



# GRC 2019:

## THE KNOWN UNKNOWNNS

---

"The future of GRC will not just be about managing known risks or monitoring compliance. It will be about sustaining an organization's social license to operate."

## EVOLVING ROLES

Chief Risk Officers (CROs), Chief Compliance Officers (CCOs), Chief Information Security Officers (CISOs), and Chief Audit Executives (CAEs)—once limited to supporting roles in the organization—are increasingly being given a seat at the table with the power to influence strategy and decision-making. With this new power comes new obligations and challenges.



## Balancing Value Protection and Value Creation


As enterprises strive to stay ahead of the curve, GRC executives will be expected to go beyond their traditional roles as the guardrails of the organization and become enablers of business performance and growth. They will need to find a balance between protecting value and creating it; between being the voice of reason in the C-suite and enabling the business to take the requisite risks to achieve the desired rewards. CROs, for instance, will be called on to help leadership teams decide when to launch a new product, or which markets to target first based on the associated risks and opportunities. In doing so, they will be seen as enablers of innovation.

## Truth-tellers and Strategic Advisors

Boards will demand more transparency. They will want to respond more proactively to potential risks and opportunities. Therefore, CROs, CCOs, CAEs, and CISOs will need to deliver insights that are forward-looking, actionable, and performance enabling. They will also need to become better story-tellers, communicating their message clearly, succinctly, and in a way that the board can understand and act on. To support these efforts, new generations of GRC solutions will be designed to predict potential risks with greater accuracy and speed than ever.

## Leading from the Front

More risk and compliance responsibilities will move down into the first line of defense. But first, organizations will need to think about how GRC can be adapted to the first line, not how the first line should adapt to GRC. How can GRC be made so intuitive that it becomes a seamless, almost inherent part of employee routines? The answers, to some extent, will lie with technology. GRC tools will increasingly be layered into the systems used by the first line in such a way that when an employee is confronted with a potentially risky or non-compliant transaction, the underlying technology will automatically trigger checklists and workflows to guide the employee towards making the right decision.



58% of internal auditors are seeking tools for predictive analysis and modeling, while 77% want data querying and analysis tools, and 60% want data visualization capabilities.

[MetricStream's State of Internal Audit Survey 2018](#)

---

## Blurring of Lines

Traditional boundaries between GRC functions will dissolve in the quest for greater integration. For instance, CISOs and CROs will begin to collaborate more closely to safeguard the digital data universe. After all, data security isn't just an IT risk – it's a business risk, and a top one at that. What's more, data security risks don't exist in isolation; they often amplify the impact of other enterprise risks such as compliance risks, reputational risks, and even financial risks. CROs, by virtue of their role, are best-positioned to understand these risk relationships. Therefore, their involvement in cybersecurity and IT risk management will grow more critical. Similarly, Chief Procurement Officers (CPOs) will become more engaged with CROs, CISOs, and heads of enterprise risk, as they assume a more active role in third-party risk management.



36% of banks and financial institutions rely on their CRO to oversee their IT risk management program.

[MetricStream's "Moving Up the IT Risk Management Maturity Curve" survey](#)

# THE INTEGRITY FACTOR

With incidents of money laundering, personal data abuse, sexual harassment, and other scandals making the headlines, GRC as we know it, is changing. It's no longer simply about managing known risks or monitoring compliance. GRC today is about sustaining the "social license to operate" – ensuring that business practices, operating procedures, and corporate behaviors are acceptable to employees, stakeholders, and the public at large. What does that portend for enterprises in 2019 and beyond?



## Performing with Integrity


We're entering a world without secrets where everything enterprises do will be scrutinized, not just by regulators and stakeholders, but by a larger, hyperconnected society with tremendous computing and communication power at its fingertips. In this world, the success of an organization will be determined not only by its achievement of sales targets or performance objectives, but also by its conduct, ethics, transparency, and fairness – in other words, its integrity and ability to align performance to its core values. GRC functions will play a key role in driving this sense of integrity throughout the enterprise.

