McKinsey & Company

Reaching the next normal of insurance core technology

Now more than ever, insurers are focusing on reimagining the role of technology, reinventing technology delivery, and future-proofing the foundation of core technology. Sixteen articles dive deep into the what, why, and how.

June 2020

Preface

The world looks very different now than it did just a few short months ago. As the COVID-19 pandemic has spread to every corner of the world, protecting employees and customers has been at the center of every leader's agenda. Insurers across geographies have demonstrated incredible resolve and resilience as they have taken workforces remote, rapidly mounted digital tools, and supported communities through this unprecedented global crisis.

Much remains uncertain, but one thing is clear: business will not return to the old normal. As insurers have adapted their processes and operating models to cope with physical distancing and shelter-in-place measures, leaders are debating the shape of the next normal and recognizing the opportunity to make some of these changes—particularly to core technology and digital capabilities—permanent.

From 2012 to 2017, technology's average share of operating costs rose by 24 percent (for P&C) and 12 percent (for life).[1] However, there is a large difference among carriers in terms of what they get out of their investment in IT. Some have managed to jump to a new frontier of productivity and operational performance, while others are still not getting the full value out of their investment.

Make no mistake: insurers' ability to thrive in the next normal will hinge on the quality and flexibility of their IT setup. And these strides in digitization and automation—and the subsequent requirements of the technology function—will most likely become table stakes after the crisis subsides.

The next normal: Reimagine, reinvent, and future-proof

In the past few years, advances in technology, data, and analytics have been accelerating the fundamental reshaping of insurers' cost structures. COVID-19 has only increased the urgency to sustainably reduce expenses and deliver business capabilities.

The next normal of core technology will see insurers making the leap from traditional to modern IT that is on the frontier of technology and operations efficiency (exhibit). Companies at the vanguard are able to deliver more business capabilities with the same amount of spending. These gains have already led several incumbents to invest the time, money, and resources in core technology transformations.

The transformation needed to reach the efficient frontier requires three bold actions: reimagining the role that the technology function plays with respect to other business functions, reinventing the manner in which the technology function delivers products and services to customers and internal users, and future-proofing the quality of the underlying technology systems that provide the organization with essential capabilities.

---

[1] Tonia Freysoldt, Sylvain Johansson, Christine Korwin-Szymanowska, Björn Münstermann, and Ulrike Vogelgesang, "Evolving insurance cost structures," April 11, 2018, McKinsey.com.

Fundamental shifts are needed to reach the efficient frontier in technology and operations.
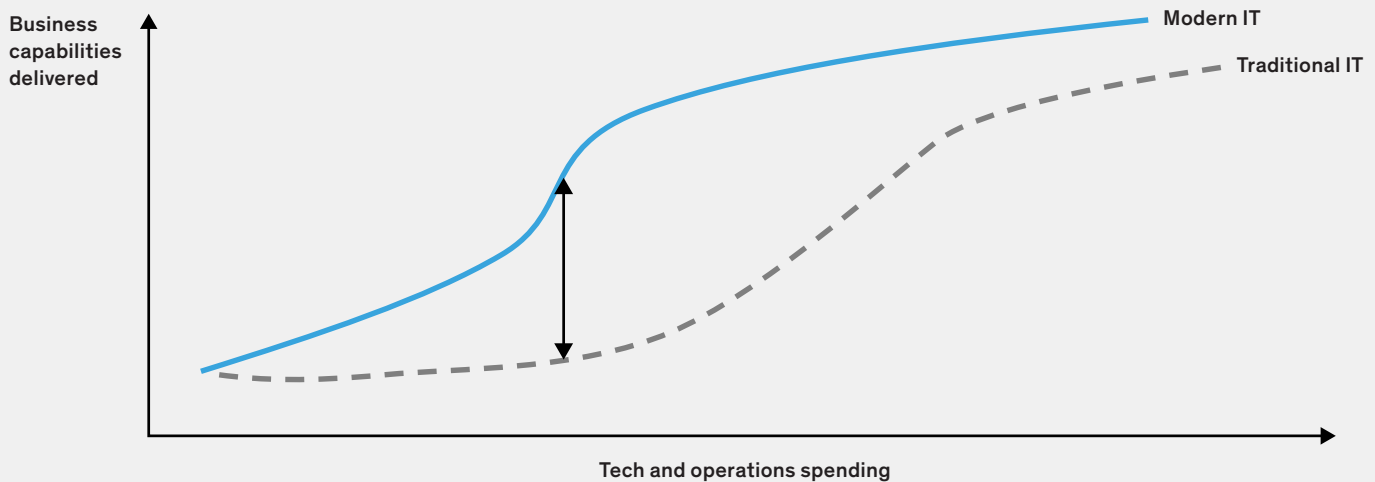
Starting the journey

