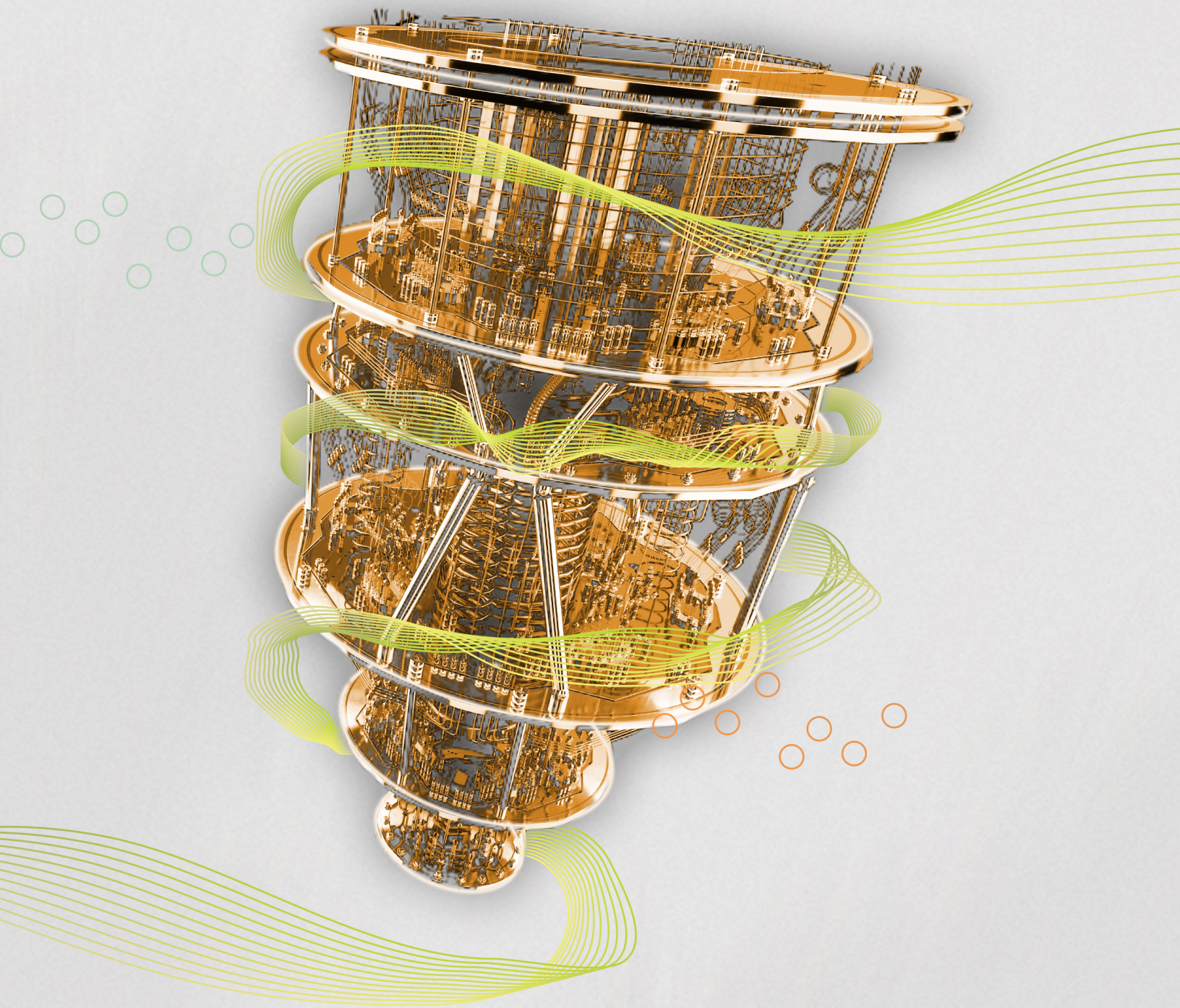
Industry spending on quantum computing will rise dramatically. Will it pay off?

Many financial services firms will load up on quantum technologies to enhance capabilities and gain a competitive edge. But they may need to play defense first.

Deloitte Center for Financial Services



Deloitte.
Insights

Quantum computing services

Quantum technologies, and their heady promise, are in the news. With the promise of breakthrough innovations in drug development, financial modeling, climate change, traffic optimization, machine learning, batteries, and more, is now the time to invest? And how much worry is warranted about quantum computing's future ability to break today's encryption? Today, the state of the mind-bending technology remains limited. Yet, tomorrow's breakthroughs are unknown. How should business leaders think about the potential and the promise of these technologies? Learn more.

