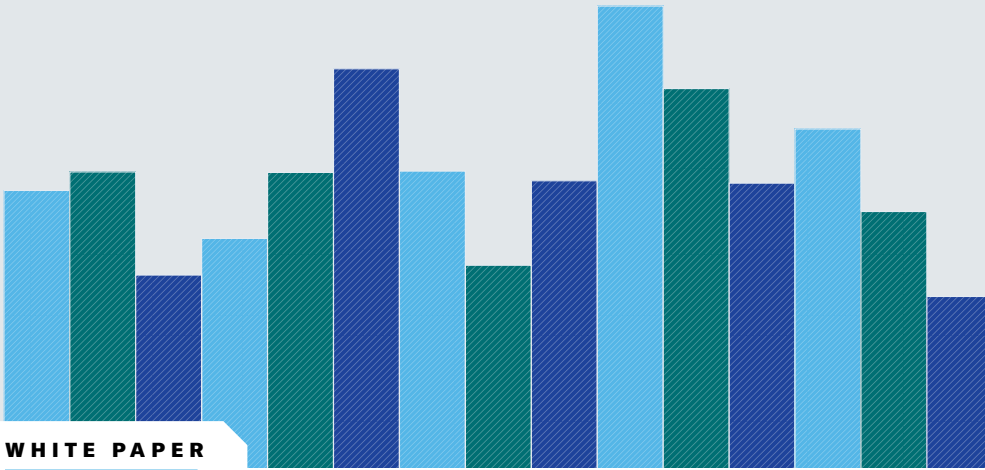Harvard
Business
Review

ANALYTIC SERVICES

Digitizing Risk and Compliance:

How AI Can Help Manage a Growing Challenge

Sponsored by

pwc

The way we do business has changed drastically. Businesses are more digitized and interconnected. The regulatory environment continues to expand. Organizations face more risk at an increased velocity. Altogether, this intensifies a need for integrated risk solutions to manage risk in an ever-changing business world.

Unfortunately, many organizations' risk systems aren't fit for this challenge. They're highly manual, or their tech solutions struggle to keep up with steady industry change and evolving risk. Yet many organizations continue with these outdated, inefficient systems instead of embracing modern technology equipped to handle modern challenges.

However, your business may need to change—too much is at stake not to. And while change may be difficult, it's also an opportunity. Take advantage of modern technologies, such as generative artificial intelligence (AI), to help accelerate your risk program and connect the dots of disparate risk areas.

To spearhead AI use, approach risk management change through these two perspectives:

1. Reinvent yourself. Get comfortable with AI so you can obtain an integrated, multi-dimensional view of processes, controls, risk, and regulations. Effective use will not only allow you to reduce the cost of compliance, but more importantly, it also will help drive valuable insights back to the business, and help meet the goals of regulations for your stakeholders. As we like to say at PwC, the process may be tech-powered, but it's human-led. Be that leader.

2. Enable business transformation. Establish an AI risk framework and governance model that allows for business innovation while safeguarding the enterprise. This balance enables companies to move swiftly while mitigating potential risks.

For any organization to flourish, they should embrace the future alongside its potential for risk, just as Harvard Business Review Analytic Services recommends in this white paper. AI alongside traditional technology can provide an integrated, multi-dimensional view of risk and regulations. We at PwC believe that wholeheartedly. In 2023, we made a $1 billion multi-year investment in generative AI. We've continued our commitment to this innovation as our own client zero, transforming our business at scale, across all our functions with the help of generative AI and implementing and operationalizing a responsible AI framework with digital tools.

Risk teams are critical to manage risk and enable necessary change. So don't just stand on the sidelines—change the way you view risk alongside us at PwC.

