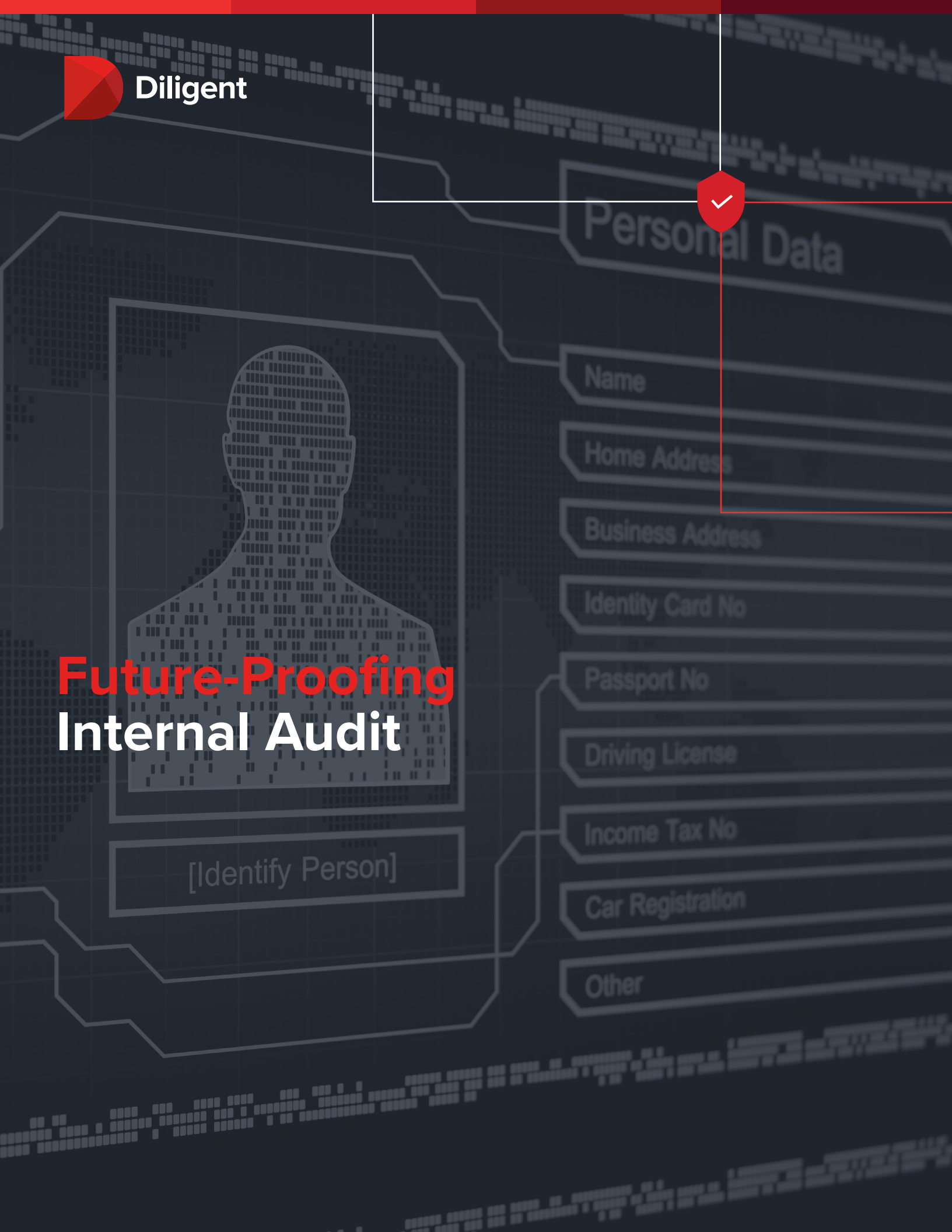
Diligent



Future-Proofing Internal Audit

Contents

Internal Audit's New Toolkit

The risk profiles of organizations are becoming more complex and difficult to manage. To remain relevant, internal audit has to respond to these challenges and deliver strategic insights, not just assurance.

Traditionally, internal audit functions focused on compliance and internal control systems. But to be a partner to the C-suite and board, internal audit must understand the organization's key risks and proactively identify emerging risks.

To meet these demands, internal auditors have to start using new tools and technologies like artificial intelligence, machine learning and robotic process automation, and to make better use of data analytics to drive strategic decisions.

Diligent

Technology Is Key

Do you have the tools to help your organization identify and manage the increased risks that come with the new digital economy?

