THE FINANCE LEADER’S GUIDE TO BALANCING RISK AND PERFORMANCE

Understand the gaps in your ERP system controls to maximize performance
# Table of Contents

The Finance Leader’s Guide to Balancing Risk and Performance

Understand the gaps in your ERP system controls to maximize performance ........................................ 3
  The ultimate trade-off: risk control vs. productivity ......................................................... 4
  Vulnerabilities within ERP systems ............................................................. 4
  A technology-driven solution, right under your nose ............................................... 5

How to illuminate risks in finance and accounting systems while maintaining high performance control systems .......... 6
  Best practices for reducing financial, business and compliance risks ............................................ 6
  Really understand the risks...
  then define intelligent control measures ................................................................. 6
  How do you know if your risk management and control measures are effective? ......................... 7
  Cutting to the actual red flags is your new secret sauce ..................................................... 8
  Gathering important input on risk and controls from across the organization ......................... 9

In search of risk management & performance improvement?
  7 Performance Hacks................................................................. 10

  Performance Hack 1:
  Put paid to problems in your purchase-to-pay cycle ........................................ 12
  Performance Hack 2:
  Stamp out waste in your payroll and expense system ........................................ 14
  Performance Hack 3:
  Plug Order-to-Cash leaks in your revenue cycle ........................................ 16
  Performance Hack 4:
  Interrogate general ledger & journal entries .................................................. 17
  Performance Hack 5:
  Seriously reduce the burden of SOX compliance ........................................ 18
  Performance Hack 6:
  Don’t get bitten by anti-bribery legislation .................................................. 19
  Performance Hack 7:
  Implement a whistleblower program to detect major fraud .................................... 20

Technology buying guide for risk and control management and analytic monitoring:
What capabilities are needed to deliver the best results? ........................................ 22

Understand the gaps in your ERP system controls to maximize performance ........................................ 24

About the Author:
John Verver ................................................................. 26

About ACL ................................................................. 26
UNDERSTAND THE GAPS IN YOUR ERP SYSTEM CONTROLS TO MAXIMIZE PERFORMANCE

Whether you bear comprehensive responsibility for the finance function or lead a part of the team focused on your own area of operational excellence, your role is fundamentally about balancing risk with opportunities to spur greater performance. The burden of managing financial risk, cash flow, strategic investment and compliance is a complex job, involving a broad spectrum of responsibilities.

How can you be confident that the risks of fraud, error and abuse are being well-managed without getting in the way of achieving your performance objectives? The typical approach is to rely on the types of internal controls that are built in to processes, and in particular, into Enterprise Resource Planning (ERP) systems. But how dependable is this approach in practice?

Think about it: central to understanding where you stand is your reliance on what your ERP system is telling you. But it is difficult (dare I say impossible) to effectively control business processes and stop leakage from within such a complex platform. In these pages, we’ll share with you the finance leader’s guide to understanding the natural gaps in your ERP system—and the specific actions you can take to grab risk by the scruff of the neck so you can focus on maximizing performance.
The ultimate trade-off: risk control vs. productivity

No system of internal controls is perfect—and they don’t have to be. Controls are designed and implemented to reduce the risks of things going wrong that may damage the organization in some way. But controls come at a cost.

If a system were to be so highly controlled that risks are reduced to almost zero, the inevitable result is an unwieldy, cumbersome and slow process that limits the ability of your organization to simply get the job done.

**So, you’re faced with a perpetual trade-off between running a high performance process versus reducing the risks of fraud, error, abuse and regulatory non-compliance.**

While some of these risks may be considered not likely to be material enough to negatively impact strategic objectives...how can you be sure? How do you know, for example, whether a series of payments that managed to circumvent proper approval procedures are not actually part of a pattern of bribery that could result in massive fines, penalties and negative publicity? What if some senior managers are manipulating sales figures or expenditures in a way that distorts financial results?