Vikas Agarwal
Financial Services Risk and Regulatory Leader
PwC

Tiffany Gallagher
Health Industries Risk and Regulatory Leader
PwC

John Sabatini
Cyber, Risk and Regulatory Clients and Markets Leader
PwC

Digitizing Risk and Compliance:
How AI Can Help Manage a Growing Challenge

Today's risk and compliance officers are responsible for monitoring a wide range of threats and interpreting an immense volume of regulations to help their organizations operate, compete, and thrive. Exploring unfamiliar markets, launching new products, engaging in mergers and acquisitions, and forming strategic business relationships all involve a conscious acceptance of risk as a means to drive success and achieve organizational objectives.

While risks are often perceived as potential threats that need to be managed, embracing risks can be a critical aspect of making informed decisions—and can even lead to a competitive advantage. Organizations with strong governance, risk management, and compliance (GRC) practices are more likely to operate in higher-risk environments with fewer participants. Their ability to confidently manage and adapt to risks positions them favorably relative to their peers. These companies can gain a strategic edge by investing in the latest GRC technologies.

Increasingly, those technologies are driven by artificial intelligence (AI). Ramayya Krishnan, professor of management science and information systems at Carnegie Mellon University, believes AI holds tremendous potential for automating today's data-intensive GRC tasks. However, while the immediate questions it poses to corporate risk and compliance officers are simple, they are also case- and context-specific: "How do I introduce AI into my business processes? Which processes should I prioritize? What guardrails should I put in place to improve productivity and reduce costs while helping confirm there's no reputational damage? The risks associated with running a fleet

HIGHLIGHTS

Governance, risk, and compliance leaders leverage artificial intelligence (AI) technology to **pinpoint risk exposure, build effective internal audit and risk management functions, and anticipate risk** interdependencies.

Among the biggest benefits from generative AI applications—backed by data, documents, and knowledge formulated by experts—are **insights that can help companies bridge gaps in current practices, improve organizational resilience, and confidently capitalize** on emerging opportunities.

By leveraging evolving AI solutions, risk and compliance officers can **focus their efforts on strategic initiatives,** mitigate emerging threats, and foster a more secure and compliant environment for their organizations.

> "With the amount of data we have, AI can help us connect the dots for better output," says Piyush Agrawal, chief risk officer at BMO Financial Group.

of autonomous vehicles is very different from the risks of managing health care data, detecting fraud, or automating HR recruiting."

GRC leaders leverage AI technology to pinpoint risk exposure, build effective internal audit and risk management functions, and anticipate risk interdependencies. According to Krishnan, digitizing risk management processes allows them to respond quickly and efficiently to evolving challenges such as cyber threats, supply chain disruptions, and regulatory changes. Conversely, institutions that lack effective risk management practices tend to be cautious and risk-averse, which often means avoiding higher-risk markets and situations—and forgoing the consequent rewards.

This paper identifies the major trends driving today's GRC strategies, reveals gaps in existing risk-management frameworks, and explains how to use machine learning, AI, and other new technologies to modernize fundamental GRC tasks. It also describes how risk and compliance executives can provide strategic guidance, develop necessary controls, and lead their organizations in the responsible use of AI.

Adapting to a New Era

The adoption of new GRC technology has gone hand in hand with the elevation of risk management. According to Piyush Agrawal, chief risk officer (CRO) at BMO Financial Group, a Canada-headquartered universal bank and the eighth largest bank in North America by assets, the role of the chief risk officer has grown in importance since the financial crisis of 2008. Many senior risk officers have become strategic business partners to the CEO; others report directly to the board of directors.

This heightened trust introduces a growing set of responsibilities. For example, in addition to credit risk and market risk, CROs in the banking industry must attend to the risks of liquidity shortfalls, cybersecurity breaches, third-party fraud, data processing errors, and money laundering, not to mention the risk of not meeting a broad array of regulatory objectives. "Above all, we are responsible for protecting our depositors' money," Agrawal says. "To that end, ensuring the safety and soundness of our banking processes is far more important than pursuing innovation."

Yet the need for safety and soundness has led the financial services industry to gradually but steadily adopt digital technologies, from simple business process automation using GRC tools to more advanced forms of robotic process automation using machine learning, pattern recognition, natural language processing, and generative AI (gen AI). "With the amount of data we have, AI can help us connect the dots for better output," Agrawal explains.

