DON’T NAVIGATE RISKY WATERS WITHOUT INTERNAL AUDITORS

Guidance on leveraging data analytics for risk management
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>Does this sound familiar?</td>
<td>3</td>
</tr>
<tr>
<td>WHAT'S RISK GOT TO DO WITH IT?</td>
<td>4</td>
</tr>
<tr>
<td>First, let’s be clear: Risk management is a management responsibility</td>
<td>4</td>
</tr>
<tr>
<td>INTERNAL AUDIT’S EVOLVING RISK ROLE</td>
<td>5</td>
</tr>
<tr>
<td>WHY BOTHER?</td>
<td>6</td>
</tr>
<tr>
<td>Redefining internal audit as a business necessity</td>
<td>6</td>
</tr>
<tr>
<td>RISK IS NOT A &quot;FOUR-LETTER WORD&quot;</td>
<td>8</td>
</tr>
<tr>
<td>SO, WHY AREN’T WE THERE YET?</td>
<td>9</td>
</tr>
<tr>
<td>ENTER RISK ANALYTICS TECHNOLOGY</td>
<td>10</td>
</tr>
<tr>
<td>So, how does data analytics technology fit in?</td>
<td>10</td>
</tr>
<tr>
<td>ASSESSING LOW, MEDIUM AND HIGH RISK</td>
<td>12</td>
</tr>
<tr>
<td>Supplement subjective evaluation with analysis</td>
<td>12</td>
</tr>
<tr>
<td>PRIORITIZING RISK WITH SCORECARDS &amp; HEAT MAPS</td>
<td>13</td>
</tr>
<tr>
<td>RISK-BASED AUDIT PLANNING</td>
<td>14</td>
</tr>
<tr>
<td>Let your data do the driving</td>
<td>14</td>
</tr>
<tr>
<td>STAYING CURRENT WITH CHANGING RISK PROFILES</td>
<td>15</td>
</tr>
<tr>
<td>EXAMPLE ANALYTICS FOR IDENTIFYING RISK</td>
<td>16</td>
</tr>
<tr>
<td>CASE STUDIES</td>
<td>18</td>
</tr>
<tr>
<td>City Of Gainesville</td>
<td>Protecting Taxpayer Dollars</td>
</tr>
<tr>
<td>Equinix</td>
<td>Covering Risk Across The Organization</td>
</tr>
<tr>
<td>Dublin Airport Authority</td>
<td>Managing Reputational Risk</td>
</tr>
<tr>
<td>6 STEPS OF APPLYING ANALYTICS FOR RISK ASSESSMENT</td>
<td>22</td>
</tr>
<tr>
<td>1</td>
<td>Build a profile of potential risks</td>
</tr>
<tr>
<td>2</td>
<td>Test data for possible risk indicators</td>
</tr>
<tr>
<td>3</td>
<td>Improve the process by implementing continuous analysis</td>
</tr>
<tr>
<td>4</td>
<td>Review results</td>
</tr>
<tr>
<td>5</td>
<td>Expand the scope and repeat</td>
</tr>
<tr>
<td>6</td>
<td>Report</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>26</td>
</tr>
</tbody>
</table>
INTRODUCTION

Does this sound familiar?

“Risk wah wah wah risk wah. Wah wah risk.”

− Miss Othmar, Peanuts Comics

There’s an ocean of information out there about risk. You’re likely already feeling the pull of the tide for internal audit to be more consultative and assume a stronger focus on risk management. As organizations navigate increasingly complex business environments, audit’s role is evolving and risk acumen is vital. But what does it mean in practical terms for your internal audit team?

Internal audit departments are in a unique position to help business leaders comprehend and navigate risk. Traditional assurance roles are expanding to encompass fraud and risk management, and internal audit is expected to play a more active role in assessing higher-level risks in an organization.

However, the problem with focusing more on risk is that you stop paying attention to things that have been deemed to be risk-free—and that assessment could be wrong, causing you to miss something significant. Or, conversely, you may recommend excessive risk mitigation and be misaligned with corporate strategy, thereby decreasing your relevance and reducing the value you provide to your organization.

