually working well and what's a problem

Data analysis to the rescue

Data is key to finding the balance between running a high-performance financial process and efficiently managing the gaps that exist in your ERP-centric controls.

Risk analytics, monitoring and risk visualization transform the effectiveness of financial control systems. They provide that exact balance between tight controls and maximum performance.

Data analysis can also provide an additional, compensating layer of control over financial processes. This helps ERP systems be more productive and efficient while reducing risk.

External auditors and high-performing finance and controls teams alike are using these methods to improve controls and strategic risk management, and help the organization become audit-ready.

Are your risk management controls effective?

Testing transactions automatically.

Traditionally, auditors and other control specialists review procedures, perform some walk-throughs and test sample transactions. Now, with specialized risk analytics and monitoring software, you can examine every single transaction to determine whether:

+ The transaction complies with the control procedures that should be in place
+ There are indications for risks and problems that have no effective control

You can do this by testing every transaction in multiple ways. For example, a payment amount to a vendor can be examined to determine that:

+ The vendor is valid, approved, not duplicated in the vendor master file and not on a sanctions list
+ The payment matches an invoice, goods received records and properly approved purchase order (PO), and there haven't been attempts to bypass any controls
+ Payments haven't been duplicated due to erroneous or deliberate changes in invoice details

You can also examine huge volumes of data to find unusual trends and predict performance.

You can look at transactions from a given business process to locate problems or opportunities for improvement. Answer questions like:

+ What would happen if we raised our prices for this segment of our customer base?
+ Why are overtime payments, or travel expenses, unusually high in one specific office?
+ Why is a previously dormant account suddenly being used for a series of journal entries?

When you use data analytics for automated transaction testing:

+ It's fairly easy to see where primary control weaknesses are happening
+ Problem transactions can be identified immediately, giving you real-time oversight of the health of your ERP processes
+ Control weaknesses that allowed the problem to occur can be strengthened
+ Problems can be addressed quickly, before they worsen
+ Transaction analysis and monitoring can actually become an additional level of control

Address red flags & minimize false positives

A common concern when starting with data analysis is wondering if you'll spend all your time reviewing false positives.

This is exactly why you should supplement your ERP controls with a risk analysis and management solution.

After all, someone in your organization needs to:

+ Examine the test results and identify what's a real threat, and what's a false positive
+ Flag exceptions, anomalies and trend reports
+ Decide what to do next

This is where a risk analysis and management solution with continuous monitoring adds some serious value. You can fine-tune automated testing thresholds to almost completely eliminate time-wasting false positives. What's left are the red flags that are most likely to represent a real control risk.

And when your finely tuned system does flag a violation, the exception management software can connect issues. For example:

+ A transaction is flagged as a violation of payment approval controls
+ The next step is for someone to immediately review approvals by that person
+ This helps determine if there are indications of a large-scale problem

A NEW LEVEL OF INSIGHT & ASSURANCE

Using data to monitor transactions and run ongoing risk assessments means the finance director or CFO, along with the rest of senior leadership, all get ongoing insight into risks. It's far more objective, quantifiable and current than using traditional techniques of sample testing and process walk-throughs.

These methods give only limited insight into what has actually taken place when millions of transactions are involved. On the other hand, a data-driven approach provides comprehensive monitoring of financial and business transactions and activities. This gives management in the three lines of defense—as well as external auditors and audit committees—increased confidence in the integrity of financial systems.

IMPROVING REPORTING CAPABILITIES

Risk and control monitoring software helps executives review processes in a more comprehensive way:

+ Generate color-coded heat maps to prioritize risks
+ Immediately see a current assessment of risk and control effectiveness in a dashboard
+ Compare risks arising from different business process areas
+ View risks in the context of enterprise-wide risk

“Proactive data monitoring was associated with 52% lower losses and frauds detected in half the time.”

» ***Association of Certified Fraud Examiners***

2018 Report to the nations on occupational fraud and abuse

7 ways to improve your risk management & performance

Key areas you can improve with a dedicated risk and control solution.

01
The purchase-to-pay cycle

Your procurement and vendor payment process is susceptible to fraud and error by vendors and employees. In most industries, funds flowing through purchase-to-pay (P2P) systems are so large that even a single error could mean big losses. And that could be easily overlooked if you only rely on controls enforced in your ERP system.

Duplicate data and poor-quality data are expensive problems for organizations—both in terms of overpayments and time wasted in resolving issues.