In this compendium, *Reaching the next normal of insurance core technology*, we begin with two articles detailing how insurers can achieve resilience amid the new world formed by the COVID-19 pandemic and how CEOs can orient the technology function to focus on the company's strategic priorities. The articles in the three chapters that follow explore reimagining the role of technology, reinventing technology delivery, and future-proofing the foundation. On the whole, the compendium offers a closer look at what it means to reach the next normal of core technology and operations and become a tech-led insurer, using examples from the insurance industry and beyond. The articles provide insight into the challenges that lay ahead for carriers as well guidance on how to navigate them—particularly in a world that has been so quickly and permanently changed by the COVID-19 pandemic.

We hope you will enjoy this compendium as much as we enjoyed putting it together. We are convinced that core technology will play an increasingly important role in shaping the future of insurance. We look forward to hearing your thoughts and discussing the future of core tech in insurance.

Krish Krishnakanthan
Senior partner, Stamford
Krish_Krishnakanthan@McKinsey.com

Ani Majumder
Partner, New York
Ani_Majumder@McKinsey.com

Björn Münstermann
Senior partner, Munich
Bjoern_Muenstermann@McKinsey.com

Peter Braad Olesen
Associate partner, Copenhagen
Peter_Braad_Olesen@McKinsey.com

Contents

Reinvent technology delivery

Future-proof the foundation

Insurance resilience in a rapidly changing coronavirus world

In times of uncertainty, carriers can pursue resilience through a staged approach to stabilizing, reimagining, and transforming operations.

by Anshuman Acharya, David Hamilton, Pradip Patiath, Zachary Surak, Grier Tumas Dienstag, and Jasper van Ouwerkerk

There is no question that addressing the humanitarian challenge of COVID-19 is the first priority of every government, business, and individual around the world. We're seeing enormous energy invested in suppressing the virus and saving lives with rigorous social measures and millions of heroic healthcare professionals and first responders putting their own lives at risk.

As the situation evolves hour by hour and day by day, it is difficult to predict its consequences with certainty. One certainty, however, is that the pandemic brings both balance-sheet and operational challenges to the insurance industry. Following are some of the most acute challenges that we are observing and anticipating for the near future across the global life and property and casualty (P&C) sectors:

Pricing, product, and balance-sheet disruptions

— Drops in interest rates forcing adjustments to new-business pricing and putting significant pressure on in-force blocks with rate-sensitive guarantees, particularly those written before the global financial crisis of 2007–08

— Risk of credit migrations leading to further balance-sheet challenges (for example, declining reserve ratios) and broader instability in financial markets (for example, disruption of normal money movements)

— Possibility of variable annuities with equity-linked guarantees breaking their hedges if the equity markets decline further

— Potential for reduced appetite for higher-value policies in a subsequent recession

Operational disruptions
— Disruption of new business and underwriting due to widespread dependence on paper applications and lost momentum in field operations caused by physical distancing

— Policy-servicing disruptions, with customer queries about parameters of coverage exceeding call-center capacity

— Performance erosion in the absence of robust work-from-home (WFH) capabilities

— Increased cyberrisk due to employees accessing systems from their home networks

Yet the crisis also presents an occasion to think hard about fostering and accelerating innovation, delivering improved customer experiences, fundamentally changing the cost structure, and upskilling and reskilling employees for the future. In addition, it reasserts the industry's relevance as a safe harbor in times of uncertainty.