Table of contents

The age of quantum computing is fast approaching, and the financial services industry should prepare now. Increased capital investments and patent filings for hardware technology indicates spending on quantum-related capabilities will likely grow quickly over the next few years.[1] Globally, the financial services industry's spending on quantum computing capabilities is expected to grow 233x from just US$80 million in 2022 to US$19 billion in 2032, growing at a 10-year CAGR of 72% (figure 1).[2] Firms that are working on developing quantum-related capabilities now could enjoy a competitive advantage as these capabilities mature.

Quantum computers are expected to radically enhance computational capabilities for complex mathematical operations, such as financial simulation and modeling.[3] They could also pose a risk to cybersecurity.[4] This risk arises from their potential ability to implement an algorithm developed in 1994 by Peter Shor (Shor's algorithm), which would render a lot of current-day cryptography obsolete.[5] Although the timeline for such an attack to be mounted is uncertain, the need to mitigate the cybersecurity risk is so significant that the time to act is now.

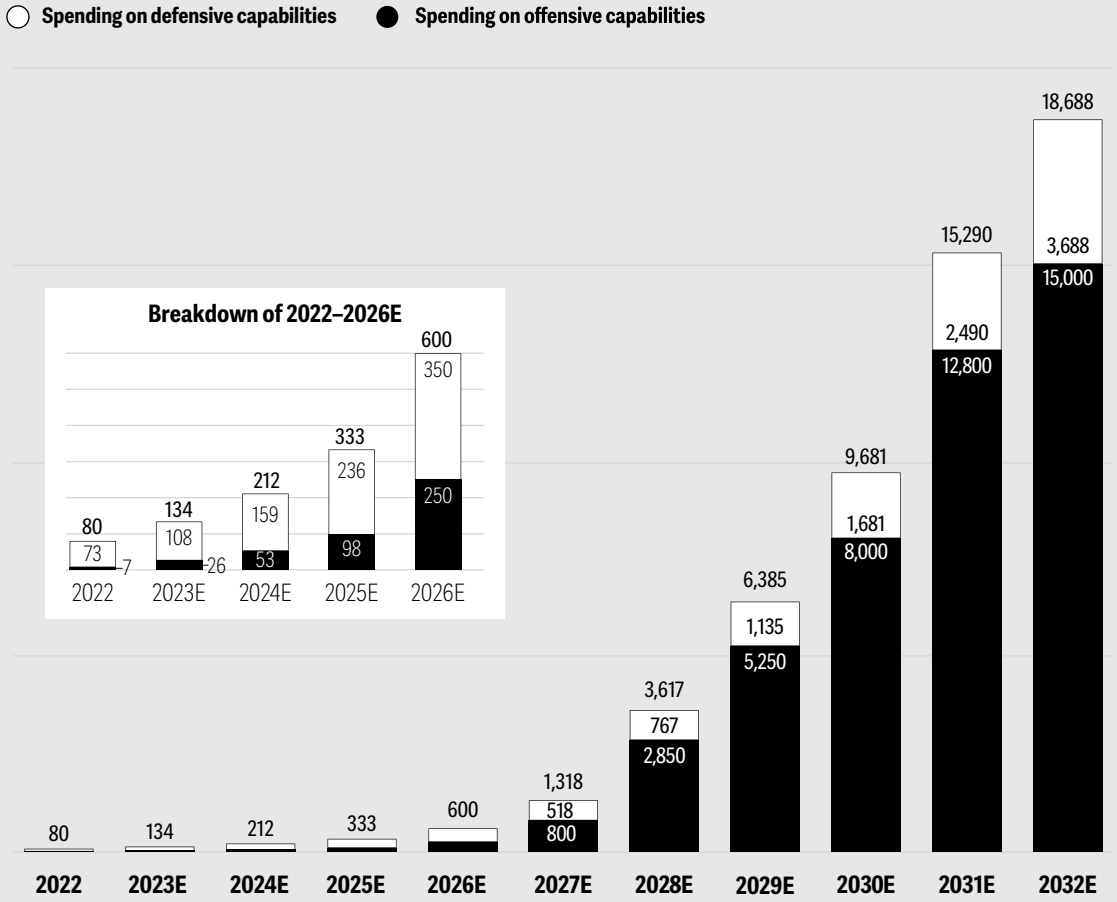
On the software and services side, two factors are driving rapid adoption: increased demand due to quantum cybersecurity vulnerabilities and the coalescence of entrepreneurial firms with point solutions that, in aggregate, provide a comprehensive mosaic of cybersecurity services. These groups are guided by solution aggregators that identify emerging technologies and guide entrepreneurs in their collaboration efforts.[6] The point of this process is to harness emerging technologies to help provide broad solutions while mitigating the risks normally associated with implementing leading-edge technologies.