## Trust: The New Currency

Trust will continue to be the largest—and most fragile—component of business value. Organizations that fail to earn and sustain the trust of their market will pay a heavy price in terms of lost business, dissatisfied customers, and damaged reputations. In fact, trust will drive corporate governance just as much as regulations. Many organizations will look to their GRC functions to build this sense of trust by ensuring that nothing slips through the cracks in product quality, ethical sourcing, data security, and other key areas. Meanwhile, the first line of defense will emerge as the key custodians of trust since they are the ones who interact directly with customers. The responsibility for training and enabling them will fall to the second and third lines of defense.

## Beyond the Checklists

Recent compliance and ethics violations—including the incidents that led up to the #metoo movement—revealed a major shortcoming in many organizations – that even though sufficient policies and training programs were implemented to curb bad behavior, they were treated as a routine procedure for the sake of satisfying a few laws. The focus was on protecting the business against lawsuits than on addressing a core issue – an approach that was often one-dimensional and lacking in depth. That will need to change if organizations want to build credible, trustworthy enterprises. They will need to treat compliance as a cultural initiative, and take steps to embed it deep into the consciousness of the entire organization, so that at every step, employees know to ask themselves, “Are my decisions and actions compliant?”



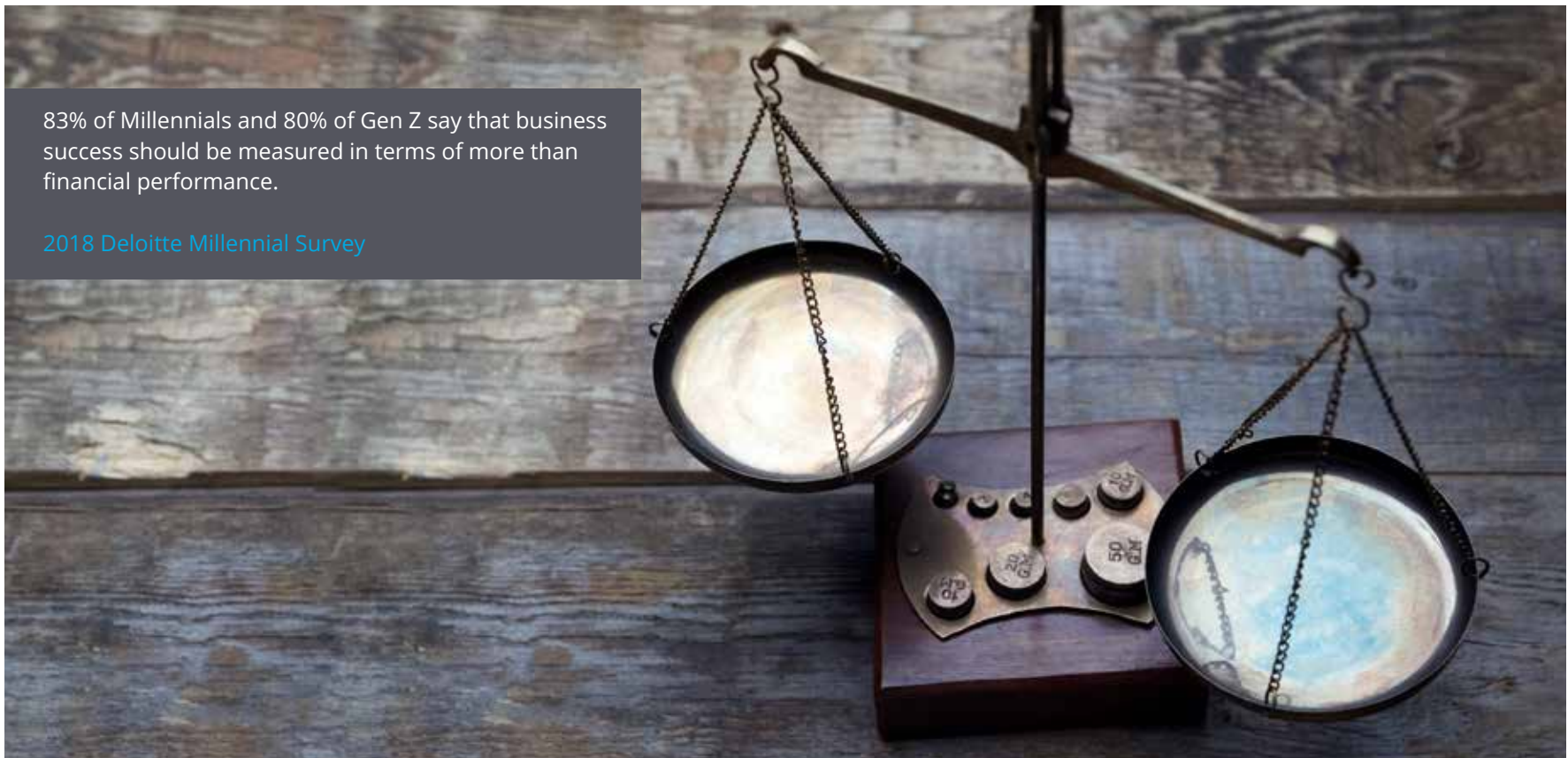
Integrity will be the foundation on which the enterprises of the future build satisfied customers, engaged workforces, and well-loved brands.