Successful COVID-19 responses from Asia have taught us four important lessons: go for pragmatic and fast solutions rather than perfect solutions (speed is a strategy unto itself), adapt a new digital way of working to engage agents and customers, stay close to customers and provide them with valuable information, and seek innovation in products, distribution, and customer reach. This article is meant to provide global carriers' decision makers with a map to tackle immediate challenges while balancing the fiduciary responsibility of positioning the business for the future. We focus here on enablers for building resilience.

Tactical and strategic levers for life and P&C carriers

Based on our global experience, especially in Asia and Western Europe, we believe that navigating this new world and emerging in the "next normal" requires a comprehensive and ambitious response across five stages—resolve, resilience, return, reimagination, and reform.[1] In this article, we consider a broad set of tactical and strategic levers for insurers across these stages—including innovating the product portfolio, driving channel migration, accelerating the move to fee-based earnings, making in-force management

---

1 For more, see Kevin Sneader and Shubham Singhal, "Beyond coronavirus: The path to the next normal," March 2020, McKinsey.com.

a strategic priority, rethinking the cost base, and upgrading talent and ways of working.

Resolve: Starting with no-regret moves

In the early days of a crisis, much of the focus has rightly been on mitigating risks for employees and ensuring operational continuity. In the most successful instances, carriers have been able to do both using the following playbook.

Expand work-from-home arrangements to all possible functions. Many insurers have already expanded work-from-home (WFH) orders to as much of the company as possible. Doing so helps to protect the health and safety of employees during the pandemic, provide continuity through the crisis, and build a strategic capability for the future. Where capabilities already exist, WFH arrangements can be scaled up with the use of clear policies and expectations and the tools and resources (high-speed internet, server/application virtualization, rapid training, and so on) employees need for collaborating internally and externally while adhering to local shelter-in-place (or similar) requirements.

For functions that typically do not allow for WFH arrangements, introducing the right workforce management behaviors and operational discipline can support productivity as well as the mental health of employees. Individual function and line leadership can turn to proven remote-working models, such as adopting daily check-ins and checkouts and frequent touchpoints in place of typical in-person staff meetings and team huddles to identify and resolve issues. It is important to rapidly establish norms for the use of collaboration tools and protocols for confidentiality and data protection to contain the risk imposed by the migration of the work environment to individuals' homes. Several enterprises in China offer helpful lessons for adapting the workforce to WFH arrangements.[2]

Prepare IT for critical-services capacity and heightened cybersecurity needs. IT preparedness for security and bandwidth needs has been

a bottleneck for some firms setting up WFH capabilities. Across the insurance industry, some carriers have shelved their remote-video capabilities to reduce bandwidth usage on their virtual private networks. By stress-testing their capabilities and adjusting capacities urgently, IT leaders can ensure continuity during the crisis, as well as reduce security risk. Further, IT leaders need to be aware of new cybersecurity threats that WFH arrangements present and consider several steps, such as accelerating the monitoring of collaboration tools, networks, employees, and end points.[3]

Resilience and return: Weathering the crisis

Given the uncertainty about the duration of COVID-19 in individual markets, a clear priority is the development of contingencies for the possibility of extended impact, including the potential for second and third waves of the virus. Building these contingencies requires taking a hard look at initiatives that will improve both the use of resources and field productivity.

Get a cross-enterprise handle on cash flows and both internal and third-party capacity. Carriers should prepare for decreased demand for products and resulting expense overruns. "P&L control towers," which monitor and manage premium and revenue inflow, as well as spending on procured products and services, can flex more dynamically than standard business units or procurement departments typically allow. Similarly, "HR control towers" manage employee upskilling and reskilling needs, as well as the recruiting pipeline, while balancing capacity for claims handlers and other positions with spiking demand.