Vulnerabilities within ERP systems

To some extent, ERP systems were originally intended to help deal with this problem. The theory was that an integrated enterprise-wide system on a single platform would not only be more efficient, but could also have sufficient built-in and automated controls to minimize the risks of bad things happening. But the reality has turned out to be different.

**There are a number of common risk exposures relating to ERP implementations. How many of these can you spot at your organization?**

- **You probably have more than one ERP platform!** In practice, larger organizations run multiple ERPs, as well as various applications that must be linked into the ERP systems. Controls in standalone applications and at the point of connection to an ERP often hide weaknesses that create additional risks.

- **There are often multiple individual instances of ERPs**, spread across many locations and business entities. When multiple instances of an ERP are in place, it may well be that duplicate invoices and payments can be processed if the same vendor is set up in both a corporate and branch entity.

- **Within any given ERP instance, it is often the case that many application control settings are not turned on.**

- **The pressures of implementation deadlines caused some controls to be overlooked** (sound familiar)? In others, there may have been a deliberate decision not to enable a control—for the sake of increased efficiency and flexibility.

- **If control settings are activated, they are subject to “workarounds”—perhaps well-intended or for the sake of efficiency—as well as deliberate attempts to bypass controls.**

- **Data entry errors** as simple as misspelling are shockingly common and virtually impossible to eliminate. For example, duplicate vendor or customer accounts are created, with slightly different spelling of names or addresses. This provides a wide (and undetected) opening for duplicate payments, error and fraud to occur.
A technology-driven solution, right under your nose

How can you achieve an optimum balance between running a high-performance financial process and efficiently managing the gaps that exist in your ERP-centric controls? The answer is in your data.

It’s no secret that technology and “big data” analysis has done much to transform marketing and the insights that can be achieved into areas such as customer behavior, product requirements and market opportunities. Business Intelligence (BI) software has likewise illuminated performance at a high level.

**What’s in it for you?** Risk analytics, monitoring and risk visualization, closely integrated into risk and control management systems, has a comparable ability to transform the effectiveness of financial control systems—providing a balance between the goals of tight control and maximizing performance.

In fact, data analysis can provide an additional, compensating layer of control over financial processes—enabling ERP systems to be very productive and efficient, while reducing risks such as fraud, error, abuse and regulatory non-compliance.

If you engage external auditors, make no mistake: they are utilizing this technology. And the highest-performing finance and control teams are now running similar analytics, not only to improve controls and strategic risk management, but also as best practices to help ensure the “audit readiness” of the organization.
Best practices for reducing financial, business and compliance risks

Risk and control management software can help you address fraud, error, abuse and compliance violations in a number of ways.

Here are the primary strengths this technology brings to the table:

✔ Manage the process of identifying risks and control weaknesses
✔ Document the policies and controls that should be in place
✔ Perform data analysis, and monitor risks and controls
✔ Review red flags and ensure that issues raised are addressed
✔ Manage the remediation of identified red flags
✔ Gather input and responses from across the organization on the status of internal controls

Let’s start by looking in more detail at areas of technology-driven best practices that play a role in balancing control and performance:

Really understand the risks...then define intelligent control measures

You’re already well aware of the general risks that exist in different business processes and the typical control measures that should be in place. For example:

» **Purchases and payments** need to be authorized by designated managers, within defined approval limits and with appropriate segregation of duties from others involved in processing a transaction.

» **Salaries and payroll** need to be approved by management, and detailed payment amounts agreed with HR system records.

» **Customer billing and discounts** given need to be based on records of goods and services delivered and according to agreed pricing schedules and manager approvals.

» **General ledger journal entries** need to be entered and approved by separate individuals within their authorization limits and with effective segregation of duties.

While defining basic risks and appropriate control measures is fairly simple, there are always variations in the way that systems and processes work. It is a constant challenge to consider all the “what-if’s” of things that can go wrong.

Once set, it’s pretty likely that you rely entirely on ERP system controls to ensure all is running well (until your auditors arrive on the scene). Which should make you wonder...
How do you know if your risk management and control measures are effective?