Many vendor billing errors are unintentional process errors. But vendors and employees can also deliberately attempt to defraud, knowing that invoice errors happen and sometimes go undetected.

Whether intentional or not, some examples include:

+ Slightly mistyping an invoice number
+ Using two accounts with different spellings for the same vendor
+ Setting up fake vendor accounts

ERP system controls prevent vendor and invoice information being entered twice, but only if they differ enough. They don't necessarily capture these sneaky tweaks—this is where data analytics helps.

CATCHING COMMON VENDOR BILLING PROCESS VULNERABILITIES

Data analysis is great at analyzing entire vendor databases to find instances of data duplication and errors.

Here are some common analytic tests that can be applied to payment data:

+ Determine if approval controls are circumvented by splitting transactions into smaller amounts just under a manager's approval limits
+ Check the validity of Social Security numbers and tax IDs to weed out fictitious contractors and vendors
+ Identify matches between vendor payment data and employee data to find "phantom vendor" schemes
+ Identify attempts to bypass controls by unauthorized changes to vendor bank account data, or to a manager's approval limits
+ Check for fraudulent or incorrect invoices by analyzing records of goods and services provided
+ Determine instances of unusually high charges for goods and services (against averages), which could signify fraudulent collusion between a vendor and an employee

02
Payroll & expense systems

Payroll is obviously a large expense area for most organizations. It's also another place where standard, ERP-enforced controls are likely to be leaky, which means employee fraud could be easily missed.

We've compiled some typical analytic tests for finding leaks and fraud in payroll, procurement cards (P-Cards), and travel and expenses (T&E) claims.

PAYROLL

+ Analyze data to find employees working abnormally high overtime hours or earning higher-than-usual bonuses
+ Match data to find payments made to employees who have left the company or who are deceased
+ Identify "phantom" employees by matching data to actual employee activity (e.g., access card data)

P-CARDS

+ Identify non-authorized personal expenditures by analyzing data that is associated with non-business items and services
+ Find transactions made at suspicious times (e.g., weekends, holidays or vacation periods)
+ Identify split transactions in which a large purchase is paid for in smaller amounts that are just under a review/approval threshold
+ Test for purchases of the same item or service within a specific time frame (e.g., one may be legitimate, the other personal)
+ Check for duplicates (e.g., a P-Card was used; the same purchase was also processed as a T&E claim)

T&E EXPENSES

+ Find duplicate claims by matching charges made through P-Cards as well as through a travel reimbursement claim
+ Compare dates of expense claims with HR records for employee vacation dates
+ Analyze claims to find expenses for airfares and hotels in non-standard locations (e.g., resorts)
+ Search for expense claims including vendor names and keywords that are associated with personal-use items and services
+ Identify airfare payments/claims for which there are no corresponding hotel or meal charges
+ Check for instances where mileage claims were made for the same time period as car rental charges or other transport costs

03
Order-to-cash process

How much money are you leaving on the table? The processes within a financial institution are, of course, very different from those in manufacturing and distribution businesses. Similar principles apply for analytics that are used to confirm that the delivery of goods or services results in appropriate billing, and that error or fraud hasn't resulted in lost revenues.

TYPICAL REVENUE CYCLE TESTS

- Match records of services or goods delivered with details of invoices
- Match invoice or other billing details to price lists
- Check for appropriate approval of discounts provided
- Check commission calculations for salespeople
- Examine accounts receivable credits and write-offs for appropriate approvals and reasonableness

04
General ledger & journal entries

Using analytics to test your general ledger journal entries is a good way of finding fraud indicators. It's not just possible financial statement fraud, but also various forms of fraud by employees who try to hide cash theft, diverted customer payments or inventory items by processing an adjusted journal entry.

Many external audit firms use standard suites of journal entry data analytics as part of their annual audit procedures and in support of SAS 99 requirements. More than in any other process areas, it makes sense for your team to run similar analytics ahead of an audit in order to make sure you're audit-ready.

TYPICAL ANALYTICS TO TEST JOURNAL ENTRIES

+ Look for a lack of appropriate segregation of duties between journal entries and approvals
+ Examine journal entries posted at unusual times (e.g., weekends or vacation periods)
+ Examine journal entries posted to previously dormant accounts
+ Check for postings between unusual combinations of accounts
+ Examine unusual and non-regular intercompany transfers

05
SOX compliance

Requirements for testing internal controls over financial reporting can be painful. However, data analysis—using the same kind of analytics as those referred to throughout this eBook—can greatly reduce the burden of regular testing.