As technology develops and vulnerabilities grow, adoption of quantum computing-focused technologies will likely increase dramatically. On the growth side of the coin, there may be less urgency, but some firms are preparing nonetheless to generate revenue and delight customers with quantum computing enabled capabilities. But before those goals can be achieved, firm leaders may need to play defense—as with more power can come more threats.

Figure 1

The financial services industry's spending on quantum computing is expected to rise significantly

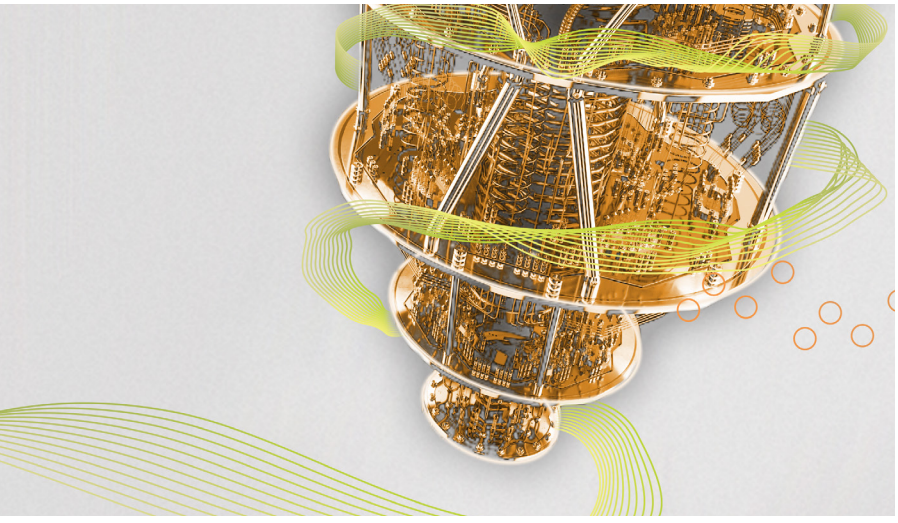
FSI spending on quantum computing capabilities (US$ million), 2022–2032



Note: We calculated defensive spending using the median quantum cryptography market size estimates of multiple market research reports with adjustments to get the share of the FSI spending. The offensive spending is a summation of the estimated spending on quantum computing talent and hardware by FSIs.
Source: Deloitte Center for Financial Services analysis.

Defending their turf: Protecting assets and enhancing cybersecurity on a quantum playing field

FSIs defensive spending in regard to quantum computing over the next few years is expected to focus on mitigating quantum-computer powered cybersecurity attacks. Data is important to industries such as financial services that handle large amounts of monetary transactions and maintain a record of vast volumes of sensitive client information. FSIs will likely be the primary target for quantum computer cyber attacks and data breaches. Industry vendors warn that quantum computers, when commercially available over the next couple of years, will likely be able to break public key encryptions, which secures 90% of all global encrypted data.[7] In fact, in the United States, a single quantum attack that disrupts access to the Fedwire Funds Service payment system for one of the five largest financial institutions would lead to cascading financial failures impacting the US GDP to the tune of US$2.0– US$3.3 trillion.[8] Some hackers are even harvesting encrypted data now with the intention of decrypting the data retroactively using a commercially available quantum computer, making this cybersecurity threat a current, not future, problem.[9]



INNOVATION IN POSTQUANTUM CRYPTOGRAPHY (PQC)[10]

Some firms are preparing to counter the potential threats that quantum computers bring. PQC has been in development for several years. PQCs are new quantum-resistant cybersecurity techniques that will have to be deployed to secure data and transactions in the future. One such emerging quantum-resistant technology uses a blockchain approach to encrypt data at the record level with a hardware-enhanced, postquantum cryptography-secure key for each data element. The innovation in this approach is twofold. First, data is secure inside the perimeter, rather than being another fence around unsecure data elements. Second, with the blockchain approach, the data and its administrative records are immutable, and tampering is traceable.[11] PQC will likely emerge with capabilities to mitigate risk based on new, government-approved techniques, coupled with novel approaches.[12]

When the National Institute of Standards and Technology postquantum cryptographic standards are finalized and published for use in 2024, this could serve as the foundation for a regulatory push toward quantum-resistant cryptography in the financial services industry.[13] With the upgrade from current cryptography to quantum-resistant cryptography, all current sensitive information may have to be reencrypted and cryptography algorithms upgraded to be quantum-resistant. The new setup will likely require significant investment in hardware, software, communications, and infrastructure. Investment in system upgrades and regulatory compliance will likely drive the quantum-resistant cryptography market for the financial services industry over the next 10 years.