Being able to review a reliable assessment of the risk and control universe is a great starting point, but your ERP system simply isn’t designed to help you here. The next essential (but often missing) step is to get insight into what is actually happening: what is working well and what is in reality a problem. It is here that ERP systems really start to let you down.

Traditionally, auditors and other control specialists would review procedures, perform some walk-throughs and test some sample transactions from time to time. You could also be asked to sign off to confirm that the controls you are responsible for are effective. Specialized risk analytics and monitoring software has fundamentally transformed this approach.

The new basic concept is not complicated: Use data analysis software to examine every transaction in an entire population of data (for example, every recorded activity thing that took place within a financial or business process) to determine whether:

1. The transaction complies with the control procedures that should be in place
2. There are indications that there are risks and problems for which no effective control is in place

This is achieved by testing every transaction in multiple ways

For example, a payment amount to a vendor can be examined to determine:

» That the vendor is a valid one, properly approved, not duplicated in the vendor master file, not on a PATRIOT Act sanctions list or in a FCPA PEP database
» That the payment matches to an invoice, which matches to goods received records, which matches to a properly approved purchase order (PO) and that there have been no attempts to circumvent approval controls by splitting PO payments into smaller amounts just under an approval threshold
» That payments have not been duplicated due to erroneous or deliberate changes in invoice number details
» And so on...

Best-in-class leaders apply dozens of similar automated tests across transactions in each business process area on a regular basis to get insight into their process health.

Examine big data volumes to find unusual trends and predict performance

Another important form of data analysis and monitoring is to examine all the transactions that took place within a given business process in search of problems and opportunities to improve. Your data is very telling in response to 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 one vendor paid twice as much as other vendors for the same type of item? Why is a previously dormant account suddenly used for a series of journal entries? What trends indicate a problem that’s consistently worsening? Or what turns out to be far less of an actual problem than was originally thought?

Of course, some people may question why any of this is necessary:

“Shouldn’t we just make sure the controls in the ERP and other applications are set up properly and rely on them?”

It is a fair question. In an ideal world, every business process application would have built-in controls that prevent any erroneous, invalid or suspicious transaction from taking place. Unfortunately, the reality is that no control is perfect or foolproof. And more controls isn’t necessarily the answer: the more controls that are in place, the more likely that processes become unacceptably slow and cumbersome—spurring employees to come up with innovative ways to bypass controls just to get their work done.

When data analysis and transaction monitoring is performed after the fact, it is relatively simple to determine where the primary control weaknesses are occurring. Problem transactions can be quickly identified and addressed. Control weaknesses that allowed the problem to occur can be strengthened to prevent a recurrence. And no one has to stay late jumping through hoops.

And, big bonus: transaction analysis and monitoring can actually become an additional level of control, both reinforcing those controls that are in place and compensating for those ERP-based controls that are either not working effectively or not in place at all.
The advantage of this approach—continuous monitoring, as it is often described—is that it provides timely notification of issues. Instead of the traditional approach of waiting for auditors to perform testing long after transactions have taken place, risk and control testing provides immediate indication of a problem, giving you real-time oversight of the health of your ERP processes. Being able to respond more quickly increases the chances that the problem can be addressed—before it worsens.

Cutting to the actual red flags is your new secret sauce

So, you’re sold and want to supplement your ERP-based controls with risk analysis and monitoring software made for the purpose. A typical objection you may run into is the potential to actually reduce performance trying to wade through volume of “false positives.” Someone needs to examine the results—flagged “exceptions” and anomalies, trend reports—and decide what needs to be done. This is a very practical concern, as the chances are that if a manager is given a list of hundreds of different items to investigate, nothing will get done. This is where monitoring can produce volumes of potentially very important information...that no one is actually using. Risks and control problems often go unaddressed because people are focused on getting on with what they think is their primary job, and inadvertently let issues escalate to the point of causing serious harm to your organization.

