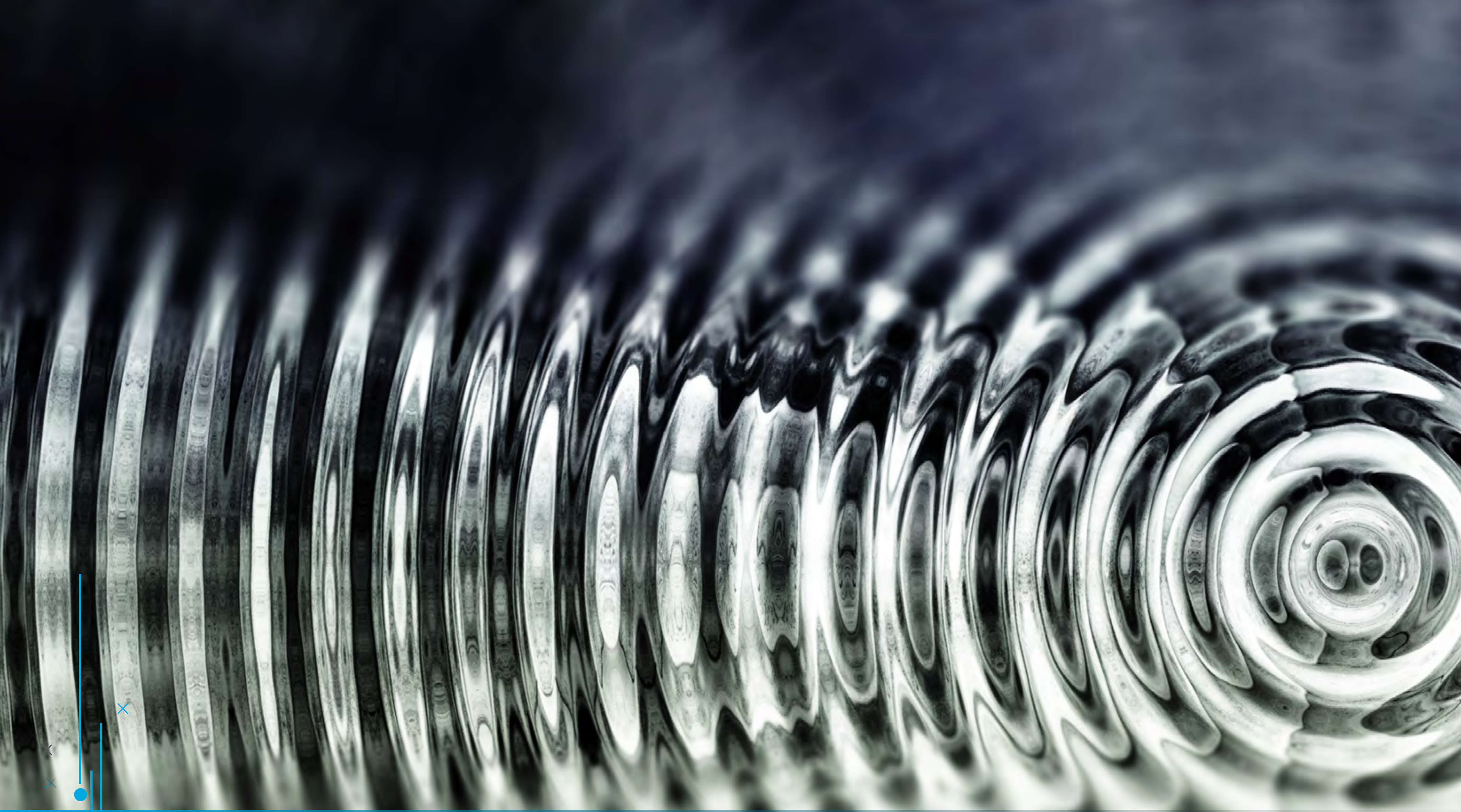
MetricStream

PERFORM WITH INTEGRITY™

THE KNOWN UNKNOWNS 2020

GRC - PERILS AND OPPORTUNITIES

The market will continue to reward risk-takers, but to play the high-stakes game, organizations will need to move beyond the siloed, fragmented risk programs of the past.