Playing to win: How quantum computing can help organizations improve customer engagement and generate additional revenue

Financial services firms are also using quantum computing to get ahead. These offensive use cases include Monte Carlo simulations, portfolio optimization, risk minimization, and complex derivative calculations.[14] Quantum computers may also be used to improve the ability of AI to derive useful information from large volumes of data.[15] Firms can also leverage the power of quantum computers to elevate the customer experience by processing customer inputs and behavior to predict their needs in near real-time.[16]

FSIs' spending on quantum computing offensive use cases is lagging defensive spending because full-scale quantum computers are not commercially available as of mid-2023.[17] Even so, spending on quantum technologies such as quantum annealers, for specific use cases, has started at firms that have made the strategic choice to be

"If you accept that there is a finite probability that a quantum computer capable of breaking asymmetric cryptography will exist, say within the next ten years, how long will it take you to upgrade your cryptographic infrastructure, and what is the expected lifetime of your data? If you do not yet know the answers to these questions, the time to act is now! Once you know these answers, you can start to prioritize your efforts and be better prepared once standards are finalized."

—Colin Soutar, Managing director, Deloitte & Touche LLP

leaders in quantum computing. These firms are expected to switch to more powerful quantum computing hardware when it becomes commercially available.

Exploiting the advantages of quantum computing requires different expertise than what is learned through programming and architecting traditional IT systems.[18] For this reason, a few FSIs, among them Goldman Sachs, JPMorgan Chase, HSBC, and Barclays, have formed teams to figure out the problems they want to address with quantum computers and programming solutions to be effective in a quantum computing platform.[19] Quantum computing capabilities can help organizations to create an information advantage over competing FSIs that can be sustained for at least the initial phase of quantum computing adoption, which may last several years.

If quantum computing reaches mass adoption in the early 2030s as expected, the information advantage will likely shift to information parity. However, the quantum capability will be no less valuable. It will likely become a necessity for at least a few areas of operation, where speed and comprehensiveness contribute to the value of business process optimization.

Firms that plan to be early movers on the offensive side will likely have to start exploring and experimenting with the potential use cases of quantum computing. On the defensive side, firms can start by inventorying their data and systems for the upcoming transition to postquantum cryptographic standards. With the combination of urgency and opportunity, quantum spending in FSIs has already begun and spending will likely accelerate for at least the next 10 years. At some point in the future, we may even see a time when quantum computing is the norm, and it is just called "computing."

Endnotes

1. Doug Dannemiller, Krissy Davis, Julia Cloud, and Tony Gaughan, *2023 investment management outlook*, Deloitte Insights, October 7, 2022.
2. Deloitte Center for Financial Services analysis: Defensive spending is calculated using the median quantum cryptography market-size estimates of multiple market research reports with adjustments to get the share of the FSI spending. The offensive spending is a summation of the estimated spending on quantum computing talent and hardware by FSIs.
3. Filipe Beato, Anne Ardon, Itan Barmes, and Chris Knackstedt, *Transitioning to a quantum-secure economy*, World Economic Forum and Deloitte, September 2022.
4. Ibid.
5. Deloitte, *Future forward readiness: Quantum risk*, 2022.
6. Joe Faxlanger (Cyber Solutions Executive, RockITek), virtual interview with the author, March 31, 2023.
7. Skip Sanzeri, "Banks need to act now to ensure post-quantum cybersecurity," *Security Today*, March 7, 2022.
8. Arthur Herman and Alexander Butler, *Prosperity at risk: The quantum computer threat to the US financial system*, Hudson Institute, April 3, 2023.
9. Nancy Liu, "'Harvest now, decrypt later' concern boosts quantum security awareness," SDxCentral, September 28, 2022.
10. Deloitte Center for Financial Services analysis.
11. Lara George (Co-founder, Walacor), virtual interview with the author, March 27, 2023.
12. Joe Faxlanger (Cyber Solutions Executive, RockITek), virtual interview with the author, March 31, 2023.
13. Deloitte, *Future forward readiness*.
14. Finance Magnates, "Harnessing quantum computing for financial analysis and risk management," April 13, 2023.
15. Aaron Raj, "Here's how quantum computing can enhance financial services," Techwire Asia, January 18, 2023.
16. Jonathan Ruane, Andrew McAfee, and William D. Oliver, "Quantum computing for business leaders," *Harvard Business Review*, January–February 2022.
17. Deloitte, *Future forward readiness*.
18. Dannemiller, Davis, Cloud, and Gaughan, *2023 investment management outlook*.
19. Greg Noone, "Who are the early adopters of quantum computers? Big banks, that's who," Tech Monitor, January 12, 2023.