Accelerate digital engagement across the customer journey. As billions of people shelter in place, the importance of digital interactions takes unprecedented priority. Insurers that have developed mature digital functions in sales and distribution, service and retention, and claims are well positioned to weather the crisis—and those that haven't must act fast to catch up:

---

[2] For more, see Raphael Bick, Michael Chang, Kevin Wei Wang, and Tianwen Yu, "A blueprint for remote working: Lessons from China," March 2020, McKinsey.com.

[3] For more, see Jim Boehm, James Kaplan, and Nathan Sportsman, "Cybersecurity's dual mission during the coronavirus crisis," March 2020, McKinsey.com.

— *Sales and distribution.* There has never been a better time to encourage sales forces and intermediaries to abandon paper and move everything—from digital lead generation to binding agreements—online, enabling reps and agents to remain productive without putting them in physical risk. In the face of COVID-19, Chinese insurers rapidly adopted video and messaging apps to enable an end-to-end customer journey that facilitates customer authentication, face-to-face digital meetings, and application completion and execution. In some cases, technology is enabling wholesalers to see 30 to 50 percent more prospects on a weekly basis. By moving entirely online, carriers can also accelerate remote and digital agent recruiting and onboarding.

— *Service.* In moments of distress, carriers would do well to increase the focus on the customer by designing and migrating to new customer journeys and automated digital service channels for all steps of the value chain. Carriers can eliminate paper forms entirely by using existing technology, such as video claims appraisal, self-serve profile changes, and a messaging-app-based first notice of loss. Leaders can rapidly expand digital-channel adoption not only for standard requests but also for new requests arising from the crisis (for example, to check coverages in lines of business affected by employee wellness, life events, or work stoppages).

— *Claims.* Carriers could start by adopting and scaling approaches to deliver simplified and convenient claims service, including increasing reliance on video-enabled adjustment for lines that cover physical damage. In the intermediate term, carriers can replace the manual process of uploading medical records and reviewing bills with automated feeds, as well as use natural language processing to gain insight from customer and claimant emails. Doing so will help claims organizations mature toward more straight-through processing, starting with simple claims, such as property damage auto

claims or medical-only workers' compensation claims. Accelerating such transformations can drive structural efficiencies in end-to-end claims and protect against future outsourcing provider interruptions and spikes in claim volume.

Strengthen collections and fraud detection. Given the economic slowdown, which is hitting small and midsize businesses and consumer segments the hardest, collections chargeoffs and fraud will likely spike in the coming months—similar to what the industry experienced in the past two recessionary cycles. Life and P&C carriers should take preventive steps to minimize operational disruption and develop and implement strategies to manage credit-risk exposure.[4] They might increase sensitivity to early-warning systems, for example, or pilot a contingency strategy in the event that call-center capacity is depleted by more than 50 percent.

The crisis will test a carrier's brand and customers' loyalty, so strengthening collections needs to be balanced with retention of at-risk customers. Carriers can consciously provide lenient arrangements to delay or spread out payments for loyal customers or specific product lines with higher risk of attrition.

Reimagination and reform: Emerging from the crisis
As regions exit the most critical crisis period, a "new normal" will set in. However, the lasting impact on the population and economy will be dramatic, affecting the demand for insurance for years to come. While taking that into account, carriers will at some point be able to focus again on longer-term strategies and initiatives.

Drive structural improvements. Since the 2007–08 financial crisis, the cost structure in insurance, as a percentage of premium, has deteriorated, indicating that the industry as a whole has not prioritized productivity improvement.[5] Once carriers have stabilized operations and started reimagining their processes and customer journeys, they can take real, urgent action to embed the changes within their core operations and beyond. A transformation office reporting to the CEO (discussed in the next section) can be empowered to set bold targets, leave

---

[4] For more, see Ademar Bandeira, Bruno Batista, Adelmo Felipe, Matt Higginson, Frédéric Jacques, Frederico Sant'Anna, and Alexandre Sawaya, "Addressing the needs of customers in delinquency impacted by the coronavirus," March 2020, McKinsey.com.
[5] Bernhard Kotanko, Björn Münstermann, Pradip Patiath, Jasper van Ouwerkerk, and Ulrike Vogelgesang, "The productivity imperative in insurance," August 2019, McKinsey.com.

no stone unturned to identify opportunities, marry transparency with individual accountability, and adopt incentives that reward superior performance. Banking, telecom, and consumer products have all successfully demonstrated the value of taking a zero-based budgeting and operating approach to drive structural improvements across the entire cost base. The insurance industry will soon look to do the same.