RISK AT THE EPICENTER

The scale and scope of risks are changing at an unprecedented pace, propelled by the increasing interconnectedness of organizations, as well as rapid disruptions in business models and technology landscapes. As organizations strive to manage these risks, what will some of their top priorities be in 2020 and beyond? We take a look.

Operational Resilience:
Preparing for the Worst

Resilience will be tested in the coming year as cyber attacks, geopolitical uncertainties, extreme weather events, and other disruptions intensify. Resilience-building will be less about avoiding disruptions, and more about minimizing their impact when they do occur – because they will. The more prepared an organization is to contain the damage and get back on its feet, the better its credibility. In 2019, a leading financial services company was quick to respond to a massive data breach, alerting law enforcement authorities, and fixing the vulnerability swiftly – all of which arguably prevented the breach from turning into a cataclysmic disaster. Today, operational resilience is high on the radar of the UK's Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA). As it finds its way to other regulatory agendas around the globe, organizations will need to be ready with strong incident response measures and business continuity programs.

Flex, not break – that's one way to think about operational resilience.

Non-Financial Risk Management:
Driven by Shareholder Value Rather Than Financial Loss

Compliance failures, misconduct, and technology disruptions will continue to amplify non-financial risks in 2020. While the financial losses and regulatory fines associated with these risks are significant, their larger impact lies in the long-term erosion of shareholder value. A risk program focused solely on direct losses will only end up meeting compliance obligations; but an integrated risk program focused on shareholder value will enable organizations to predictively identify and proactively respond to non-financial risks. The key differentiator of a shareholder value-focused risk program is its integrated view of risk-reward relationships that comes from mapping shareholder value indicators to strategic initiatives, associated risks, and regulations. This tightly-knit data model can provide rich, real-time risk intelligence to minimize potential financial losses, while also optimizing shareholder gains.

Third-Party Risk:
More Pervasive than You Think

In early 2019, financial regulatory authorities imposed severe fines on an independent bank for failing to implement sufficient oversight on a vendor. A few months later, a leading European bank reported an unauthorized data breach through a website hosted by a third party. Incidents like these will continue to remain top challenges in 2020 and beyond, especially as more third parties gain access to sensitive data. Organizations will need to ensure that third-party risk monitoring and due diligence processes meet the highest standards. The first step is to ensure sufficient visibility across the third-party ecosystem. The more effectively organizations understand how third parties map to processes, business units, risks, compliance requirements, and controls, the better they can prioritize and direct their risk mitigation investments.

Just about everything we do today has some level of third-party involvement whether we're aware of it or not.

Thriving in the Reputation Economy

In a hyperconnected world where negative news travels swiftly, business decisions and actions will be governed not only by legal or compliance considerations, but also by reputational ones. If an organization makes the news for the wrong reasons—perhaps due to an unhappy consumer or a disgruntled employee—the reputational repercussions can be enormous, often leaving permanent scars. Today, customers and stakeholders are looking not just at what an organization delivers, but how it was delivered. Were sales practices unethical? Was customer data compromised? Were suppliers exploited? These questions will continue to surface as organizations expand their focus to intangible assets like trust and reputation where the value of a business will increasingly be found.

Integrated Risk Management:

A Strategic Advantage

The market will continue to reward risk-takers, but to play the high-stakes game, organizations will need to move beyond the siloed, fragmented risk programs of the past. These programs, which traditionally looked at risks in isolation, were not designed to respond to fast-changing risk environments, or to understand the interconnectivity of risks. Future risk programs, by comparison, will focus on building an overarching integrative layer that maps the relationships between different risks—including their impact and related issues—while tying them back to business objectives. In these integrated risk management (IRM) programs, the underlying technology i.e. the IRM platform will act like a general ledger, providing a single, transparent system of record for risk data, incidents, and responses across the enterprise. The result? Real-time, targeted risk insights to support strategic decisions.