This is where the ability to fine-tune automated testing thresholds becomes very important. Fine-tuning allows false positives to be almost eliminated, so that the system only identifies red flags that are very likely to represent a real control risk. There is no need to be fielding (or ignoring) constant false alarms.

And once your finely tuned system red flags a violation, one of the great benefits of data analysis and exception management software in the big picture is the ability to connect issues. For example, if a particular transaction is flagged as a potential violation of payment approval controls, the next step can be to immediately review every approval made by that individual to determine if there is a pattern that indicates a larger scale problem.

“PROACTIVE DATA MONITORING was associated with 54% lower losses and frauds detected in half the time.”

Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse*

The ACFE’s most recent report shows that the average loss within those organizations that had implemented “proactive data monitoring/analysis” was $92,000, compared to $200,000 in those that did not. The study shows that this form of anti-fraud control is the most effective one out of 18 categories in reducing the amount of loss from fraud.

It is also very effective in reducing the average duration of fraud: by 50%, from 24 to 12 months.
Ongoing risk assessment and status reporting

Best practice use of risk and control monitoring software not only manages the workflow aspects, but also allows the entire process to be reviewed and for the current status of all monitoring activities to be illustrated and quantified. This is where software plays another uniquely powerful role: it provides the ability for executive management to see a current assessment of the entire universe of risks and control effectiveness. The risks arising from different business process area can be compared—and also put into the context of other enterprise-wide categories of risks.

Masters of the Risk Universe: Risk and control analytics technology gives you the ability to generate a visual color-coded heat map of risks, for example, as well as drilldown capabilities to see the detail of specific issues. It also enables the ability to report, for example, that $X billion of transactions in the purchase-to-pay cycle were examined and Y%, representing $Z million, were found to involve control breakdowns. **Of these, A%, or $B, resulted in recovery of funds and improvements in control procedures.**

Gathering important input on risk and controls from across the organization

**Surveys, questionnaires and analysis of responses**

Software that supports automated surveys and questionnaires can gather large amounts of information directly from individuals in different control roles across the organization and rapidly interpret what is found. Analysis of survey responses to issues is a new and rapidly developing area in the world of risk and control management.

In the case of SOX and ICFR compliance, just as one example, individuals can be asked to sign off on control effectiveness questions. The information can be quickly consolidated and used to support the SOX certification process in a far more efficient way than traditional techniques.
IN SEARCH OF RISK MANAGEMENT & PERFORMANCE IMPROVEMENT?

7 PERFORMANCE HACKS...
The premise of this guide is that despite your diligence, the nature of your ERP system means that it will let you down in key areas, leading to enhanced risk and reduced performance.

Here are the hottest spots to interrogate with technology designed for the job.
Your procurement and vendor payment process is one that is particularly susceptible to fraud and error, caused by vendors as well as by employees—reducing performance. Funds flowing through procure-to-pay systems are so large in most industries, that even a very low rate of error or fraud can mean eye-popping losses, which you are extremely likely to overlook if relying on ERP-enforced controls.

Vendor billing errors remain among the most common problems in purchase-to-pay systems. Many instances are simply process errors inadvertently made by vendor systems or employees. However, there can also be deliberate attempts to defraud, by vendors or by colluding employees, simply because they know that invoice errors can occur and remain undetected.

“But I already have controls to detect duplicate invoices.”

–You

Well, ERPs will not allow the same invoice number for the same vendor to be entered twice, but what if the invoice number is accidentally or deliberately miskeyed? What if there are actually two different accounts for the same vendor, with slightly different spelling of the name? This is definitely happening.

Another control weakness arises when vendors are set up more than once in the system. This often occurs because of variations in the spelling of corporate names when they are entered. An ERP system will normally prevent a duplicate vendor from being established if name and address information are identical. But if they differ sufficiently, the entries are accepted. Duplicate data and poor quality data are often a very expensive problem for organizations—both in terms of overpayments and time wasted in resolving issues. Clearly, if this is possible in your environment, performance is being affected.