Technology adoption is the main driver behind future-proofing the internal audit function. While people and processes form the foundation, technology is the accelerator that internal audit needs to be more innovative and effective.

A study by Protiviti[1] revealed that adoption of nextgeneration internal audit capabilities is still in its infancy. However, 71% of chief audit executives (CAEs) believe their audit functions have high impact and influence—and they plan to increase their investment in innovation in the next few years.[2] Going forward, CAEs need to take the lead in getting this fundamental technology transformation on the audit committee's agenda.

This eBook explores technologies that CAEs and internal audit teams must adopt to future-proof their audit functions and increase efficiencies.

[1] **Protiviti,** 2019, Embracing the next generation of internal auditing
[2] **Deloitte,** 2018, The innovation imperative: Forging internal audit's path to greater impact and influence

Digitalization & Digital Transformation

Digitalization isn't a business buzzword—it's about using technology to improve performance and create new business opportunities.

With so many advances and changes in corporate and consumer technology, digitalization now involves integrating many different types of technologies. These include cloud computing, mobile, big data analytics, machine learning, artificial intelligence (AI) and the internet of things.

This drive toward digitalization and automation—along with investments in robotics, machine learning, AI and advanced analytics—is a new form of business transformation commonly referred to as Industry 4.0.[3]

And nearly all audit teams are taking advantage of these technologies to some degree. A recent Protiviti report revealed that 76% of internal audit groups are going through a digital transformation.[4]

For most large organizations today, it's not a question of if digital will disrupt their business, but when.

Even when executives are aware of emerging technologies that have disruptive potential, it's often difficult to determine how that disruption will impact the organization.

But this isn't news: digital transformation has been happening for many years. Big changes in past decades included the introduction of automated workflows, electronic workpapers and dedicated audit management systems. When these technologies first emerged, they were seen as disruptive, but now they're standard practice. Getting current digital technologies to that same state of standard adoption is the goal of CAEs and audit committees, who drive the pace of change.

[3] **KPMG,** 2019, Top 20 risks in internal audit before 2020
[4] **Protiviti,** 2019, Embracing the next generation of internal auditing


Diligent

Internal Audit's Increasing Cybersecurity Role...

Cybersecurity risk is growing and evolving globally, and so is internal audit's role in mitigating it.

According to the 2019 audit capability survey, cybersecurity risk is the #2 priority for CAEs.[5] And with major cyberbreaches appearing in news headlines more frequently, cybersecurity is on internal audit's radar more than ever.

Internal audit works to manage cyberthreats by providing independent assessments of existing risk and helping the audit committee and board understand and address that risk. Deloitte[6] reports that many organizations recognize the need for a third line of cyberdefense—an independent review of security measures and performance undertaken by internal audit. Cybersecurity isn't the sole responsibility of the security or IT teams—it impacts and involves all business areas. In a traditional siloed approach, each department treats risks independently. There's no common language or framework to examine cyber risk holistically. Focusing on risk removes these silos while making it possible for business process owners to prioritize and act on findings.

By using a common risk language across departments and with individuals in all three lines of defense, an auditor can truly evaluate the effectiveness of a cybersecurity program and get an accurate picture of where the organization stands.

A risk-based approach also lets internal audit meet expectations set by the board and identify major tactical and strategic gaps in cybersecurity governance.

COMMON INTERNAL AUDIT CYBER RISK ACTIVITIES

01 Independently evaluate preventive and detective measures related to cybersecurity.

02 Evaluate IT assets of privileged-access users for standard aspects like security configurations, malicious software and data exfiltration.

03 Track remediation diligence.

04 Conduct cyber risk assessments of service organizations, third parties and suppliers.

[5] **Protiviti,** 2019, Embracing the next generation of internal auditing
[6] **Deloitte,** 2017, Cybersecurity and the role of internal audit

Diligent

Performing Cyber Risk Assessments

Only half of internal audit leaders indicated their groups have conducted cyber risk assessments.

Among those that have conducted cyber risk assessments, three-quarters have developed a cyber audit plan based off the assessment.[7]

By performing a comprehensive cyber risk assessment, internal audit can present objective evaluations and findings to the audit committee and board members, and use those findings to develop a broad internal audit plan that includes cyber risk.

A cyber risk assessment can also be structured to generate a list of cybersecurity gaps and provide the organization with a road map for short- and long-term remediation activities.

CYBER RISK ASSESSMENT STEPS

1

Characterize the system (process, function or application)

Answer the questions: What is it? What data does it use? What vendors are involved? What is the data flow? Where does the information go?

