GRC Vision, 2019 To 2024

Vision: The Governance, Risk, And Compliance Playbook

by Renee Murphy and Christopher McClean

January 25, 2019

Why Read This Report

Risk management professionals are used to helping steer their organizations through uncertainty, and as fast as business and technology are advancing, they should be looking five years into the future to guide their current strategy. Many key trends will amplify strategic and digital risks and transform the core responsibilities of risk management. This report outlines these global business and technology trends and their long-term implications, helping risk managers better prepare for the potential impacts that will shortly ensue.

Key Takeaways

Regulators Are Still Falling Behind, Ceding Oversight To Customers And Employees

While government and industry regulators lack the capacity to guide emerging technology and business models, customers and employees are banding together on social media to demand that companies they work with behave better.

Emerging Technologies Represent Challenges And Opportunities For Risk Managers

The aggressive collection and use of data, along with new technologies like IoT devices and machine learning, are creating new data integrity risks for companies in every industry. At the same time, these new analytic and automation capabilities will help risk management leaders better identify and manage risks across their organization.

GRC Vision, 2019 To 2024

Vision: The Governance, Risk, And Compliance Playbook

by Renee Murphy and Christopher McClean
with Stephanie Balaouras, Nick Hayes, Claire O'Malley, Trevor Lyness, and Peggy Dostie

January 25, 2019

Table Of Contents

Related Research Documents

Beware The Coming Data Integrity Crisis

Extend Compliance And Risk Management To What Really Matters For Your Business

GRC Vision 2017-2022: Customer Demands Escalate As Regulators Falter

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Regulators Continue To Cede Oversight To Customers And Employees

Business and technology change is accelerating, with the promise of hyperadoption driving companies to transform every aspect of their customer engagements. To stay ahead of the digital disruption curve, they're assembling teams with incredible creativity and technical talent. Meanwhile, regulators charged with overseeing these companies and protecting consumers against unsafe products lack the bandwidth and skills to keep up.[1] The evidence is growing: Risk management professionals at big tech companies are building their own frameworks to guide their version of ethical behavior, and big businesses continue to win their battles against the government.

But customers aren't simply acquiescing. To punish offending companies — and reward those with better reputations — they're articulating their values on social media and encouraging others to respond, effectively launching collective bargaining campaigns. And they're doing it on an unprecedented scale:

- **Customers are punishing bad corporate behavior more than regulators are.** It's easy for companies with large coffers to look at regulatory settlements (with no admission of guilt) as a cost of doing business. However, while Wells Fargo launched its advertising campaign trying to reestablish customer trust after its "eight is great" scandal, 14% of the company's customers said they planned to switch to another bank, with estimated losses of $99 billion in deposits and $9 billion in revenue.[2] Similarly, after a number of privacy and workplace harassment scandals rocked Uber in 2017, customers left in droves, with 14% saying they would never return, 18% saying they would return with better privacy assurances, and 28% saying they would return when the CEO, Travis Kalanick, was fired. When the dust settled in June 2017, he stepped down.[3]
- **Customer pressure is also rewarding companies that stick to their values.** Consumers using their collective voice to demand change can be a good thing for companies that express and live by values those customers care about. At a time when racial issues were intensifying around the NFL, Nike took a risky bet with a nationwide ad campaign supporting Colin Kaepernick for his decision to kneel during the national anthem. Ultimately, customers responded positively, Nike's stock rose in value by over $6 billion, Kaepernick's jersey sold out overnight, and Nike picked up a lot free, positive press.[4]
- **Employees have joined the call to regulate their employers' behavior.** Like customers, employees prefer to associate with companies that share their values. Even without formal unions, employees of large firms are using social media networks as platforms for collective bargaining in the form of walkouts and protests. Google employees staged a walkout over the company's handling of sexual harassment claims.[5] Earlier in the year, Amazon employees effectively protested their employer's working with US Immigration and Customs Enforcement.[6]

New Trends Are Elevating Risk, Requiring More Advanced Controls

Along with the shift in oversight, new business models and technical advancements will require risk managers to expand the scope of processes and decisions they assess, while also providing new tools to take on these challenges. Four key trends will disrupt the field of risk management over the next five years.