For BMO Financial Group, early steps with AI included using machine learning programs to read and assess a growing set of banking regulations. "A lot of the controls have been built to make sure that we are never in default of a regulation," Agrawal continues. "And because these regulations can change very quickly, our digital tools can actually go into our documentation and machine-read the offerings we have for our clients, to ensure that they don't run afoul of the regulation."

For example, if a new lending regulation for first-time homebuyers changes the limit on the loan-to-value ratio from 80% to 75%, that change can be read by a machine and applied across a bank's lending strategies. "The moment the new regulation comes out, all the lending strategies are associated with the new prescribed regulation," Agrawal says.

Similarly, to help detect and prevent money laundering, a software program can use pattern recognition technology to process transactions and then queue up anomalies for a bank officer to investigate. "Human agents can deal with the exceptions that the machine identifies, rather than having to go through the entire data set," he adds. "We rely heavily on these tools to help us reduce tedious manual work and free up capacity for higher-value work."

Automating Regulatory Compliance

According to Krishnan, some of the low-hanging fruit for AI automation includes demonstrating compliance with data privacy mandates such as the General Data Protection Regulation and California Consumer Privacy Act, along with industry-specific regulations in retail, finance, health care, and other industry domains.

For example, managed care organizations such as AmeriHealth Caritas must comply with the Health Insurance Portability and Accountability Act (HIPAA), which imposes limitations on how protected health information (PHI) can be used and disclosed. HIPAA also ensures that patients have access to and control over their own data.

> AI-powered automation will streamline manual tasks, freeing up resources for strategic initiatives. Ultimately, this could help Medicaid companies identify high-risk providers, predict fraud trends, and even personalize communication to deter fraudulent activity.

"Our primary focus as a Medicaid company is to responsibly handle member information and ensure that our patients receive high-quality care," says Adrian Mebane, executive vice president and chief risk officer for AmeriHealth Caritas, a national Medicaid managed care organization serving approximately 5 million people in 13 states and the District of Columbia.

But especially robust systems are needed when compliance with data privacy regulations becomes increasingly complex. AmeriHealth Caritas must navigate the unique requirements and regulations of government agencies in each of its states and regions, all of which have unique business requirements, information systems, and workflow procedures—not to mention occasional disagreements about how data is reported at federal and state levels. For Mebane and his team, that means AmeriHealth Caritas needs systems in place to uphold HIPAA guidelines and safeguard PHI and personally identifiable information.

"Medicaid often deals with an underserved population, some of whom don't traditionally get access to care," Mebane says. "So it's critically important for us to make sure we're delivering what is required. We must report to state regulators, but equally important is conducting thorough due diligence to ensure that we have appropriate contractual terms, insurance coverage, and cyber protection measures in place to effectively protect this sensitive data."

That's no small task, given the disparities throughout AmeriHealth Caritas' coverage areas. Some states require data to be submitted in spreadsheets, others through secure websites. While business intelligence and reporting software help streamline the process, there is still a manual component involved in populating spreadsheets accurately—and an imperative to do the job correctly.

"Failing to meet state contracts not only raises concerns about the well-being of our members and their access to appropriate care. It also affects our bottom line," Mebane notes. "To improve our operations, we collaborate closely with our data team and performance management team, focusing on areas such as contract adherence."

AmeriHealth Caritas' risk management team can see the advantages of AI automation for everything from categorizing risks to identifying interdependencies during risk assessments. According to Mebane, the journey begins with breaking down information silos from each coverage area, as well as establishing internal governance structures to maintain data integrity. "We are focused on growth and development," he says. "Therefore, it is crucial for us to have a keen awareness of the risks associated with entering new markets, as well as with maintaining existing state contracts. We need to be problem solvers, not police officers. My team maintains a dedicated lens on identifying and mitigating risks. Ensuring this level of internal governance keeps the company accountable and remains a key priority."