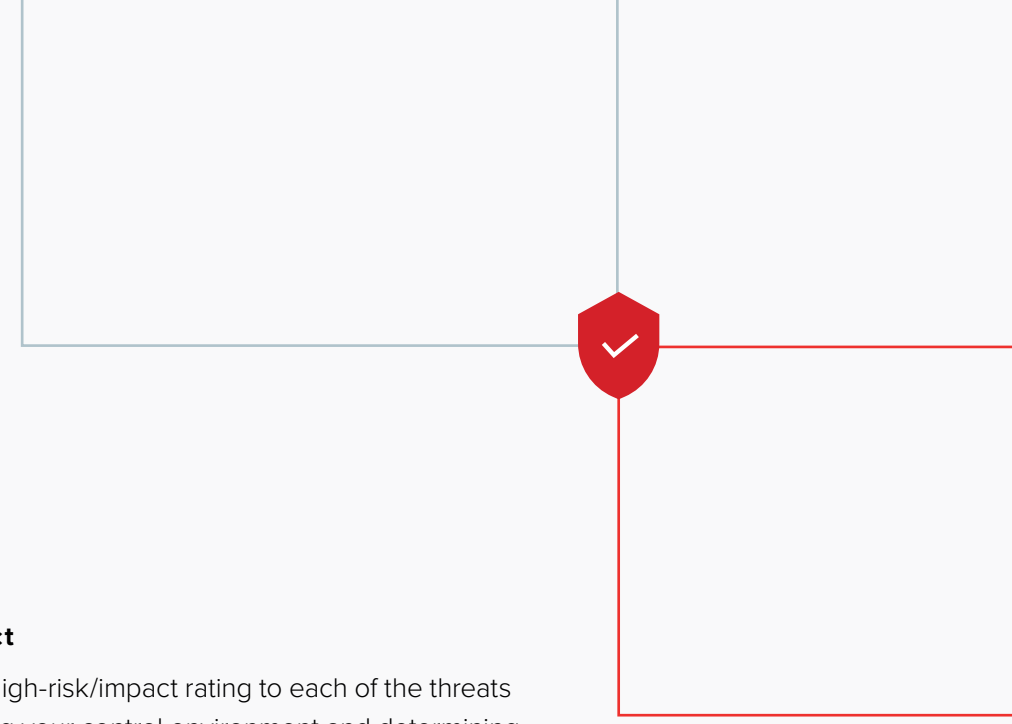
2

Identify threats

Threats will vary within each organization, but common ones include:

- Unauthorized access
- Misuse of information by a privileged user
- Data loss
- Service disruption

[7] **Deloitte,** 2018, The innovation imperative: Forging internal audit's path to greater impact and influence



3 **Determine inherent risk & impact**

Apply a standard low-, medium- or high-risk/impact rating to each of the threats you've identified (without considering your control environment and determining a "what-if" scenario where the risk happens).

4 **Analyze the control environment**

Identify threat prevention, mitigation and detection controls (e.g., controls for user provisioning, administration, data center security, business continuity) and their relationship(s) to identified threats.

5 **Determine a likelihood rating**

Assess the likelihood, within your control environment, of any given exploit or risk actually occurring within your organization (again, using a low, medium or high rating).

6 **Calculate your risk rating**

The risk rating equation is pretty simple: impact (if exploited) x likelihood (of exploit in the control environment). Using a scoring system of low, elevated and severe will help with determining the levels of individual risk rating scores, which is the next step.

7 **Prioritize risks**

Use your preferred risk ratings/scoring system to prioritize your risks in order of magnitude.

8 **Document results in a risk assessment report**

Produce a risk assessment report to support management in making decisions on budget, policies and procedures.


Diligent

How Internal Audit Can Help Mitigate Cyber Risk

As the third line of defense, internal audit and has a big role to play in addressing cyber risk.

WHAT STEPS CAN INTERNAL AUDIT TAKE?

- Work with management and the board to develop a cybersecurity strategy
- Improve the organization's ability to identify, assess and mitigate cybersecurity risk
- Heighten awareness and knowledge on cyberthreats and ensure that the board remains highly engaged with cybersecurity matters
- Integrate cybersecurity risk into the audit plan
- Evaluate the cybersecurity program against established frameworks (e.g., PCI DSS, NIST)
- Share with stakeholders that the strongest prevention is a combination of awareness, training, vigilance and technology
- Emphasize that cybersecurity monitoring and cyberincident response should be a top management priority
- Address any IT/audit staffing and resource shortages, as well as any supporting technology/tools that are needed

Diligent

Machine Learning & Robotic Process Automation

In recent years, emerging technologies like artificial AI, machine learning and robotic process automation (RPA) have all been impacting internal audit.