Internal audit has access to extensive insight into the business via risk and control analytics technology. How can this wide view of the organization and business processes be leveraged to help pinpoint areas of risk for management? And how do you become more efficient and effective at pinpointing risk assessments?

In this eBook, we’ll outline how to leverage data analytics to test the controls designed to mitigate risk, identify areas where risk is not known, and become more efficient at managing low-risk areas.
First, let’s be clear: Risk management is a management responsibility

Internal audit’s role is to provide assurance around risk management. Have we identified the key risks to our organization? Do we have processes, controls and strategies in place to manage or mitigate that risk?

Internal audit departments already play a critical role in safeguarding organizations from loss and providing assurance around business activities. **There is no better place for organizations to look than to their internal audit function for a cross-departmental view of risk.**

Within the COSO-based risk management framework, management’s role is to do a top-down risk assessment for their organization and identify risks that are likely to negatively impact their objectives. Appropriate controls (be they IT-based automated controls or policy-enabled manual controls) can then be put in place to mitigate those risks. While this is a management activity, internal audit departments are a key component in effective governance and can contribute significantly to improving overall risk management assurance.

Furthermore, successful internal audit departments have a unique understanding of business processes and the ability to analyze the transactional data that they generate. This unique mix of business and IT domains enables internal audit to evaluate the operating effectiveness of these processes and the internal controls that have been put in place to mitigate business risks.

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, controls, and governance processes.”

The Institute of Internal Auditors (The IIA), *Standards and Guidance*
Prior to the economic downturn following the 2007-2008 financial crisis, many organizations were focusing their governance, risk management and compliance (GRC) activities on evaluating risks in their financial controls for compliance requirements such as Sarbanes-Oxley (SOX) or similar legislation.

But, the tides changed. With the downturn, the tide swung back to pre-SOX days. And since then, there has also been giant leaps forward in the availability of data. Operational risks are again keeping executives up at night and now remain the central focus of effective GRC strategies. There’s increasing pressure on organizations to make better, more informed decisions and to gain greater insights into the risks to performance. That means more pressure on internal audit departments to provide heightened levels of insight into organizational risk.

With that has come a shift in the risk management role played by internal audit, and the role expected to be played in the future.

**ROLE DESCRIPTION**

<table>
<thead>
<tr>
<th>ROLE DESCRIPTION</th>
<th>Current Role</th>
<th>Future Role</th>
<th>No Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Informally provides consulting and advice on risk management practices.</td>
<td>77%</td>
<td>14%</td>
<td>9%</td>
</tr>
<tr>
<td>2. Is the catalyst in forming risk management.</td>
<td>48%</td>
<td>14%</td>
<td>38%</td>
</tr>
<tr>
<td>3. Has active participation in implementing risk management.</td>
<td>45%</td>
<td>20%</td>
<td>35%</td>
</tr>
<tr>
<td>4. Participates as part of a formal risk management function.</td>
<td>43%</td>
<td>30%</td>
<td>27%</td>
</tr>
<tr>
<td>5. Provides independent assurance on risk management.</td>
<td>40%</td>
<td>35%</td>
<td>25%</td>
</tr>
<tr>
<td>6. Assists and advises a separate risk management function.</td>
<td>28%</td>
<td>21%</td>
<td>51%</td>
</tr>
</tbody>
</table>

*Figure 1: Current and future expected role of internal auditors in risk management. The Institute of Internal Auditors Research Foundation, Internal Auditing’s Role in Risk Management*
Redefining internal audit as a business necessity

Why take on more, you ask?

The IIA is calling for a self-assessment on the profession itself. Do internal audit departments support their organization’s big picture goals? What value does internal audit provide? Is internal audit regarded as relevant? With an increasing focus on risk throughout most industries, internal audit departments are, fortunately, well-poised for demonstrating their relevance and the value they provide to any organization. It’s time for internal audit to embrace its unique position and demonstrate the critical role it plays.