Future-proof the organization. As the crisis resolves, carriers can take a comprehensive approach to redesigning their operating models, to both reduce dependence on legacy operations and increase resilience during future events. This approach could include exploring geographic disaster recovery, site operational risk protocols, supply chain resilience (for example, business process outsourcing and vendor redundancy), and workforce flexibility. Finally, carriers may also consider introducing new products suitable for a recessionary economy, such as higher-face-value life insurance policies without a medical exam and basic and more price-competitive small-business insurance.

Organizing for resilience: A practical way to get started

Despite the significant uncertainty created by COVID-19, carriers cannot afford to wait and observe how the situation evolves. It is essential to rapidly deploy an ambitious, top-down resilience plan across the five stages, while engaging the full gamut of levers across the value chain. To execute and balance immediate action with flexibility to tackle evolving challenges, insurers can mobilize resources organized into three teams: a disruption office focused on resolve and stabilizing operations, a strategy office dedicated to resilience and return, and a transformation office to reimagine, reform, and embed the changes (exhibit).

Disruption office: Stabilize operations (weeks 1–4):
Carriers that haven't already done so should consider launching a disruption office, possibly led by the chief operating officer, which would be an integrated "nerve center" to ensure the adequate

discovery of risks, coordinate the portfolio of remedial actions based on scenarios and triggers, and deploy sufficient resources where and when needed.[6] The core objectives of this team would be to work through bottlenecks and keep the response moving while allowing autonomy for core operations to maintain continuity and for strategists to think about the future road map.

An effective cadence would include specific, rolling 48-hour and one-week goals to achieve near-term priorities and a dashboard to track progress and manage threats in real time. The team's focus would span the spectrum of stakeholders—employees, customers, and the business. The following are some of the common actions carriers are implementing to stabilize their operations:

— Employees: Rolling out measures to tackle the changing environment and communicate the carrier's support—for example, more flexible working times, childcare subsidies

— Customers: Ensuring that customer-care units are reachable; keeping customers informed of capacity constraints; deploying self-service, automation, and additional capacity to tackle personnel shortages in service-critical functions; and minimizing customer-data risk of cyber exposure

— Business: Ensuring business continuity by immediately stress-testing solvency; modeling cash-flow, P&L, and balance-sheet impact in three or four scenarios; and identifying potential triggers of significant liquidity events. They also are adjusting new-business pricing, taking into account new economic variables, and (most applicable to life insurers) considering removing some products from the shelf entirely.

Strategy office: Reimagine processes and journeys (weeks 1–8):
A strategy center can be used to implement a top-down, fresh perspective on the future operating model. The center can be led by the head of strategy or someone in another role who is well equipped

---

6 For more, see Mihir Mysore and Ophelia Usher, "Responding to coronavirus: The minimum viable nerve center," March 2020, McKinsey.com.

An illustrative action plan models actions of the disruption, strategy, and transformation offices.

| Week 1 | Week 16 | Potential leader[1] |

Disruption office
Stabilize operations (weeks 1–4)
- Ensure adequate discovery of risks.
- Coordinate remedial actions and deploy sufficient resources to take care of employees and customers.
- Establish rolling 48-hour and 1-week goals with dashboards to manage threats in real time.

Chief operating officer

Strategy office
Reimagine processes and journeys (weeks 1–8)
- Develop transformative road map for the new normal.
- Apply zero-based approach to design more resource-efficient processes, offering better customer experience.
- Scale approach across the value chain, from sales to servicing.