How data analytics solves the duplicate and erroneous data challenge

Data analysis is very effective at analyzing entire vendor databases and finding instances of data duplication and error. It uses sophisticated algorithms to find misspelling and data entry errors. In the case of vendor processes, it can be used to analyze all purchase and payment transactions over a period of time and look for combinations of variables that indicate a likely problem. Tests can identify an identical amount paid to a vendor within a given timeframe, or an identical invoice number and amount paid to two different vendors.

It is not unusual to apply up to 10 different variations of potential duplicate tests that can bring problems to light. Excessive numbers of false positives are managed by allowing the search parameters and combinations to be varied by an authorized user of the monitoring system.
Dealing with many common vendor billing process vulnerabilities

Here are a number of analytic tests that are typically applied to payment data:

» Tests to determine if procurement and payment approval controls are circumvented by "splitting" transactions into smaller amounts just under a manager's approval limits

» Tests for payments to fictitious contractors and vendors by checking validity of SSNs and tax IDs

» Identify matches between vendor payment data and employee data to find "phantom vendor" schemes

» Identify attempts to bypass controls by short-term unauthorized changes to vendor bank account data, or to manager's payment approval limits

» Tests for fraudulent or incorrect invoices by checking details to records of goods and services provided

» Analyze payment data to determine instances of unusually high charges for goods and services when compared to averages that can signify fraudulent collusion of a vendor with an employee who authorizes purchases
Payroll is obviously another large expense area for most organizations and again, standard, ERP-enforced controls are very likely to be leaky. The performance drain can be material, but more concerning is the undercurrent of employee fraud you are almost certainly blind to.

Here are some typical analytics for finding leaks and fraud in payroll, P-cards and T&E expenses:

**Payroll**
- Analyze data to identify abnormally high overtime and bonus payments
- Match data to determine payroll amounts paid to individuals who have left employment or are deceased
- Identify "phantom" employees by matching data to indicators of actual employee activity, such as swipe card data

**Procurement Cards (P-Cards)**
- Identify expenditures on items typically associated with personal use by looking for merchant codes, vendor names and key words that are associated with non-business items and services
- Identify transactions made on weekends, holidays or while the employee is on vacation
- Identify split transactions in which a large purchase is paid for in smaller amounts, just under a review/approval threshold
- Test for purchases of the same item or service within a specific timeframe (e.g., one purchase may be legitimate, the other may be intended for personal use)
- Check for duplicates in cases where a P-Card was used for a specific purchase and the same purchase was also processed as a T&E claim
Travel & Entertainment (T&E) Expenses

» Compare claims data to uncover claims by multiple employees for the same expense

» Compare dates of expense claims with HR records for employee vacation dates

» Analyze claims to find expenses relating to airfares and hotels in non-standard locations (e.g., vacation resorts)

» Identify claims for meals for multiple persons made on the same day and at the same location as claims made by other employees

» Find duplicate claims by matching charges made through procurement credit cards as well as through a travel reimbursement claim

» Search for expense claims including vendor names and key words 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
How much money are you leaving on the table? The processes within a financial institution are of course very different from those in a manufacturing and distribution business. Nonetheless, similar principles apply for analytics that generally seek to determine that the delivery of goods or services results in appropriate billing, and that error or fraud has not resulted in lost revenues.

Typical revenue cycle tests include:

» 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 sales people
» Examine accounts receivable credits and write-offs for appropriate approvals and reasonableness
Analytic testing of your general ledger journal entries can be a good way of finding indicators of fraud—not just of possible financial statement fraud, but also of various forms of fraud by employees who attempt to hide theft of, for example, cash, diverted customer payments, or inventory items by processing an adjusted journal entry.

Many external audit firms make particular use of 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 help ensure "audit readiness."