No. 1: Silicon Valley Is Becoming The Next Wall Street, And Not In A Good Way

Because of its massive scale, its ability to negatively impact wide swaths of humanity, and its history of bad behavior, the financial industry deals with a vast number of federal, state, and market regulators. As Silicon Valley increasingly demonstrates dubious privacy practices, business models that circumvent existing laws, and a pattern of disregard for employee and customer well-being, tech firms are on the path toward greater regulation as well. Even if the regulators are falling behind in innovation and scale, there's reason to think that this increased oversight will be difficult for any companies making money from tech innovations and use of data:

- **Tech firms are making an unconvincing case for self-regulation.** If Silicon Valley is after the kind of self-regulation physicians and lawyers enjoy, they should address their Facebook problem before it's too late. Although Mark Zuckerberg called for Facebook to be regulated, the regulation he is asking for is weak and ineffectual. Since the Cambridge Analytica scandal, Facebook was caught retaining users' videos, allowing Russian meddling, propagating fake news, secretly deleting Zuckerberg's messages while keeping and sharing users' messages, spreading hate speech in Myanmar, and moving 1.5 billion accounts out of Ireland and back to American data centers rather than follow the GDPR. That's not what contrition or self-regulation looks like. And regulators know it.

  In a Reuters/Ipsos survey of 2,237 people, 46% said they want companies that have their personal information to be more regulated, 63% want to see less targeted advertising, and 51% don't trust Facebook.[7]

- **Authorities aren't stopping with GDPR.** By far the most massive move to wrangle inappropriate use and protection of data, GDPR promises a new level of corporate respect for personal privacy, and hefty fines to encourage real change.[8] But even as more governments around the world are adopting similar language in their new privacy laws, authorities are taking Facebook, Google, Microsoft, and other tech giants to task over perceived lapses in good business practices like privacy protection. Regulators that can't figure out new tech and business models simply ban them.

No. 2: Data Integrity Risks Are A Mounting Threat To Your Business

As digital transformation fundamentally changes the way your businesses collects, processes, and relies on information, it's exposing your company to substantial and unmitigated data integrity risk. If left unchecked, attackers that manipulate your firm's data (rather than steal it) could cause disastrous losses for your firm.[9] We've already seen examples of data integrity attacks resulting in massive

physical damage (Stuxnet), widespread political implications (voter manipulation), and the potential for corporate fraud on a scale we've never seen before (deep fakes). Key aspects of this growing trend will require risk managers' immediate attention:

- **Your business relies on data like never before.** Data is being created and consumed at a rate faster than ever. From finance planning the yearly budget to marketing picking what customers to target to HR making hiring, firing, and salary decisions, every department in your business extensively relies on data. And the advent of technologies such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), chatbots, intelligent agents, and more are drastically increasing this data dependence. While these technologies can significantly help win, serve, and retain customers, automated decision-making technologies are a clear target for data tampering.
- **Attackers can manipulate data without hacking into your network.** Protecting your firm's data integrity doesn't just mean ensuring attackers don't get inside your networks. Attackers can target your company externally by manipulating your reputation via social media, fabricating news stories, or even using bots to mimic customers on your website.[10] In 2013, a fraudulent tweet using the Associated Press' Twitter account announced that explosions had injured President Barack Obama at the White House: Reaction temporarily wiped out $136.5 billion of the S&P 500's value.[11] In May and June 2018, Twitter banned more than 70 million accounts in an attempt to crack down on the flood of propaganda and bots influencing news consumption, although more work needs to be done.[12]

No. 3: Third-Party Risk Is Getting More Complicated And Difficult To Control

Companies are still struggling to exercise effective risk management across their growing partner ecosystems. What sets many of these third-party mishaps apart is that companies invest so little in their due diligence of third parties. However, the ones that do put in the effort have been making good, tough decisions to protect their business and brand. Recent events have shown striking differences in approach and results:

- **Poor due diligence now affects mergers, acquisitions, and other relationships.** Companies may have a mature process to review a segment of their third-party relationships (e.g., suppliers) for a small scope of potential risk (e.g., financial instability). However, very few have comprehensive programs covering all categories of third-party risk. In an embarrassing disclosure, Marriott reported in November 2018 that hackers had access to roughly 500 million customer records of its subsidiary Starwood for at least two years before it acquired the company in 2016.[13] Just as embarrassing, consulting firms Bain & Company, KPMG, and McKinsey & Company all took heat for their lack of customer due diligence after accidentally assisting South African Revenue Service officials plunder state resources.[14]
- **Proactive third-party risk management protects the business and brand.** On the positive side, firms that anticipate third-party risk events have been able to sever relationships before they hurt their brand. In the wake of the February 2018 school shooting in South Florida, many banks,

airlines, retail stores, and other companies severed their business relationships with the National Rifle Association. Meanwhile, REI went a step further and stopped selling Bolle, CamelBak, and Giro brands, because their parent company, Vista Outdoor, also manufactures assault-style rifles.[15]

No. 4: GRC Vendors Will Push Robotics And Analytics To Keep Pace With Business

When it comes to machine learning and AI, even the most advanced tech companies such as Amazon and Google struggle with discriminatory or otherwise biased outputs from their data models.[16] As these initiatives take hold and represent larger portions of corporate revenue, compliance and risk management teams will need more-effective technologies to ensure their firms' automated processes, data models, and analytics engines produce their intended outcomes. Risk managers will need to get up to speed on AI, intelligent agents and chatbots, and RPA.[17] Risk and compliance use cases will transition quickly from theory to practice — with some early pilots already proving GRC value:[18]