“Relevant internal auditors are regarded by their stakeholders as indispensable assets and as professionals who are tirelessly committed to helping the organization achieve goals by providing independent, objective, and candid audits stemming from insightful, dynamic assessments of risk. I urge all internal auditors to mitigate their risk of obsolescence by moving quickly to self-assess how they measure up against this relevance yardstick.”

− Denny Beran, CIA, CCSA, CPA, CFE, Chairman of the Board, The Institute of Internal Auditors

Quoted in “Assess our relevance,” Internal Auditor Magazine.
"Age of integrity"

The business owns the integrity. Internal audit’s role is to help the business identify the risks.
What many forget is that not all risk is bad. A complete absence of business risk virtually guarantees limited growth. Taking risks within your organization’s risk tolerance and risk appetite can help your organization grow and achieve your goals.

You need to understand your organization’s risk appetite before you can audit it.

“The recent spate of business crises and our organizational responses to them have highlighted a surprising misconception: that risk is the opposite of reward. It is not; loss is the opposite of reward. Risk simply represents the possibility that a loss or reward will occur.”

— Shayne Gregg, Partner, Enterprise Risk, Deloitte,
“The New Chief Audit Executive: Leadership in the risk intelligent organization”
Some common obstacles that get in the way of more frequent oversight of high-risk business processes include:

**Lack of availability of resources**
There just aren’t enough audit staff to increase assurance and value-add services and there isn’t enough money to hire more.

**Sheer volume of business transactions**
It is time-consuming and difficult to scrutinize the enormous volume of data from complex, modern business applications that process all that data.

**Communication challenges**
Where internal audit has the ability to identify control breaches or indicators of risk, how can this be communicated to management?

The goal is to make these processes integral to risk assessment and audit activities, and to make them sustainable and repeatable. How do you do that? This is where data-driven technology takes the helm.
So, how does data analytics technology fit in?

Internal auditors can use analytics to test the operating efficiency and effectiveness of the controls that are created by management to address risk, as well as to identify areas where risk is not known.

How does technology, specifically risk and control analytics technology, directly support the more detailed risk assessment process for auditors?

Use risk analytics to determine where to focus audit attention. Consider using a risk scorecard and heat map to assist with this process.

Once an area has been selected for internal audit, the first step may be to perform an overall analytics review of activities within an area to assess more specific risk points that warrant detailed audit investigation. For example:

» Why are overtime amounts significantly higher in one region than the norm?
» Why within one branch are very large volumes of expense transactions occurring just under the threshold where additional approval is required?

A drill-down approach to risk assessment can be used to drive development of a specific audit program and identify those areas that need greatest audit focus.

Once this has been assessed within an audit program, consideration can be given to determine whether data analysis technology can be used to improve efficiency and effectiveness of a given audit procedure.

By using technology to test 100% of transactions, an auditor is best able to determine that controls are effective and risks mitigated.

Leveraging analytics to address lower-risk areas enables the reallocation of key resources for higher-stakes risk.

“Successfully addressing these demands requires a combination of leadership, processes and tools from internal audit. These include, most prominently, a stronger role in boosting the organization’s overall risk management capabilities as well as greater use of automation and analytics, such as continuous auditing, to deliver greater efficiency and effectiveness.”

— Shayne Gregg, Partner, Enterprise Risk, Deloitte,
“The New Chief Audit Executive: Leadership in the risk intelligent organization”
“Basing audit plans on an annual snapshot of risk is like relying on a security camera that films once a day for five minutes.”

− Richard Chambers, “Responding to Change”, Internal Auditor Magazine
Just the facts, ma'am: A real-world example of how data helps remove subjectivity

Acme Inc. had quite a few people with active IDs in their SAP financial reporting system who were no longer employed with the organization—a risk that many organizations face. Acme felt the risk was low, because: a) Acme took people's swipe cards when they left, so they couldn't enter the building, and b) Acme removed people’s network access, so they couldn’t log in to access SAP.