Typical analytics to test journal entries include:

» Look for lack of appropriate segregation of duties between entry and approval
» Examine journal entries posted at unusual times, on weekends and when an employee is on vacation
» Examine journal entries posted to previously dormant accounts
» Check for postings between unusual combinations of accounts
» Examine unusual and non-regular inter-company transfers
PERFORMANCE HACK 5:
SERIOUSLY REDUCE THE BURDEN OF SOX COMPLIANCE

Requirements for testing Internal Controls over Financial Reporting (ICFR) are a burden for you and your team. The good news is that data analysis, using the same kind of analytics as those referred to throughout this guide, is now well proven as a method of reducing the burden of regular testing.

Compliance with SOX can be achieved in large part by automating key control tests through the use of transaction analysis. The entire SOX certification process is also considerably helped by using technology to automate the process of obtaining controls test confirmation and sign-offs.

TO LEARN MORE, DOWNLOAD ACL’s FREE eBook
“The Essential Guide to Seriously Reducing the Burden of ICFR/ SOX/ A-123 Compliance”

info.acl.com/SOX-OMB123-eBook.html
Supplementing ERP-based controls with risk analytics software can have a big role to play in helping to address the risks of failing to comply with anti-bribery and corruption regulations such as FCPA and the UK Bribery Act. They not only help to find specific instances of potential bribery, but also help you make the overall compliance process more efficient.

In cases where FCPA violations have occurred, for example, the U.S. Department of Justice has accepted that the implementation of data analysis and monitoring can result in the reduction of fines and penalties. This in itself is good justification for using data analysis to test for possible instances of bribery and corruption.

The types of analytics applied for anti-bribery compliance purposes include, for example:

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

Aside from analytics, software for questionnaires and self-certification can be used to support the processes for anti-bribery compliance, saving you a lot of time. An automated process can, for example, ask managers to confirm that they understand an organization’s policies around anti-bribery and anti-corruption and confirm that they have not been involved in any contravening activities.

Systems can also be established to provide pre-approval of activities which could potentially be seen as being an instance of bribery or conflict of interest. This data can also be linked to the relevant controls in in a risk and control database, providing full-circle oversight by combining pre-approval controls with detective controls.
PERFORMANCE HACK 7:
IMPLEMENT A WHISTLEBLOWER PROGRAM TO DETECT MAJOR FRAUD

Hotlines and other forms of whistleblower reporting systems are among the most effective means for detecting certain types of fraud and abuse, and this is definitely not going to be a feature of your ERP solution. Integrated workflow technology gives you the ability to gather information anonymously and then connect the reported incidents into other components of risk and control systems. Individual reports from hotlines and whistleblower reporting websites, for example, can be linked to an assessment of a particular type of risk exposure or control effectiveness. They can also be aggregated into a central repository and included in overall risk status reporting dashboards.

Reported incidents can also be connected into a full escalation management process, where certain conditions can instantly be flagged and broadcast to investigators for review. Aggregated data with associated comments and resolution efforts can be analyzed with visualization tools to gain insight into trends and areas of greatest risk.

Learn how ACL’s automated workflow technology can help you build whistleblower or incident reporting web forms and much, much more:

capabilities-sheet-workflow-remediation-of-analytic-results.pdf
Incident Reporting
Crystalis Ventures

Instructions
Reporting Responsibility
Any person with a concern relating to Accounting Standards or compliance with the Company’s Code of Ethics may submit their concern in writing by one of the following methods:
- By telephone or email on a confidential and anonymous basis through Whistle Blower Security, a hotline service to handle any complaint on a confidential and anonymous basis which is unrelated to the Company and reports directly to the Chair of the Audit Committee by:
  VoiceMail Message
  Call 1-888-999-4225 FREE to talk to leave a confidential message.
  OR
  Email message to: audit_chair@acl.com
  This Whistleblower service will maintain your anonymity if you so request. However, use of a non-identifiable or third party email address may also be used to maintain anonymity.
  OR
  (b) in writing to the Chair of the Audit Committee of the board of directors as follows:
  Mr. Brian Chung, Confidential
  Suite 1500 - 860 Howe Street
  Vancouver, BC V6Z 1W8