One big risk for any Medicaid company involves identifying and mitigating fraudulent medical claims—an immense problem that costs approximately $60 billion per year,

Institutions that lack effective risk management practices tend to be cautious and risk-averse, which often means avoiding higher-risk markets and situations—and forgoing the consequent rewards.

according to the U.S. Department of Health and Human Services. Medicaid companies can use AI to improve oversight, detect breaches, and confirm that network providers comply with contractual agreements.

Mebane believes large language models (LLMs) could be trained to help companies like AmeriHealth Caritas verify that health care providers are paid accurately. Machine learning algorithms can sift through vast amounts of data, identifying nascent risks and facilitating proactive mitigation strategies. Predictive analytics can anticipate potential regulatory changes, allowing organizations to adapt and remain compliant. And AI-powered automation will streamline manual tasks, freeing up resources for strategic initiatives. Ultimately, this could help Medicaid companies identify high-risk providers, predict fraud trends, and even personalize communication to deter fraudulent activity.

Setting Up Intelligent Defenses

In today's constantly evolving risk landscape, Nasdaq is focused on maintaining operational resilience, which requires assessing a near-constant barrage of potential cyber threats, supply chain disruptions, and regulatory changes, all while keeping critical information systems online. Nasdaq operates 15 exchanges across North America and Europe and provides market infrastructure and anti-financial crime technology as well as trading, clearing, securities listing, and other information services to a global client base.

"We have to make sure Nasdaq has solid infrastructure and that our products and services are reliable and always available," says Catherine Addona-Peña, chief risk officer at Nasdaq and cochair of Nasdaq's AI strategy and governance committee. "We've been using proprietary AI technology quite successfully for years and have prioritized a strong governance framework and controls in our product development life cycle," she continues. "With the explosion of generative AI,

we saw an opportunity to continue our leadership and start taking advantage of third-party solutions as well."

For example, Nasdaq is embedding AI in its cybersecurity alert processes to streamline malicious attack monitoring and investigations. "We've started using AI in our data analytics to look across all of our platforms to see where a potential threat might apply," Addona-Peña says.

In addition, Nasdaq's internal audit team utilizes robotic process automation software as part of an auditing solution that identifies potential anomalies and singles them out for scrutiny by a human agent. "Internal Audit is constantly taking in data and identifying potential exceptions as part of their continuous auditing solutions," she explains. "Obtaining real-time audit data allows them to identify potential risks immediately and ensures we remain on the cutting edge of risk management."

Nasdaq also uses AI algorithms for monitoring financial transactions across the financial ecosystem to determine whether there is potential fraud, money laundering or any other type of nefarious activities.

Proceeding with Caution

BMO's Agrawal sees lots of potential for AI applications, but he is wary about rushing new prototypes to market. "Nobody wants to lose out on the next big thing," he admits. "However, the banking industry must be very cautious, because errors can have big consequences. Unless our risk managers are satisfied with the controls, prototypes must remain in the development phase, not in the implementation phase."

Some industries are formulating consortia to help establish consensus about AI issues that need to be regulated, leading to helpful guidelines for public and private companies. For example, the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce, has developed a framework to better manage risks to individuals, organizations, and society associated with AI.

Nasdaq's Addona-Peña sees the wisdom in that approach. "We think the NIST framework has the right rigor, and it's used across multiple industries, so we commonly assess our risk control framework against this standard."

In addition to the broad industry-agnostic consortia represented by the NIST AI framework, Krishnan believes similar consortia will arise in health care, pharma, insurance, and other industries. As AI models gain momentum, he expects these regulatory bodies will provide a standard mechanism by which compliance can be checked and reported, as well as a way to vet AI models to make sure that they aren't leading companies down the wrong path. "Think of it as a sort of AI safety institute or underwriter's lab for AI," he says, adding that somebody has to establish governance—"ideally in conjunction with the industry experts in each sector."
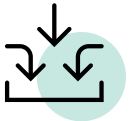
"The 'Big 5' consulting firms are bringing together integrated risk management; integrated governance, risk management, and compliance; and integrated compliance across the organization, and they have the expertise to help executives maintain a consistent level of awareness and protection," says Philip Harris, research director for governance, risk, and compliance services at International Data Corp.