Machine learning and RPA can transform the audit function. RPA uses technology to automate a process like collecting data, while machine learning uses algorithms to analyze data and make correlations and predictions.

Let's take a look at some of the current and future applications of machine learning and RPA in internal audit.

Machine Learning

Machine learning is a category of AI that's based on the idea that machines can be taught to learn similarly to humans.

Machine learning can use models to perform data analysis, understand patterns and make predictions. It's still an emerging technology in internal audit, and it's primarily in the research and development phase.

Several of the larger CPA firms are creating machine learning systems, and smaller firms will be able to benefit from the technology as it improves.

While its applications may be relatively immature, the potential benefits of this technology for cutting-edge internal audit teams are exciting. Here are a few real-life examples.[8]

EY

EY is using machine learning to detect anomalies and fraudulent invoices. The company revealed that the technology is 97% accurate at identifying faulty invoices. The technology has helped EY significantly minimize its risk exposure when it comes to violating sanctions, anti-bribery regulations and other aspects of the Foreign Corrupt Practices Act.

DELOITTE

Deloitte is using machine learning to review hundreds of thousands of legal documents to identify change control provisions as part of a client's sale of a business unit. This process used to keep dozens of employees occupied for half a year, but now, a team of eight takes less than a month to complete it, freeing up staff to focus their time and energy on other work.

ASSURANCE DEPARTMENTS

AI is being used to increase efficiencies and reduce manual tasks. Instead of performing random sample-based testing, AI can be used to analyze the entire general ledger and identify high-risk transactions.

Clearly, AI can drastically increase efficiencies, reduce manual tasks and free up audit staff for critical thinking. Through the process of learning from exceptions, and auditors' conclusions/judgments, machine learning eventually becomes more accurate as it learns to better identify exceptions in the data.[9]

For a deeper dive on machine learning's applications in GRC, read our eBook *Machine learning essentials.*

[8] **The CPA Journal,** 2019, Machine learning in auditing: Current and future applications
[9] **International Federation of Accountants,** 2018, Why accountants must embrace machine learning

Diligent

Robotic Process Automation

With automation technologies advancing quickly and early adopters demonstrating their effectiveness, RPA is starting to gain some traction in internal audit functions.[10]

RPA is a much more accessible form of AI. It involves the use of software robots to automate repeatable processes with rules-based systems. These robots are easy to configure, require little IT or data science expertise, and can be quickly trained and deployed to automate manual tasks.

RPA & INTERNAL AUDIT

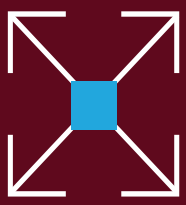
By using automation, internal auditors can get more done with the same resources, including:

- Improving the quality and consistency of internal audit processes
- Improving the efficiency of planning, testing and reporting activities
- Increasing coverage and frequency of testing
- Expanding the audit scope for individual audits
- Moving from limited sample testing to full population testing
- Managing labor and geographical constraints

RPA USES IN INTERNAL AUDIT

- Risk assessments. Robots can help classify risks using predefined rules, data points and trends for risk assessment. This allows for quicker identification of high-risk areas and transactions.
- Assistance in testing controls. Robots can test entire populations of data—not just samples—which increases confidence in controls and frees up internal auditors' time.
- Collecting data and processing high-volume transactions. Robots can process large volumes of data faster, more efficiently and with greater accuracy than manual or spreadsheet-based methods.
- Data gathering and cleansing. Robots run custom analytics, like extracting the data for use by internal auditors, including validation for completeness of fields, comparisons and duplications.

[10] **Deloitte,** 2018, Adopting automation in internal audit



PwC estimates that 45% of work activities can be automated & this automation could save organizations up to $2 trillion in global workforce costs.[11]

[11] **PwC,** 2017, Robotic process automation: A primer for internal audit professionals

Diligent

Data Analytics

Data analytics is one of the leading technologies shaping the future of internal audit.

This is supported by CAEs, who identified limited data use as one of the top 10 risks of 2018.[12] And, according to an article by Internal Auditor,[13] internal audit departments still aren't widely using data analytics and other valuable technology tools.

The problem is that many internal audit departments, especially those struggling with resourcing, don't know where to start. Protiviti surveyed more than 1,500 CAEs and found that internal audit departments are still trying to develop a formal methodology for integrating data analytics.[14] And many audit functions only use analytics tools as "point solutions" on a case-by-case basis, rather than as part of a broader strategic initiative throughout the entire audit process.