About the authors

Colin Soutar
csoutar@deloitte.com

Dr. Colin Soutar is a managing director in Deloitte Risk & Financial Advisory. He leads Cyber & Strategic Risk products and technology within the Government & Public Services practice and is the Deloitte US Cyber Quantum Readiness leader. Soutar has more than 25 years of experience in biometrics, digital identity, and cybersecurity technologies. He also serves on the World Economic Forum Global Future Council for Cybersecurity.

Scott Buchholz
sbuchholz@deloitte.com

Scott Buchholz serves as the national emerging technology research director for Deloitte Consulting. He also leads efforts in exploration of quantum computing and related technologies, working to solve customer challenges with these advanced technologies. As a chief technology officer for Deloitte Consulting LLP's Government and Public Services, he works with government clients to use technology to innovate in their operations, technology, and mission delivery.

Doug Dannemiller
ddannemiller@deloitte.com

Doug Dannemiller is the head of investment management research at the Deloitte Center for Financial Services in Deloitte Services LP. He is responsible for driving the center's research platforms and delivering world-class research for our clients. He has more than 20 years of experience in research, strategy, and marketing in the investment management and wealth management industries.

Mohak Bhuta
mobhuta@deloitte.com

Mohak Bhuta is an assistant manager at Deloitte Center for Financial Services in Deloitte Support Services India Private Limited. He focuses on research, analysis, and writing reports on the most current and pressing topics for the investment management industry.

Acknowledgments

Authors **Mohak Bhuta** and **Doug Dannemiller** wish to thank the following Deloitte Center for Financial Services colleagues for their insights and contributions: **Patricia Danielecki**, **Sean Collins**, **Neerav Shah**, **Alice Hartnett**, **Seth Raskin**, and **Paul Kaiser**.

About the Deloitte Center for Financial Services

The Deloitte Center for Financial Services, which supports the organization's US Financial Services practice, provides insight and research to assist senior-level decision-makers within banks, capital markets firms, investment managers, insurance carriers, and real estate organizations. The center is staffed by a group of professionals with a wide array of in-depth industry experiences as well as cutting-edge research and analytical skills. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights. Read recent publications and learn more about the center on Deloitte.com. For weekly actionable insights on key issues for the financial services industry, check out the Deloitte Center for Financial Services' QuickLook article series.

Connect

To learn more about the vision of the DCFS, its solutions, thought leadership, and events, please visit www.deloitte.com/us/cfs.

Subscribe

To receive email communications, please register at www.deloitte.com/us/cfs.

Engage

Follow us on Twitter at: @DeloitteFinSvcs

Contact us

Industry leadership

Monica O'Reilly
US Financial Services Industry leader | Principal | Deloitte and Touche LLP
+1 415 783 5780 | monoreilly@deloitte.com

Monica O'Reilly leads the US Financial Services Industry group focused on the banking, capital markets, insurance, investment management, and real estate sectors.

Center for Financial Services

Jim Eckenrode
Managing director | Deloitte Services LP
+1 617 585 4877 | jeckenrode@deloitte.com

Jim Eckenrode is managing director of the Deloitte Center for Financial Services, responsible for developing and executing Deloitte's financial services research agenda, while providing insights to leading financial institutions on business and technology strategy.

Doug Dannemiller
Research leader | Deloitte LLP
+1 617 437 2067 | ddannemiller@deloitte.com

Doug Dannemiller is the head of investment management research at the Deloitte Center for Financial Services in Deloitte Services LP. He is responsible for driving the center's investment management research and delivering it to clients.

Deloitte.
Insights

Sign up for Deloitte Insights updates at **www.deloitte.com/insights**

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Karen Edelman, Rupesh Bhat, Arpan Kumar Saha, Aditi Gupta, and Hannah Bachman
Creative: Natalie Pfaff, Alexis Werbeck, Meena Sonar, Govindh Raj, and Pooja Lnu
Deployment: Atira Anderson
Cover artwork: Natalie Pfaff