While organizations such as NIST can help confirm that AI models meet certain criteria for safeguards and reliability, Krishnan stresses the importance of engaging with a strategy consulting firm that has a practice devoted to applying AI frameworks to a particular company's needs. "Many organizations need help operationalizing AI so they can put new AI models to work, as well as help identifying which business processes to prioritize," he says.

Agrawal believes outside experts can help the banking industry gain traction with gen AI systems through thorough testing. "Proving the resiliency of AI models involves meticulous training and testing," he says. "How many times did the AI system make an error in the dataset that we have provided to it versus what our expectation is for error rates when that same process is performed manually? These consulting firms can run your prototype against millions of cases to prove that the number of false positives has shrunk to a bare minimum."

A third party with targeted industry experience can also help senior risk officers and compliance officers ask the key questions to keep AI projects on track. Because these firms often work directly with C-suite executives, including CFOs and CEOs, they are adept at navigating not only the leading enterprise risk factors but also the key issues of payback and ROI. "What is the cost of completing these projects, and what is the anticipated return?" Agrawal continues. "What data expertise do we need? What metrics do we put in place to track ROI? There are economic as well as technological considerations that these senior risk and compliance officers may need help with."

Identifying Risk Management Gaps

Among the biggest benefits to be derived from gen AI applications—backed by data, documents, and knowledge formulated by experts—are insights that can help companies bridge gaps in current practices, improve organizational resilience, and confidently capitalize on emerging opportunities. These areas of vulnerability may not be immediately evident. Yet AI models can identify possible risks and exposures that risk officers might overlook through traditional research methods, such as uncovering third- and fourth-party relationships that could potentially impact an organization's supply chain in the event of a geopolitical conflict. By uncovering these relationships and considering these overlooked factors, these models can help organizations make informed decisions to mitigate risks and protect their operations while growing their businesses.

Unfortunately, companies that struggle to understand the current state of their risk exposure may be unsure how to proceed with these advanced risk-management initiatives. According to Philip Harris, research director for governance, risk, and compliance services at Needham, Mass.-based research firm International Data Corp., these firms may not prioritize the most pressing risks or understand the cost of noncompliance.

Here again, help is at hand as service providers and consulting firms step up to help organizations solve these challenges. "The 'Big 5' consulting firms are bringing together integrated risk management, integrated GRC, and integrated compliance across the organization, and they have the expertise to help executives maintain a consistent level of awareness and protection," Harris says.

Frank Lawrence, deputy chief compliance officer at Meta, agrees that technology is needed to help evaluate signs of risk and noncompliance on an integrated basis. "We're in a new normal now, where you're going to have to start looking at all those signals and combining them across domains. That's where technology comes in—whether it be GRC systems, knowledge management systems, or generative AI systems. You need to make sure you have the right signals and the right data sources so that your company makes the right decisions based on the right information throughout the organization."

Lawrence manages critical legal and compliance operations for Facebook and other Meta organizations. Like all multinational firms, his team must contend with a globally diverse regulatory environment marked by a wide range of regional variants. For example, when Meta launched Threads last July, the rollout was delayed in the European Union for

"The one thing that is always on our minds is how to leverage data to identify our risk exposures," says Abhinav Aggarwal, global head of controls at Citigroup Inc.

six months until Meta could demonstrate compliance with the Digital Markets Act, a new EU regulation targeted at Meta and other large gatekeepers of the digital economy.

In addition to international diversity, Meta must contend with a functional overlap that complicates regulatory compliance. Regulations used to be thematically focused on one specialization or domain, such as privacy laws, competition laws, financial services laws, and health care laws, each propagated as a distinct regulatory entity. In response, companies formed multiple compliance departments to stay up to date with these various regulations. However, newer laws and regulations tend to overlap multiple domains, calling for a broad cross-functional view.