However, Acme’s external audit firm argued that the risk was high because people could have potentially shared passwords and could possibly remotely access the system.

Acme and their external auditors could have spent weeks debating and not gotten anywhere, because both of the risk arguments were based on subjective assumptions.

Instead, using a fairly simple set of analytics, they were able to quantify the exposure in a way that no one could argue with.

First, they ran a test to see, of the former employees that still had access to SAP, if there were any IDs that were used after the date of employment termination (which tells us the ‘likelihood’ of this risk). Second, they also were able to look at the activities undertaken by those IDs (which tells us the ‘impact’ of this risk).

Now they could talk facts instead of assumptions, and agree together upon an appropriate course of action.

Supplement subjective evaluation with analysis

Controls exist to address risks, minimize surprises and pitfalls, and help an organization achieve its objectives. Many risks happen every day, but are inconsequential. Others are a big deal. With so many controls and so many areas of an organization, it's only logical that you should look at the ones that can bite you. In other words, look at the risks that have a high impact on the organization and/or a high probability of occurring.

The challenge is that “impact” and “probability” are highly subjective. Ask three different people and they’ll have three different opinions. Analytics can help to quantify risk, and help eliminate the subjectivity around topics like “likelihood” and “impact.” By analyzing 100% of the data, we can quantify this risk in a way that wasn’t possible before. In fact, we can eliminate the subjectivity of the “how likely is this?” conversation by saying “last year this happened X% of the time.” And in some cases we can quantify the bottom line impact with “given both the direct costs of this type of error and the indirect costs of fixing it, the cost is roughly $XXX,XXX.”

Analytics can help make a low/medium/high determination. This doesn’t apply to all risks (e.g., risks that have not impacted us but may in the future, such as the likelihood of a water shortage in a key supplier region). But, where possible, analytics can be used to supplement the subjectivity of the risk assessment process, and add facts to areas where we also need to make educated guesses.

“Internal audit seems to be taking a pragmatic approach to the challenge of reduced budgets and has adopted a targeted approach to managing the risks: 72% are narrowing audit scope to target key risks, 33% are using questionnaires to identify higher-risk entities, and 29% are conducting fewer local business unit visits.”

— Ernst & Young, “Driving ethical growth—new markets, new challenges”, 11th Global Fraud Survey
As you begin to use analytics to measure risk in your organization, at some point you may find that the more data you collect, the more challenging it may be to make sense of that data. Ultimately your objective from this exercise should be to help answer the question “where should I focus my audit attention next?” Here’s where a risk scorecard and risk heat map can come into play.

The concept of a risk scorecard is simple. Using a scorecard, you aggregate the results of each risk indicator that is important to you to come up with a risk “score.” Depending on how you choose to aggregate your risks (e.g., by location, by division, by manager, etc.), you can then begin to compare these segments relative to one another and quickly highlight risky areas, as well as those where risk is suddenly changing. In a more advanced version of a risk scorecard, you can even weight these risks given their overall importance in your risk landscape to create a risk heat map.

While it can take some effort to get your model right, the outcomes can be a game-changer when it comes to prioritizing audit resources. In these heat map examples to the right, for example, you don’t need to know a whole lot about this organization to quickly see that the entity specified by the red bubble has something very different happening and probably warrants some attention.

Figure 1: Example risk heat maps in the ACL Platform
Let your data do the driving

Use data analytics during your next audit planning phase with an eye for assessing risk through data-driven indicators.

Focus on today’s and tomorrow’s risks. Effective use of analytics helps internal auditors identify changes in internal processes and provide timely insight into the business. With data analysis, you can monitor business risks to ensure you are auditing today’s risks, not just those identified yesterday.