SOX compliance can be achieved by automating key control tests through the use of transaction analysis. The entire SOX certification process is also helped by using technology to automate getting controls test confirmations and signoffs.

01
Document processes, risks & controls

02
Evaluate & test controls

03
Report

04
Certify

06
Anti-bribery legislation

Supplementing ERP-based controls with risk analytics software helps address the risk of failing to comply with anti-bribery and corruption regulations like the *Foreign Corrupt Practices Act* (FCPA) and the UK *Bribery Act*. They help find specific instances of potential bribery and make the overall compliance process more efficient.

The use of data analysis and monitoring can sometimes result in lower fines and penalties if FCPA violations occur. This in itself is excellent justification for using data analysis to test for possible instances of bribery and corruption.

Aside from analytics, software-based questionnaires, surveys and self-certification all support the processes for anti-bribery compliance and save you a lot of time. An automated process can, for example, ask managers to confirm they understand an organization's policies around anti-bribery and anti-corruption, and confirm that they haven't been involved in any contravening activities.

Systems can also be created to provide preapproval of activities that could potentially be seen as being an instance of bribery or conflict of interest. This data can be linked to the relevant controls in a risk and control database, providing full-circle oversight by combining preapproval controls with detective controls.

EXAMPLE ANALYTICS FOR ANTI-BRIBERY COMPLIANCE

+ Search for suspect keywords relating to payments and other forms of benefit
+ Identify unusual payments and funds transfers made through bank accounts in high-risk regions

07
Using a whistleblower program to detect major fraud

Hotlines and other forms of whistleblower reporting systems are good at detecting certain types of fraud and abuse. Integrated workflow technology means you can gather information anonymously and connect the reported incidents into other components of risk and control systems. For example, individual reports from hotlines and whistleblower reporting websites can be linked to an assessment of a particular type of risk exposure or control effectiveness. They can also be aggregated into a central library and included in dashboards reporting overall risk status.

You can connect reported incidents into a full escalation management process. Certain conditions can instantly be flagged and sent to investigators for review. Aggregated data with associated comments and resolution efforts can be analyzed with visualization tools to gain insight into trends and risk areas.

What to look for in a solution

Data analysis software designed specifically for control testing and detection of fraud, waste and other risks also has specific functional capabilities.

In general, look for:

+ Pre-built analytic routines such as classification, stratification, duplicate testing, aging, join, match and compare, as well as various forms of statistical analysis, including Benford analysis, all of which help to find fraud indicators
+ Data manipulation capabilities for combining, matching and extracting data
+ Data visualization—to spot unexpected anomalies and to provide new insights
+ Ability to perform complex testing and fraud detection
+ Ability to access a broad range of data sources and types
+ Support for full automation and scheduling of analytics
+ Comprehensive logging of all procedures performed (which is important in generating complete trails to support detailed investigation)
+ Ready access to an online repository of proven analytics
+ Online best practices training

Fix the gaps in your ERP system controls

Without technology, your job would be impossible. Your ERP system is core to achieving your objectives and serves you well in creating streamlined processes that promote performance. However, ERP systems can definitely let you down in the details—and the human workarounds that create fraud, waste and abuse.

A huge opportunity exists for the savvy finance leader to take advantage of technology to monitor and interrogate the gaps that exist in their organization's ERP-based controls.

Take a closer look at your environment. Chances are there are millions of dollars to be saved in reduced waste and, even more importantly, great opportunities to detect patterns that help you unlock future performance.

Ready to learn how our HighBond platform gives you oversight of critical controls and ERP process gaps?

To transform your organization's risk and control monitoring, financial process health and performance, call 1-888-669-4225, email info@wegalvanize.com or visit **wegalvanize.com**.

Galvanize
is now Diligent

ABOUT THE AUTHOR

John Verver, CPA CA, CMC, CISA

John Verver is a former vice president of Galvanize. His overall responsibility was for product and services strategy, as well as leadership and growth of professional services.

An expert and a thought leader on the use of enterprise governance technology, particularly data analytics and data automation, John speaks regularly at global conferences and is a frequent contributor of articles in professional and business publications.

ABOUT GALVANIZE

Galvanize, a Diligent brand, is the leading provider of GRC software for security, risk management, compliance and audit professionals. The integrated HighBond platform provides visibility into risk, makes it easy to demonstrate compliance, and helps grow audit, risk and compliance programs without incurring extra costs.

wegalvanize.com