To contend with this diverse regulatory environment, consultants and systems integrators are hard at work adapting large language models to particular industries and functional domains. For example, one large consulting firm is collaborating with Microsoft (a major investor in OpenAI's ChatGPT family) to create gen AI models for cybersecurity. "They're looking at all the laws, all the reporting obligations, all the potential incidents for cyber so firms can point these models to their internal IT systems, share the code base, share the changes, and detect any vulnerabilities," Lawrence says. "These models are still in beta, but they are very interesting."

Other consulting firms are working with law firms and in-house counsel to apply gen AI systems to a wide range of risk scenarios. "If you think of the GRC world, where you constantly have new obligations, [these apps] can look at the source law to determine the pertinent legal obligations, write the control objectives, compare and contrast your existing controls to identify gaps, and, finally, write a testing plan to verify compliance," Lawrence sums up. "I don't know if we've seen scaled consistent use cases in practice just yet, but I've seen some prototypes that are very promising."

Automating Regulatory Compliance

LLMs such as OpenAI's ChatGPT, Google's PaLM, and Meta's LLaMA are highly proficient at understanding and generating natural language. With proper training, these powerful language models can help organizations automate regulatory compliance and manage risks by interpreting and implementing written regulations. Basic tasks such as deciphering obligations and translating them into concrete actions can be challenging and time-consuming for human workers. A gen AI application can leverage an LLM to identify regulatory texts, translate them into obligations, generate control descriptions and test steps, and perform automated testing.

Citigroup Inc., one of the world's largest financial services companies, is experimenting with gen AI to assist the firm in managing risks and controls, as well as to automate some of these data-intensive tasks. "The one thing that is always on our minds is how to leverage data to identify our risk exposures," says Abhinav Aggarwal, global head of controls at Citi.

Citi is exploring machine learning technology to evaluate how data can flow most efficiently to pertinent information systems. "This is important for auditing purposes as well as for risk management purposes," Aggarwal continues.

To effectively automate other types of GRC tasks, Aggarwal points out, today's general-purpose LLMs should be trained on an organization's enterprise data. "Part of the challenge involves integrating internal data with the vast trove of data on the internet and elsewhere," he explains.

Aggarwal suggests how a gen AI application could potentially be used to write control descriptions. For example, instead of 10 people writing a particular control in 10 different ways, the app would ensure that all controls are written consistently. The technology could also be applied to the task of testing controls and cascading changes throughout the risk and control environment. "If a control fails, a gen AI app could notify the user where that same control exists and then alert the control owners to the issue," he explains. "It could also look at the data holistically to see if a pattern is emerging or evolving. Banks have hundreds of thousands of controls, so it is a practical application of the technology."

Aggarwal believes large systems integrators and consulting firms can help facilitate these initiatives, but the value proposition needs to be very clear before these projects move from development to production. IDC's Harris agrees, adding that the most promising prototypes have emerged in the realm of cybersecurity. Instead of performing periodic risk assessments, he says, today's holistic GRC solutions can continuously scan an IT environment to determine whether any hardware or software systems are out of compliance. "Whether it's switches, servers, firewalls, or any other IT asset, these continuous compliance solutions can tell you what needs attention," Harris notes.

"We're starting to see integrated risk management where the business areas, the finance areas, and the cyber areas are coming up with one definition of risk for the entire organization," says IDC's Harris.

AI helps in this context by normalizing the data as it is ingested, yielding one consistent body of information that can be analyzed at the executive level. This type of automation is particularly valuable for organizations that must comply with multiple security frameworks, such as Payment Card Industry Data Security, CIS Critical Security Controls, and ISO/IEC 27000-series standards. "You no longer have to combine these frameworks to figure out the baseline," Harris says. "Instead, these common control frameworks use AI technology to manage risk across a broad range of domains. The AI engine makes sure that risk data is consistently captured, stored, and assessed. This allows compliance analysts to spend their time reviewing processes or reviewing documentation."