Depending on your organization and the industry that you’re in,

- Revenue by location, division or product line
- Revenue backlogs (by value and age)
- Personnel changes in key positions (legal, finance, R&D)
- Volume of manual journal entries or credit notes
- Aging A/R balances or inventory levels
- Vendor management (number of vendors, transaction volume)
- P-Card vs. PO procurement
- Average days for customer payment
- Travel and entertainment expenses reimbursement
- Fraud risk

Prioritized risk: Do less with less

“It’s not about doing more—it’s actually okay to do less, as long as the less is comprised of more impactful audits.”

– Rod Winters, Microsoft, speech at The IIA GRC Conference

Audits don’t need to be cyclical, they just need to address where the risk is.

A focus on risk can intelligently determine where the resources go. A risk-based audit plan executed with the right technology to improve efficiency can allow an audit team to do less with less, while providing a higher level of assurance.
With a top-down approach, management identifies the risks. What internal audit needs to ask, in the case of compliance risks for example, is: do we have sufficient controls to prevent regulatory breaches? Or in the case of financial risks: an internal auditor can look at the volume of manual journal entries or credit notes (a high occurrence of either may be an indicator of fraud risk, or the risk of errors being made by manual human intervention).

There are many different types of risk. To understand your risks, you need to understand your business. The internal auditor needs to understand operational, reputational, financial, fraud and other risks relevant to the business and identify opportunities for testing. Using analytics to look at 100% of the transactions provides a fairly precise understanding of the risk.

Rather than thinking of a control as fixed, consider that the control is only relevant inasmuch as it addresses a risk. If we’ve looked at 100% of the transactions and we haven’t seen evidence of the risk, it can only mean one of two things:

1. The control is working, or
2. Even if the control isn’t working, the risk is low and therefore we may not need a control here.

The results of this analysis can be used to periodically review controls to assure risk management and to make adjustments as needed.

Some typically high-risk areas (by industry):

**Manufacturing:**
Vendors, supply chain, inventory

**Banking:**
Loans, debt liability, assets, general ledger

**Healthcare:**
Medicare billing fraud

Solution Demo:
ACL Inspirations

Description:
View hundreds of risk scenarios and tests collected from ACL initiatives worldwide. View analytics ideas by industry:

- Manufacturing
- Banking
- Healthcare
... and more!

https://accounts.aclgrc.com/inspirations
To determine what to test with data analytics, consider: What should your data look like if a mitigating control is in place and working? And what might be anomalous in the data if a risk is not being successfully managed? Also, be aware that what you don’t know is risky. Think about how reliable your master data is—bad data is in itself a risky scenario. Let’s have a look at some potential risks and analytics testing opportunities in some example business processes.

<table>
<thead>
<tr>
<th>Travel and entertainment: Duplicate reimbursement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Scenario</strong></td>
</tr>
<tr>
<td>Employees may make charges on a corporate procurement card, and in addition to running these through the P-card payment process, also submit these for cash reimbursement as part of the T&amp;E process.</td>
</tr>
<tr>
<td><strong>Challenge</strong></td>
</tr>
<tr>
<td>T&amp;E payment management systems are oriented towards timely capture and processing of employee claims and are rarely integrated with P-card processing and payment systems.</td>
</tr>
<tr>
<td><strong>Analytic Solution</strong></td>
</tr>
<tr>
<td>Using both exact matching and similar matching techniques, identify claims submitted for reimbursement on both corporate purchase cards and employee T&amp;E expense reports.</td>
</tr>
</tbody>
</table>
### Travel and entertainment (T&E): Supplier spend report (e.g., hotels)

<table>
<thead>
<tr>
<th>Risk Scenario</th>
<th>Challenge</th>
<th>Analytic Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees may not be using approved travel suppliers such as hotels and airlines, negating the impact of negotiated discounts with these suppliers.</td>
<td>Accumulating useful management information from the detailed T&amp;E expense data is often difficult to do.</td>
<td>Utilize the T&amp;E expense data gathered for control testing to generate key performance indicators and other summary information that has value to decision makers.</td>
</tr>
</tbody>
</table>