- **Artificial intelligence will accelerate existing GRC processes.** Even early applications of automation and analytics can generate impressive GRC benefits.[19] IBM Watson's Compliance Assist solution helps legal and compliance pros with tasks related to eDiscovery and contract management, analyzing and visualizing risks hidden within the unstructured data of lengthy documents.[20]
- **Bots will support risk and compliance effort like control testing and risk mitigation.** Bots are poised to make major contributions to GRC functions by augmenting human work. Emagia offers its digital assistant Gia to assist CFO customers in their daily work routines. One task Gia performs on request is to query disparate ERP systems to extract relevant billing, legal, and M&A activity related to a common project.[21] There's also a new chatbot, Spot, on the market, which acts a whistleblower hotline interface for reporting workplace harassment and discrimination and Leena, which will automatically answer employees' HR questions.[22] The list of relevant GRC bots will surely expand.

Recommendations

Recalibrate Your Risk Register; Embrace New Technologies

Business and technology changes are going to drastically shift the risk landscape for businesses over the next five years. For example, you'll have to widen the scope of your risk assessments to take data integrity risks, third-party risks, and risks to customer and employee sentiment. Thankfully, you'll also have access to many of these same new technologies to lighten your load and broaden your scope as needed. Amid this chaos, put yourself and your company in the best position to capitalize on new opportunities:

- **Embrace advanced analytics and automation.** As automation becomes commonplace, risk management leaders will need to foster their team's science, technology, engineering, and math (STEM) skills as well as robotics quotient (RQ), which measures people's ability to work with automated entities.[23] The internal audit team at the Australian bank ANZ is in the process of training

all of its staff on data analytics and has updated its staff capability and development framework to reflect new automation and analytics skill priorities.[24] As the bank pushes toward AI and automation, it's also encouraging employees to pursue a master's degree in data analytics.

› **Focus on ethics and values as regulatory guidelines fail.** Many of the technical, data, and customer engagement decisions your executive colleagues will make in the next five years will take the company into uncharted territory. Previously, when adopting a new technology, releasing a new product, or testing a new business model, it was often good enough to have the legal team review applicable laws and set guidelines. Now, as legal guidelines don't exist for many of the initiatives we'll soon face, you'll have to facilitate conversations to determine how ethical implications, customer and employee expectations, and corporate values guide your direction.

› **Reconsider how you categorize and measure risk.** The astronomical value of intangible assets means that any risk with a potential brand impact should likely rise to the top of your enterprise risk register. You should also consider the complexity of your firm's third-party ecosystem and reliance on those firms maintaining a high degree of consistency, resilience, and performance. Very few of these risks fit into traditional operational, financial, or reputational categories; instead, categorize risk based on which assets it targets, the source of the risk, and the different types of potential impacts.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Endnotes

[1] See the Forrester report "GRC Vision 2017-2022: Customer Demands Escalate As Regulators Falter."

[2] Source: "October 2016 Wells Fargo Mini-Study," cg42, October 2016 (http://cg42.com/wp-content/uploads/2016/12/cg42-Wells-Fargo-Mini-Study-102016vF.pdf).

[3] Source: Mike Isaac, "Uber Founder Travis Kalanick Resigns as C.E.O.," The New York Times, June 21, 2017 (https://www.nytimes.com/2017/06/21/technology/uber-ceo-travis-kalanick.html).

[4] Source: Alex Abad-Santos, "Nike's Colin Kaepernick ad sparked a boycott — and earned $6 billion for Nike," Vox, September 24, 2018 (https://www.vox.com/2018/9/24/17895704/nike-colin-kaepernick-boycott-6-billion).

[5] Source: Daisuke Wakabayashi, Erin Griffith, Amie Tsang, and Kate Conger, "Google Walkout: Employees Stage Protest Over Handling of Sexual Harassment," The New York Times, November 1, 2018 (https://www.nytimes.com/2018/11/01/technology/google-walkout-sexual-harassment.html).

[6] Source: Hamza Shaban, "Amazon employees demand company cut ties with ICE," The Washington Post, June 22, 2018 (https://www.washingtonpost.com/news/the-switch/wp/2018/06/22/amazon-employees-demand-company-cut-ties-with-ice/?utm_term=.c9573dc3b897).

[7] Source: Chris Kahn and David Ingram, "Americans less likely to trust Facebook than rivals on personal data: Reuters/Ipsos poll," Reuters, March 25, 2018 (https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3).