Organizations with highly integrated risk programs tend to exceed profitability targets more often, and achieve higher growth than those with less integrated programs who may struggle to realize value and achieve the desired outcomes (Deloitte[i]).

DEEPENING FAULT LINES

As we enter the fourth industrial revolution, the opportunities ahead are tremendous, but so are the associated risks. “Known unknowns” can come from anywhere, hitting organizations where it hurts most. Staying ahead will require better risk awareness and vigilance. With that in mind, we examine some of the top risks to watch for in 2020.

Cyberwarfare:
Redrawing the Battle Lines

Recent stand-offs between sovereign nations represent the dawn of a potentially new stage in warfare where attacks are exchanged not on a battlefield but in cyber space. It could fast become a way for countries to demonstrate power without bloodshed. Yet, for companies caught in the cross-fire, it represents a whole new level of risk. Cyber weapons can infiltrate and shut down entire networks, as we've seen multiple times in the past year. Today, cyber weapons are affordable and widely available not just to nation states but also to criminals eager to take advantage of software vulnerabilities and poor cyber hygiene. Given the ramifications of these issues and the scale at which they can impact not just organizations but entire countries, cyber resilience efforts will need to be stepped up.

The Challenge of Misinformation

With fake news becoming an ecosystem unto itself, people will find it harder to separate fact from fiction. Today, social media has outpaced print newspapers in the U.S. as a news source[ii]. False news stories can spread like a virus on these channels, embedding themselves deep into people's memories and influencing the way they think. All it takes is one fake story about a brand to damage the company's reputation, and create widespread distrust. Magnifying the challenge are "deep fakes". Almost anyone can manipulate digital images or videos for corporate sabotage or other malicious purposes. The big question in 2020 will be whether or not tech giants, publishing platforms, and governments are doing enough to stem the flow of misinformation. How much responsibility are they willing to take for the problem, and how much are they ready to invest in combating it? That remains to be seen.

False news travels significantly farther, faster, deeper, and more broadly than the truth. In fact, falsehoods are 70% more likely to be retweeted than the truth (MIT Initiative on the Digital Economy)[iii].

Compliance:
A Personal Liability for the C-suite

With the CEO of a major tech company being held directly responsible for future violations of data privacy rules at his organization, compliance has moved from a corporate issue to a personal one. Meanwhile, new legislation has been proposed to criminally charge corporate executives when customer data is breached. These developments, coming as they do against the backdrop of the UK Senior Manager's Regime and Certification Regime (SMR/CR), signal a new era of accountability in compliance. No longer can CEOs claim ignorance about risk or compliance incidents in their enterprises. Their personal reputations are now at stake. Compliance initiatives are therefore likely to receive a greater thrust as CEOs seek to stay informed about risk and compliance incidents. Real-time compliance monitoring and measurement will become increasingly essential.

GRC @ DIGITAL SPEED

New digital advancements are enabling GRC functions to add value to their organizations in ways that haven't been possible before. Yet to fully realize the benefits of technology, GRC programs, processes, and systems must be able to keep up with the speed of digital transformation.

"Predict to Prevent":

The New GRC Mantra

The crystal ball is here. With emerging technologies like artificial intelligence (AI), GRC functions will be able to predict and prevent risks, issues, and incidents before they occur. Advanced analytics will sift the signal from the noise, uncovering hidden risk insights in big data to optimize decision-making. AI engines will automatically scour internal databases and external feeds, cross-referencing information to identify risk patterns, as well as to detect control weaknesses. Using these insights, management will be able to swiftly contain potential issues, or act on upcoming opportunities. Meanwhile, natural language processing tools will leverage the power of semantic analysis to connect the dots between thousands of issues—both past and present—in order to identify the best remediation actions. Robotic process automation (RPA) will support continuous control monitoring as well as full sample-auditing, making it easier to detect anomalies. All these advancements will enable GRC functions to deliver greater value, and act as true strategic advisors to the business.