1. Is this a violation of or non-compliance with the Company’s Code of Ethics, including:
   - Violation of any corporate policies, including health & safety, environmental, operational or ethical
   (a) Yes
   (b) No

2. Is this a complaint or concern regarding the Company’s compliance with Accounting Standards
(a) Yes
(b) No

Submit
Modern, easy to use and collaborate interfaces and platforms

You can’t eliminate a risk if you can’t see it—and software only adds value if you and your team actually use it. These are two important principals that should help guide your selection of risk and control monitoring software. This category of software has advanced as rapidly as software in the general consumer market, transforming the historic implementation challenge into what is now a simple and rapid process. Usability has also taken huge strides with interfaces that are genuinely intuitive.

Portability is another feature of modern audit and risk software, supporting use not just on desktops and laptops, but also on tablets and phones. This enables your control specialists with the ability to gather and access information, as well as perform testing and processing, without being tied to an office or desk. This can be a game-changer in terms of getting your team to actually use it.
Integrated support of all aspects of risk, control and audit processes

Old-school products tend to have compartmentalized functionality with separate software product components for different aspects of risk and control management processes, in addition to data analysis and monitoring. While these often can support data exchange between components, they are often not closely and consistently integrated. For example, analytic or survey capabilities are provided by separate products that are not closely integrated with specific risk and control functionality.

Modern software products, on the other hand, offer a high degree of integration, with seamless integration of functionality for:

- Defining and documenting risks and controls
- Assessing and ranking risks
- Assessing and testing control effectiveness
- Analyzing transactions and data
- Investigating results
- Managing exceptions
- Remediation and escalation workflow
- Automated questionnaires and surveys
- Dashboards and reporting
- Standard analytic tests
- Data and test repositories
- Data analysis and monitoring

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, compare, as well as various forms of statistical analysis, including Benford analysis, all of which have a role to play in helping to find fraud indicators
- Data manipulation function capabilities for combining, matching, 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 of 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
UNDERSTAND THE GAPS IN YOUR ERP SYSTEM CONTROLS TO MAXIMIZE PERFORMANCE

You simply couldn’t do your job without technology. Your ERP system is core to achieving your objectives and broadly serves you well in establishing streamlined processes that promote performance. ERP systems though, will definitely let you down in the details, and the human workarounds that create fraud, waste and abuse.

It’s a natural law.

Today, like never before, a huge opportunity exists for savvy finance leaders to take advantage of technology that is designed from the ground up to monitor and interrogate exactly the gaps that exist in your ERP-based controls. Take a closer look at your environment. Chances are there are millions to be saved in reduced waste and, even more importantly, great opportunities to detect patterns that help you unlock future performance.

What are you waiting for?
Get insight into your ERP process health, compliance risk & financial exposure

Do you know where your ERP is leaking? Let us help.

ACL’s comprehensive platform can help you get oversight of your critical ERP processes—so risky transactions and process control gaps aren’t overlooked and potentially undercutting your operational excellence, margins, or compliance.

For a free assessment of how your organization can better use technology to continuously monitor process risk, measure process health, protect revenue, and move the needle on performance, call 1-888-669-4225 or email info@acl.com.
About the Author:
John Verver

John Verver, CPA, CISA, CMC, is an acknowledged thought leader, writer and speaker on the application of technology, particularly, data analysis, in audit, fraud detection, risk management and compliance. He is recognized internationally as a leading innovator in continuous controls monitoring and continuous auditing and as a contributor to professional publications. He is currently an advisor to ACL, where he has also held vice president responsibilities for product strategy, as well as ACL’s professional services organization. Previously, John was a principal with Deloitte in Canada.

About ACL

ACL delivers technology solutions that are transforming audit, compliance, and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL’s integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best.

Visit us online at www.acl.com