[8] GDPR is the most dramatic change in data protection and governance in the last 20 years — and jurisdictions around the world are using it as a model for their own regulations. To help security, privacy, and other risk professionals cope, we reviewed the emerging vendors in the GDPR compliance and privacy management software market. For more on the market we uncovered, see the Forrester report "New Tech: GDPR And Privacy Management Software, Q4 2018."

[9] As organizations rush to capitalize on the value of data, security leaders who have historically emphasized data confidentiality will face a new battle over data integrity, where malicious actors tamper with, corrupt, and manipulate the data on which insights-driven businesses depend. We examine the new investments, capabilities, and roles that security leaders will need so they can give their business colleagues confidence to use and trust the data they collect. For more information, see the Forrester report "Beware The Coming Data Integrity Crisis."

[10] To learn more about common bot attack patterns and the best ways to prevent them, see the Forrester report "Stop Bad Bots From Killing Customer Experience."

[11] Source: Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," The Telegraph, April 23, 2013 (https://www.telegraph.co.uk/news/worldnews/barackobama/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html).

[12] Source: Craig Timberg and Elizabeth Dwoskin, "Twitter is sweeping out fake accounts like never before, putting user growth at risk," The Washington Post, July 6, 2018 (https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/).

[13] Source: Taylor Telford and Craig Timberg, "Marriott discloses massive data breach affecting up to 500 million guests," The Washington Post, November 30, 2018 (https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests).

[14] Source: Renee Bonorchis, "Bain says guilty of 'serious failure' with Sars," Moneyweb, December 19, 2018 (https://www.moneyweb.co.za/news/south-africa/bain-says-guilty-of-serious-failure-with-sars/).

[15] Source: Gene Johnson, "REI to halt sale of CamelBak, other brands because parent company also makes assault-style rifles," Chicago Tribune, March 2, 2018 (http://www.chicagotribune.com/business/ct-biz-rei-vista-outdoor-20180302-story.html).

[16] As organizations apply advanced analytics and AI throughout their IT, operational, and customer-facing environments, the threat of biased machine learning models grows. We demonstrate how biased models are bad for business and the severe business impact they can cause — all with reputational, regulatory, and revenue consequences at stake. See the Forrester report "The Ethics Of AI: How To Avoid Harmful Bias And Discrimination."

[17] Automation technologies include a wide range of technologies, all of which drive improvements in scale, velocity, and other business metrics. In fact, the potential of this next line of automation is so great, Forrester believes it will revolutionize the business impact of technology. See the Forrester report "The CIO's Guide To Automation, AI, And Robotics."

[18] For example, Cognizant helped a major life sciences company implement RPA to tackle burdensome quality management and safety reporting requirements. Cognizant developed specially tailored bots to take over the formerly manual activities of data entry, sorting, and submission preparation for associated safety reports — resulting in a fully automated, zero-touch process. As a result, the life sciences company saw reporting time reduced by 30%, first-time form accuracy improved from 85% to 99%, related regulatory compliance rise from 95.7% to 96.1%, and on-time compliance improved from 88.6% to 91.9%. Source: "Pioneering Robotic Process Automation at a Major Life Sciences Company," Cognizant (https://www.cognizant.com/case-studies/life-science-robotic-process-automation).

[19] The evolving systems, technologies, and data dynamics underlying advanced analytics use cases can have meaningful implications for GRC. In particular, these sophisticated tools and techniques that analyze massive quantities of structured and unstructured data can build meaningful digital risk insight that automates associated process at unprecedented speed and scale. See the Forrester report "Build Digital Risk Insight."

[20] Source: "Watson Business Solution: Compliance Assist on IBM Public Cloud," IBM (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=21014921USEN).

[21] To learn more about how to successfully enhance employee productivity with technology, see the Forrester report "The Technology-Augmented Employee."

[22] Source: Victoria Turk, "This bot for workplace harassment takes the bias out of reporting," Wired, October 9, 2018 (https://www.wired.co.uk/article/julia-shaw-spot-ai-workplace-harassment-reporting-startup) and Ron Miller, "Leena AI builds HR chatbots to answer policy questions automatically," TechCrunch, June 29, 2018 (https://techcrunch.com/2018/06/29/leena-ai-builds-hr-chat-bots-to-answer-policy-questions-automatically/).

[23] Forrester's definition of robotics quotient (RQ) is: "A measure of the ability of individuals and organizations to learn from, adapt to, collaborate with, trust, and generate business results from automated entities, including software like RPA, AI, physical robotics, and related systems." See the Forrester report "RQ: Assess Your Readiness For Working Side By Side With Robots And AI."

[24] Source: "2018 State of the Internal Audit Profession Study," PwC (https://www.pwc.com/us/en/services/risk-assurance/library/internal-audit-transformation-study.html).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.