With the three lines of defense, there used to be three sources of truth. But today, with advances in GRC technology, there is just one source of truth – the machine (Insights from the CXO Roundtable, GRC Summit 2019).

Empowerment of the Front Line

New GRC software will be built not just for the second and third lines of defense, but also for the front line. In fact, with technologies like AI, the front line will no longer need to undergo intensive training on GRC tools, or be well-versed in GRC terminologies, in order to report a risk or issue. All they will need to do is talk to a virtual assistant (VA). Through a casual conversation in natural business language, the VA will capture front line observations on potential issues, incidents, and control weaknesses. These insights will then be automatically routed to the second line of defense for further investigation. The VA will also follow up with front line users on the status of a reported issue, thus strengthening user engagement. As more users begin to participate in risk reporting, richer insights will flow up to the management and board, enabling them to proactively identify and mitigate potential risks.

Through technology, it is possible to empower everyone, in a personalized manner, so that we can have not just a few participants in risk, but rather all the tens of thousands of employees and third parties across the globe.

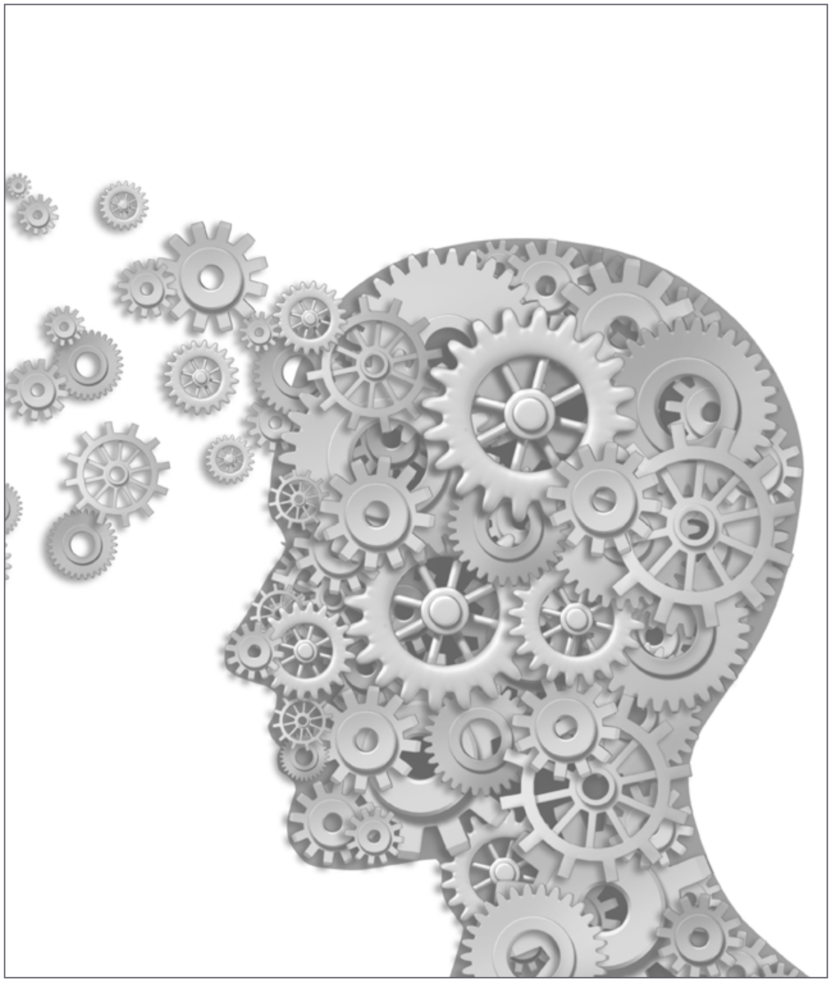
The Agility Imperative

As technology evolves at an unprecedented pace, the data security processes that govern it must become more agile. For too long, security has been treated as an afterthought in the race to release or adopt new technologies. But today, customers want 100% security 100% of the time. That means thinking about security right from release 1, not release 1.5 or later. The challenge for IT teams is not just to ensure that security is baked into the software lifecycle from the start, but also that it keeps up with the speed of digital transformation. The more agile security testing is, the faster new software can be rolled out. That will call for greater collaboration among development, operational, and security teams. SecDevOps, or "security at speed" will become more important than ever.

The Reskilling Revolution

To be seen as credible business partners in a digital era, risk and other assurance functions will need to refine their current skills, while also acquiring new ones. Future GRC practitioners will be digitally-savvy with a strong understanding of technology trends to challenge and advise the business on potential risks. They will also have in-depth knowledge of the business, collaborating seamlessly with teams across the enterprise to strengthen innovation, while mitigating downside risks. Meanwhile, as GRC functions themselves adopt smart technologies to optimize efficiency and productivity, they will need to evolve the skills required to gain the most value from these tools. Expertise in data science, modeling, and advanced analytics will be key for GRC practitioners to efficiently sift through data and derive intelligence to drive strategic decisions. Some teams will focus on bringing in outside talent to meet these requirements, while others will develop it in-house. Whatever the approach, skills diversity will be essential for GRC teams to deliver the value that future digitalized organizations need.