While these holistic GRC solutions are fairly new, Harris foresees rapid adoption within the next five years. "We're starting to see integrated risk management where the business areas, the finance areas, and the cyber areas are coming up with one definition of risk for the entire organization," he adds. "One report can show all the top risks."

Keys to a Successful Implementation

To gain the benefits of AI technology, Harris emphasizes the importance of adhering to solid GRC principles and establishing regulatory frameworks to govern new models. "Particularly when you use AI to support business-critical decisions based on sensitive data, you need to be sure that you understand what the AI applications are doing, and why," he advises. "Are they making accurate, bias-free decisions? Are they respecting user privacy? You need to have somebody independently vetting these new models to make sure they are doing exactly what they're supposed to be doing."

Harris and other experts provide the following guidance on effectively implementing AI in the GRC domain.

Automate manual tasks for knowledge workers.

Gen AI applications can automate many aspects of risk and compliance programs such as transforming regulatory text into actionable steps, including identifying obligations, generating control descriptions and test steps, and performing automated testing. "By harnessing data we can identify patterns and assess where the impact might be," says Aggarwal at Citi.

Assess complex regulatory documents.

Machine learning applications can be trained to identify key information in documents, such as specific obligations, deadlines, or reporting requirements. This can save officers significant time by automating the initial information-gathering process. "[These programs] can read through thousands of documents and thousands of inventories to reveal where we need to focus our efforts and enhance our controls," BMO Financial Group's Agrawal says.

Identify and mitigate fraud.

By analyzing vast datasets and mimicking fraudulent patterns, gen AI systems can help prevent money laundering, identify

> By using AI technology to understand and effectively navigate prevalent risks, organizations can position themselves for growth, resilience, and long-term success.

fraudulent Medicare claims, and prevent suspicious financial transactions. "In particular, the technology can be used to fight Medicaid fraud by analyzing data for anomalies, automating fundamental research tasks, and generating audit reports," says Mebane at AmeriHealth Caritas.

Streamline attack monitoring and investigations.

AI empowers cybersecurity professionals by sifting through massive amounts of data in real time, pinpointing anomalies and suspicious activities that might indicate a cyberattack. This allows them to focus their investigation efforts on the most critical threats, saving valuable time and resources. "AI helps us to mitigate those types of risks more swiftly and efficiently to ensure we are maintaining operational resiliency across our business," Nasdaq's Addona-Peña says.

Align with industry consortia to establish helpful guidelines.

Industry consortia like NIST convene experts from various sectors to develop best practices for safe, secure, and trustworthy AI development and deployment. "The NIST AI risk-management framework provides some general principles, helping to ensure that organizations are meeting or complying with the standards that have been put in place," Carnegie Mellon's Krishnan says.

Engage consultants with proven AI expertise.

A third-party firm with targeted industry experience can help senior risk officers ask the key questions to keep AI projects on track. "A competent service provider brings all facets of risk management under a single global platform to enable better collaboration, quality, and insights and to better serve each client's needs," IDC's Harris says.

Conclusion

Today's senior risk officers must respond decisively to cyber threats, be alert to the realities of financial fraud, manage disputes with business partners, monitor geopolitical risks, pay attention to stringent consumer protection laws, and navigate the complexities of corporate contracts, to name just a few pressing concerns. It's a tough environment, especially for businesses that are intent on continually growing, transforming, and reinventing themselves.

By using AI technology to understand and effectively navigate prevalent risks, organizations can position themselves for growth, resilience, and long-term success. As the examples in this report illustrate, emerging gen AI applications can automate a variety of tasks, from writing controls to simulating risk assessment scenarios. By leveraging evolving AI solutions, risk and compliance officers can focus their efforts on strategic initiatives, mitigate emerging threats, and foster a more secure and compliant environment for their organizations.