## Profit and Purpose: Both Matter

Ten years from now, no organization or brand will be able to succeed without doing good and doing well — i.e. delivering financial performance while also making a positive contribution to society. Social purpose will need to be embedded into the very fabric and heart of the enterprise. Why? Because Millennials—the next generation of shareholders, customers, and employees—are demanding it. The way in which GRC professionals help organizations achieve their social purpose—whether it's to improve the quality of people's lives as a health care organization, or to provide safety and security for the life savings of customers as a bank—will determine the future of the digital economy.

83% of Millennials and 80% of Gen Z say that business success should be measured in terms of more than financial performance.

[2018 Deloitte Millennial Survey](#)



# WEAK LINKS

As cyber threats, financial fraud, regulatory fines, and other risks continue to escalate, GRC functions will need to be more vigilant -- to proactively spot and address the areas of concern that could potentially derail their enterprises.





## Operational Technology Outages: A New Peril

In 2019, the cybersecurity conversation will move beyond business-specific threats and vulnerabilities, to focus more strongly on the larger, more perilous threats to critical infrastructure. While power grids have been in focus ever since the infamous [2015 Ukraine grid attacks](#), other critical facilities such as water supply networks, gas pipelines, and transportation systems have also become sources of worry for cybersecurity experts. Earlier this year, the FBI [sounded the alarm](#) about Russian hackers attacking the U.S. electric grid, water processing plants, and aviation facilities. A few months before that, the British government's top cybersecurity official had [warned](#) of similar attacks on the UK's energy, telecom, and media industries. These incidents are only likely to escalate as malicious actors look to strike at the very heart of a city or nation. The question is, will cyber defenses be able to keep up?

## The Third-Party Maze

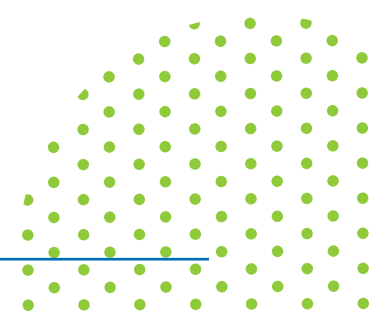
In 2018, leading organizations across retail, air travel, and the entertainment industry suffered major data exposures due to vendor security vulnerabilities. Around the same time, the European Banking Authority (EBA) [published its draft guidelines on outsourcing](#) for financial institutions. Going by these trends, third-party risk management will become an increasingly important priority in 2019. Organizations will be expected to document all third-party relationships, segment them based on risk, and conduct periodic reviews. They will also need to implement effective policies and controls for outsourcing, while ensuring effective oversight of the third-party ecosystem, including sub-contractors.