Are organizations upskilling their CISOs? 84% of executives prize a CISO's ability to educate and collaborate across the business. Yet only 39% encourage staff to develop a wider knowledge of how the business works (Harvard Business Review Analytic Services in association with PwC[iv]).



ETHICS AND INTEGRITY – THE PATHWAY TO TRUST

Around the world, organizations are being pulled up for unethical practices such as misusing personal information, spying on people through smart devices, and licensing surveillance technology. In 2020, what are the key ethical issues that will be important for organizations to think about as they endeavor to build better trust and credibility?

Digital Transformation and Ethics:

Two Sides of the Same Coin

As we seek to co-author the future of the digital age—to build high-tech societies that are utopian in both reach and possibilities—it will become increasingly important to ground ourselves not just in science, but in questions of ethics, sustainability, integrity, and social impact. Technologies like the cloud, AI, virtual reality, and IoT are opening up a new world of opportunities, but they're also amplifying insecurities. Smart devices that eavesdrop on human conversations, robots that make life-or-death decisions for humans, fake news that results in fatal consequences – these are real fears. Mitigating them without compromising on the opportunities offered to us by technology may well be one of the biggest challenges of the digital age – a challenge that we cannot hope to solve without GRC.

Responsible AI Engineering

While investments continue to pour into AI, ethical concerns abound. How do we prevent harmful biases from being encoded into the technology? How do we ensure that the system doesn't override its original objective in favor of an unwanted outcome? How do we build transparency into the underlying algorithms? It's no longer just about what AI is capable of doing, but also what it should be doing. Effective governance of bots is the next horizon for GRC. Recently, the European Commission released a series of guidelines to encourage the development of "trustworthy" AI[v]. Not only do they call attention to AI transparency, non-discrimination, and accountability, but they also emphasize technical robustness. Are the algorithms reliable enough? Is there a fallback plan in case something goes wrong? These concerns will become increasingly critical as we move to an AI-driven era where self-driving cars, autonomous weapons, and other AI applications become a reality.