### Payroll: Ghost employees

<table>
<thead>
<tr>
<th>Risk Scenario</th>
<th>Challenge</th>
<th>Analytic Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll disbursements may be generated for fictitious employees.</td>
<td>Management is typically responsible for verifying employees, but there is a potential risk of management collusion.</td>
<td>Perform a variety of tests to detect potential ghost employees, such as multiple disbursements to the same bank account, or employees with no system activity.</td>
</tr>
</tbody>
</table>

### Anti-bribery regulations, e.g., FCPA: Suspicious vendors and customers

<table>
<thead>
<tr>
<th>Risk Scenario</th>
<th>Challenge</th>
<th>Analytic Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Foreign Corrupt Practices Act (FCPA) imposes penalties on US companies who engage in corrupt practices with foreign businesses or government entities.</td>
<td>Potential problems can be hidden within large volumes of transactions, but only a single violation can result in penalties.</td>
<td>Alert compliance teams to suspicious vendors using techniques, including comparison of vendor name and address details against external prohibited vendor lists (GSA, OFAC), Politically Exposed Persons databases, payment method and country of origin.</td>
</tr>
</tbody>
</table>

### Payroll: P2P examples (split purchase orders)

<table>
<thead>
<tr>
<th>Risk Scenario</th>
<th>Challenge</th>
<th>Analytic Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees are circumventing individual purchase authorization limits by splitting a single purchase activity across multiple POs.</td>
<td>No automated way of knowing when two or more POs together exceed an authorization limit. Manual review of POs is not practical.</td>
<td>Identify cases where multiple POs relate to the same purchasing activity and direct to an appropriate individual for investigation and follow-up.</td>
</tr>
</tbody>
</table>
Let’s look at some examples of how a few organizations are leveraging risk and control analytics technology to manage their risks.
Organization Profile

City of Gainesville is the largest city and county seat of Alachua County, serving as a cultural, educational and commercial center for the north central Florida region. The City Audit Team reports to elected officials and is responsible for identifying and flagging risks in the best interests of the public.

Challenges

» The risk of making decisions that are not in the best interest of taxpayers—resulting in revenue loss, exceeded budget allocations or violating federal or state laws.

» Using manual workpapers.
» Slow internal processes
» Lack of standardized templates.

Technology Solution

ACL GRC Platform + Analytics module

Benefits & Results

Automated workpapers
Replaced time-sucking manual processes.

Data-driven risk management
Protecting public funds and improving services.

Access data anywhere
Secure cloud-based technology.

Do more with less
Increased team performance.

✔ Workpapers are automated and moved into the cloud for secure, easy access.
✔ Standardized templates are customized to better suit municipal government auditing standards, Yellow Book.
✔ Also using the platform to conduct COSO internal control surveys and build storyboards to visualize risk profiles.

“I needed something I could get up and running quickly with a very small staff. My solution was ACL GRC and I also bought ACL Analytics, of course. And life has changed significantly since that time.”
Company Profile

Equinix connects the world’s leading businesses to their customers, employees and partners inside the most interconnected data centers. Operating in 40 markets worldwide, Equinix works with mostly major financial institutions and their trading partners, the major ISPs and large enterprises.

Challenges

» Working in silos without a comprehensive view of risk.
» Spending large amounts of time putting together risk maps and reports for the board and management.
» Disparate information sitting in emails and documents across multiple departments.

Technology Solution

ACL GRC Platform + Analytics Server module

Benefits & Results

Enterprise-wide risk oversight
Seamlessly integrated and flexible.

Cross-functional collaboration
Single, unified performance.

Aggregate, data-driven reporting
Reliable, data-driven enterprise risk management.

Minimal IT burden
Easy to implement, easy to learn.

✔ The ACL Platform gives teams an overarching view of governance, risk and compliance programs across the whole organization.
✔ Information is now shareable inter-departmentally on the same platform, for better oversight and risk mitigation.
✔ Risk activities are now integrated from start to finish.
✔ Quick and easy implementation, seamlessly integrated yet flexible.