## Senior Management: Focus on Accountability

Right from the 2002 Sarbanes-Oxley (SOX) Act, to the 2016 UK's Senior Managers Regime (SMR), regulators have been saying that the buck stops with senior management. No longer can CEOs claim to be ignorant of toxic cultures breeding in their organizations. They will be held accountable for setting the tone of integrity, compliance, and ethics across their enterprises. They will be expected to ensure effective corporate governance, while also building a pervasive culture of risk awareness, and imposing strong consequences for misbehavior. Even in the US, which is heading towards an era of deregulation, the growing power of consumer sentiment will compel senior management to take responsibility for the culture in their organizations.

57% of organizations do not have adequate knowledge and appropriate visibility of sub-contractors engaged by their third-parties.

[Deloitte's Extended Enterprise Risk Management \(EERM\) Global Survey 2018](#)

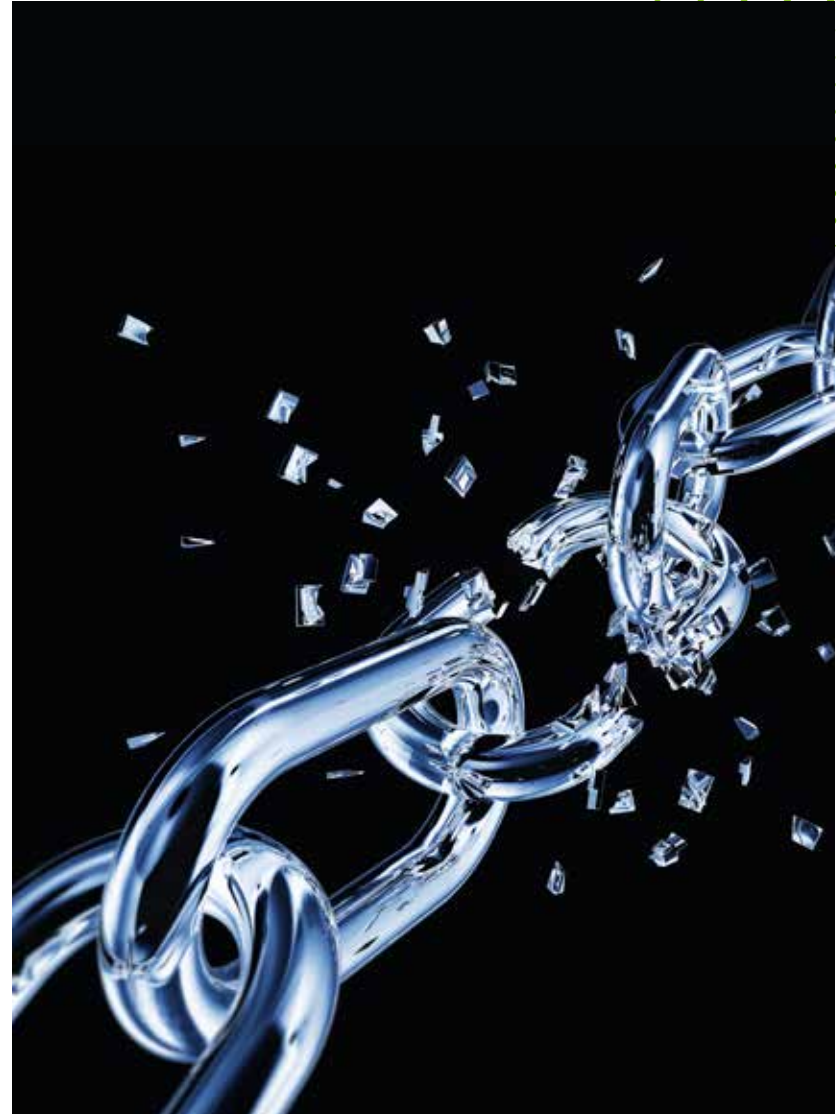


## Data Localization: New Digital Barriers

With major markets like [India](#) and [China](#) imposing data localization mandates, global companies will be under pressure to rethink their information governance mechanisms. No longer will they be able to store data however they see fit, or enable the free flow of information across borders. Many organizations will have to make arrangements with local cloud service providers, or build their own data centers – both of which come with significant costs. From a security perspective, data risk assessments and monitoring activities will likely become more decentralized. So will compliance management, as data localization laws vary from one region to the next. GRC professionals will need to stay one step ahead of these trends, tracking and understanding them, while educating the business on the best way forward.

## Operational Resilience: No More Excuses

Operational resilience has caught the eye of UK regulators, particularly the [Prudential Regulatory Authority \(PRA\)](#) and the [Financial Conduct Authority \(FCA\)](#). The underlying message is that financial institutions can no longer play the victim card when disruptions occur. They must be prepared with a strong resilience strategy and plan that allows them to deliver proficient services at all times, even in the midst or aftermath of a disruption. Business leadership will be responsible for driving this culture of resilience across the three lines of defense.





# TECHNOLOGY TRAJECTORIES

Where is GRC technology heading? How will it address the weak links and known unknowns ahead? What do users need to be careful about? Here are a few key trends.

## Artificial Intelligence as a Service: Going beyond the Data

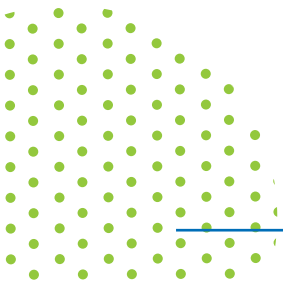