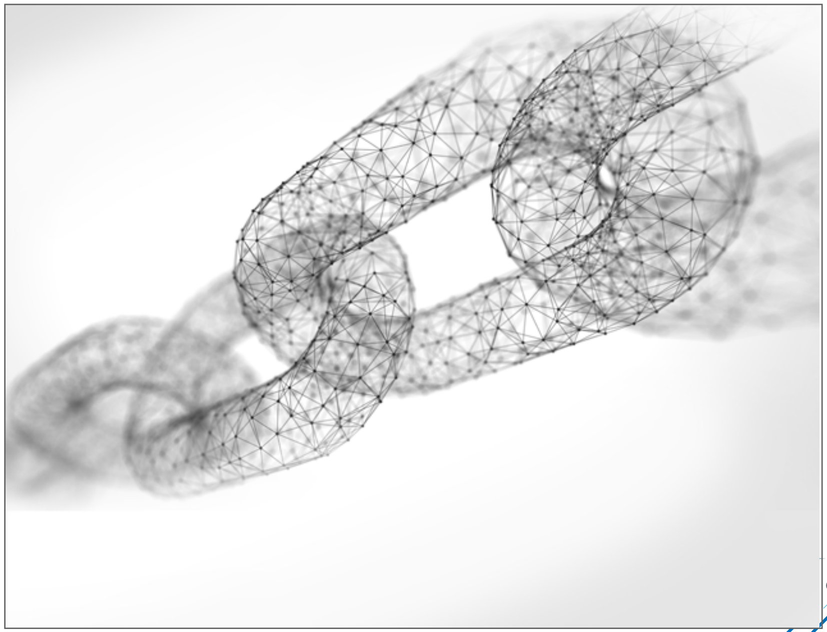
80% of risk professionals are not confident about the governance in place around AI (KPMG[vi])

GRC as the Sorting Hat for Big Data

Data will continue to be the lifeblood of the modern digital economy. However, it will only be as valuable as the level of trust invested in it. If big data is "the new oil," the role of GRC will be to determine the value of that data. Can it be trusted? Or is it biased and deceptive? In many organizations, corporate data is either untamed or suppressed, leading it to degenerate into toxic waste that increases organizational liability. At the other end of the spectrum is "inclusive data" – i.e. data that is trusted and transparent. GRC will act as a "sorting hat" for this data, sifting and organizing it based on issues of governance, friction, obfuscation, security, and ultimately ethics. In fact, going forward, data ethics will emerge as a strategic business weapon.

Blockchain:
Being Vigilant about Weak Links

The buzz around blockchain will continue as loyalists hail its self-governing decentralized model, as well as the accountability and transparency it offers. However, concerns surrounding the governance of blockchain will continue to persist. Are there sufficient mechanisms in place to prevent the financing of terrorists and other criminals, as well as interference with monetary policy? Are there controls to guard against "51% attacks" when a cyber criminal or a group of hackers control the majority of nodes in a blockchain? How do we ensure that personal information and trade secrets are not published openly on a blockchain? How do we minimize the environmental impact of blockchain activities like bitcoin mining? Currently, blockchain may be seen as the answer to digital trust issues, but without appropriate safeguards, it could very well lead to rampant misuse and large-scale issues.



Contact us
www.metricstream.com

[i] Reimagine risk: Thrive in your evolving ecosystem - Deloitte's 2019 survey of risk management, April 11, 2019 - Chris Ruggeri, Chris Vanuga, Keri Calagna, Cynthia Vitters, Michael Fay

[ii] Social media outpaces print newspapers in the U.S. as a news source – Pew Research Center, December 10, 2018 - By Elisa Shearer

[iii] The Spread of True and False News Online - MIT Initiative on the Digital Economy Research Brief - By Soroush Vosoughi, Deb Roy, and Sinan Aral

[iv] Evolving the CISO Role to Make Cybersecurity a Competitive Advantage – Harvard Business Review Analytic Services, Sponsored by PwC, 2019

[v] Ethics guidelines for trustworthy AI - High-Level Expert Group on Artificial Intelligence, April 8, 2019

[vi] AI | Compliance in Control – Financial Services Regulatory Challenges – KPMG, 2019