“It doesn’t require much IT support, if any at all. We just found it was a very cost-effective approach compared to some of the others. And it provided the integration capabilities and the flexibility that we needed. It gives us that overarching umbrella for how we look at governance, risk and compliance.”

− Rod Verhulp, VP of Finance

Watch: Expert Advice Video

Watch Case Study: Enterprise Risk Management at Equinix
Company Profile

Dublin Airport Authority (daa) is a state-owned organization that operates the two largest airports in the country.

Operating on a completely standalone commercial basis, daa doesn’t receive any extra funding and receives all income from aeronautical activity and commercial business activities.

Challenges

» Managing various security and health and safety risks—a top priority because they could result in significant fines or impact airport operations.

» Inordinate amounts of time spent updating, re-editing and sharing documents—cutting into audit and risk activities.

Technology Solution

ACL GRC Platform + Analytics Server module

Benefits & Results

Quick set-up

Up and running within days.

Data-driven

Analytics are integrated into workflow.

Easy to use

User-friendly and intuitive, without needing external support.

More time

Cut down the administrative burden of managing spreadsheets and docs.

✔ The ACL Platform has helped streamline inefficient processes and save time on administrative work.

✔ Analytics testing is integrated into workpapers management—in one system.

✔ Increased output of work with less bodies.

“We’re carrying out a significant amount of extra work that we weren’t doing a couple of years ago. We’ve also saved significantly on headcount—so I mean we’re doing more work with less bodies, and we’re achieving much deeper penetration and the work is so much more insightful. So it’s been of immeasurable benefit.”

− Kevin Goulding, Group Head of Internal Audit, daa
So, where do you start?

Step by step, here’s a basic framework of how you can begin to apply data analytics to assess risk and controls in your organization...

While generic software like spreadsheets can get you started, purpose-built risk and control analytics technology will support more complex and valuable testing, issue management and remediation, and long-term sustainability.
Build a profile of potential risks

- Develop a profile of potential risks as part of a risk assessment.
- Consider using a risk scorecard and risk heat map to prioritize.

Test data for possible risk indicators

- Include ad hoc testing in addition to more formalized or regular tests.
- Consider the spectrum of automated testing, ranging from ad hoc to repetitive through to continuous, where appropriate.
Improve the process by implementing continuous analysis

- Use continuous analysis to test and validate the effectiveness of your controls—on a timely basis.
- Provide management with immediate notification of red flags.
- Create processes for control remediation.
- Implement continuous analysis on a comprehensive basis across business process areas.

Review results

- Investigate patterns and indicators that emerge from your analyses.
- Quantify the risk.
- Identify and target high-risk areas.
- Consider the use of risk monitoring dashboards.
Expand the scope and repeat

- The process of building a profile, testing data, improving controls and reviewing information needs to be done on a regular basis.

Report

- Make recommendations on how to tighten controls or change processes to reduce the likelihood of non-compliance.
- Follow up and see if those recommendations have been acted upon and if they have had the desired effect.
- Communicate, communicate, communicate. Impart “tone at the top” to the organization.
- Why? Because unresolved exceptions have a negative impact on the organization.
CONCLUSION

We've looked at how to start applying data analytics to risk assurance. What's next?
Use risk and control analytics to assist in assessing risks in your organization; it will help drive increased efficiency into your audit work and identify data-driven indicators of emerging risks.

1. Organizations that have gained the most from this process are those in which internal audit leadership at the CAE level has been a strong advocate.
2. Take your maiden voyage by applying the six steps to a risk area in your organization.
3. There’s a lot to do, but you can always find help. You’re now charting a course towards greater, and much more efficient, risk assurance.

If you don’t have the time or the in-house expertise to figure out where data analytics fits into your organization’s risk assurance, it may be time to talk to someone who can help.

Contact an ACL expert for a free consultation on how you can get the most out of data analytics.

info@acl.com | 1-888-669-4225
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.

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 15,000 customers around the globe—including 89% of the Fortune 500—tells our story best.

Visit us online at www.acl.com