Over the next five years, AI specialists will continue to be a scarce resource. However, the demand for the intelligent use of accumulated risk data will only increase. As a result, AI experts will begin to offer AI as a service (AlaaS), particularly to industries where data is too valuable not to be analyzed. Health care and legal will be the two industries that will adopt AlaaS first to evaluate valuable GRC data, and to solve core issues in less time. The importance of taxonomy-based contextualization and layering of human intelligence will be the most value accretive in these industries.


## Cyber Risks: Auto-remediation Leads the Way

Over the next five years, AI and advanced analytics will enable cyber risk professionals to set up systems where 80% of incidents will be self-remediated based on past data that is automatically gathered by bots and other tools. These systems will assess cyber risks and incidents continuously to detect patterns, flag the biggest risks, and suggest mitigation paths. In fact, the cyber ecosystem will probably be the first in the organization to run on a self-governance model wherein the entire process of risk identification, assessment, and mitigation will require minimal human intervention.

## Data: No Longer the New Oil

With GDPR, a new template has been made available to regulators and law makers to give online users more control over their information. We believe that the tussle between online advertisement revenue and user privacy will deepen in the next three years as both sides seek more control and power over data. A new ephemeral approach to data management, propagated by a select few organizations such as [Snap](#) and [DuckDuckGo](#)—where data is either not collected or auto-destructed in a finite period—will gain traction, and slowly become the new norm for online users and, consequently, online organizations.





MetricStream is the independent market leader in enterprise cloud applications for governance, risk, compliance (GRC), and quality management. MetricStream apps and software solutions improve business performance by strengthening risk management, corporate governance, regulatory compliance, audit management, vendor governance, and quality management for organizations across industries, including banking and financial services, health care, life sciences, energy and utilities, consumer brands, government, technology, and manufacturing. MetricStream is headquartered in Palo Alto, California, with an operations and GRC innovation center in Bengaluru, India, and sales and operations support in 12 other cities globally. ([www.metricstream.com](http://www.metricstream.com)).

US: +1-650-620-2955  
+1-212-363-2955

UK: +44-203-318-8554  
India: +91-(0)80-4049 6600

© 2018 Copyright MetricStream  
All rights reserved.