The survey notes that while 66% of internal audit functions that don't currently use data analytics plan to do so as part of the audit process within the next two years, 34% still have no plans to do so.

Embracing data analytics will be a core part of the future-forward internal audit department. Figure 1 shows a flowchart (adapted from PwC) detailing how an internal audit department could implement a data analytics program.

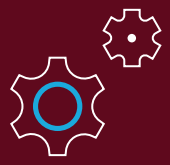
Not only does internal audit need to see data analytics as a standard part of their business functions—they also have to take an increased data governance role, driving the standards and policies around data collection and quality, and the formal management of data assets across the organization.

[12] **PwC,** 2017, Robotic process automation: A primer for internal audit professionals
[13] **Internal Auditor,** 2018, Out of step with analytics
[14] **Protiviti,** 2018, Internal audit capabilities and needs survey

FIGURE 1: DATA ANALYTICS PROGRAM IMPLEMENTATION FLOW

Information management

Analytics skills & tools



Data-oriented culture

01
Identify data sources

Review and identify data sources between source systems, reporting data and application-level data

02
Define frequency

Define data source required on an ongoing basis (daily, monthly, quarterly and one-time needs)

03
Repeatability

Develop both manual and automated processes to reduce the burden of gathering data

04
Define resources

Define concentric circles of core team, analytics champion and department-wide skill set uplift

05
Choose technologies

Identify capabilities and needs in terms of analytics, visualization, data management and monitoring solutions

06
Create training

Create programs and incentives to develop an analytical mindset and competencies

07
Develop methodology

Develop execution and quality standards for analytics across audit planning and controls testing

08
Create awareness

Ensure technology tools within the department align to methodology and support ability to track methodology adherence

09
Share wins

Define “success metrics” and communicate and share wins across the department to shift culture

Adapted from: PwC, 2018, Transforming internal audit through data analytics

Diligent

Internal Audit's Role In Data Governance

As data becomes an increasing part of our daily personal and business lives, strong digital and data governance is essential.

Data governance helps organizations comply with data security and personal information policies and regulations, and also ensures data accuracy, integrity and proper data management. The internal audit department of every organization should be involved in this process.

Organizations need trustworthy, clean, accurate and accessible data to remain competitive. For example, RPA relies on good data to efficiently and accurately process information. But if there is no overarching data governance guiding this process, the likelihood of poor data is much higher. The risk that new technologies won't operate effectively also increases.

The future-forward internal auditor needs to ask:

- Is data governance an area of focus within your technology audits this upcoming year?
- Are you confident about data controls—including those for security, privacy, access and accuracy—in the organization's use of new technologies?

Internal audit can't be involved in every project, and neither can other governance, risk and compliance (GRC) areas such as risk management or compliance. But if tied closely to the organization's digital/ innovation strategy, and if involved early in significant initiatives, internal audit can expand its risk coverage by helping to shape data governance. A data governance framework can guide the many projects that embed the same emerging technology for different use cases, improving the odds that control considerations get embedded too. Internal audit can then focus on testing to see that guidelines are followed and upheld. In a recent study by PwC, 40% of high-performing internal audit teams helped to establish the governance standards for the organization.[15] Are you ready to join that 40%?

[15] **PwC,** 2019, State of the internal audit survey

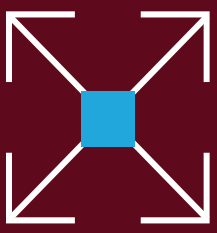
Diligent

Conclusion

While the skill of internal auditors and the right processes are a big part of the equation, emerging technology is the best way to future-proof internal audit.

It's not about replacing humans with machine learning or robotics, and internal auditors shouldn't fear this digital transformation.

Being a champion for these advancing technologies is actually a win-win situation for internal auditors. Work becomes more efficient, accurate and automated, and auditors have more time to focus on strategic initiatives and career development.



Ready to find out how Audit Management can help you add value, better manage your audit workflow & deliver strategic insights?

About Diligent Corporation

Diligent™ is the leading governance, risk and compliance (GRC) SaaS provider, serving more than one million users from over 25,000 organizations around the globe. Our modern GRC platform ensures boards, executives and other leaders have a holistic, integrated view of audit, risk, information security, ethics and compliance across the organization. Diligent brings technology, insights and confidence to leaders so they can build more effective, equitable and successful organizations.

For more information or to request a demo:

Email: info@diligent.com | Visit: diligent.com