Head of strategy

Transformation office
Embed changes (weeks 4–16+)
- Set up robust execution engine, drive rigorous decision-making cadence, and implement radical transparency (impact, resource needs, and roadblocks).
- Establish common methodology for valuing impact and a digital program-management platform to provide clarity on initiatives.
- Create informed plan to maintain focus on organizational health and culture to achieve sustainable performance excellence.

Chief transformation officer

[1] In partnership with the CEO, chief financial officer, chief human resources officer, and chief information officer.

to understand the current operation but is also a visionary who will create a truly transformative road map for the new normal that can be rapidly deployed as the organization stabilizes.

This strategy team can apply a zero-based approach to reimagine processes and customer journeys. The approach considers the minimum (zero-based) budget, staffing, and external spending required to maintain baseline operations, from sales and distribution to in-force servicing. Processes can then be built using analytics, automation, and sourcing best practices to design a more resource-efficient alternative that also offers improved customer experience. These efforts will make possible several of the digital journeys discussed in the previous section.

Transformation office: Embed the changes (weeks 4–16+):

As a carrier stabilizes, it will be able to mobilize the broad participation of the organization during the crisis to embed the new normal into the fabric of the company. Doing so requires the carrier to set up a robust execution engine, led by a chief transformation officer who drives the weekly cadence of decision making (not process) and creates radical transparency—of impact, interdependencies, resource needs, trade-offs, and roadblocks. Coupling this engine with a common methodology and language for evaluating impact and a digital program-management platform will help the carrier understand the maturity and progress of each initiative.

Second, the carrier can fundamentally rebase expectations of its people and footprint, starting with an evaluation of what it was able to achieve while operating in an entirely remote manner and with capacity constraints. Leaders are now learning, on a whole new level, what their teams are capable of—and it will be important to ensure that those breakthroughs aren't lost in a transition back to the physical office. Leaders can roll up what will probably be a large number of initiatives emerging from the strategy office into an integrated plan, against which they will be able to measure performance and set budgets going forward. Doing so would help avoid siloed or watered-down execution. In addition, carriers could formalize the remote-working model, cross-train their workforce, and embed flexibility into the operating model to ensure that they will be better poised to respond to future crises.

Of course, sustaining the new operating model requires an informed plan that focuses on organizational health and culture. The plan could be informed by an assessment of the elements that have bred the carrier's success, such as alignment with a shared vision, shared goals, and incentives at every level as well as clear roles and transparent performance.

———————

First and foremost, insurance leaders need to manage the immediate threat to people's health and well-being and be sensitive to those customers most affected by the crisis. To exit the crisis with a more customer-focused, efficient, and resilient organization, insurance leaders need to plan ahead, engage the gamut of strategic and tactical levers discussed here, and use radical transparency to advance change. Insurers can sustain momentum and make long-lasting changes even in the challenging times ahead.

This article was originally published on McKinsey.com in April 2020.

Anshuman Acharya is a consultant in McKinsey's Chicago office, where **Pradip Patiath** is a senior partner. **David Hamilton** is a partner in the Detroit office, **Zachary Surak** is a partner in the New Jersey office, **Grier Tumas Dienstag** is an associate partner in the Boston office, and **Jasper van Ouwerkerk** is a senior partner in the Amsterdam office.

© Xavierarnau/Getty Images

The CEO's new technology agenda

Technology performance has become critical to business success. Here's how a CEO can focus the technology function on a company's strategic priorities.

by Klemens Hjartar, Krish Krishnakanthan, Pablo Prieto-Muñoz, Gayatri Shenai, and Steve Van Kuiken

We have seen numerous companies boost their financial performance after their CEOs made it a priority to strengthen the technology function and bring more technology capabilities closer to the business's strategy and operations. Fulfilling this mandate, however, can be a challenge. Most CEOs already have a long slate of priorities, and relatively few feel comfortable enough with technology to push for transformative changes in that functional area. Even CEOs who are attuned to the threat of digital disruption and are thinking about how their companies can create value with digital tend to discount the IT function's importance.

Nevertheless, it's clear from our experience that CEOs can exert a uniquely constructive—and valuable—influence on the IT function. CEOs can do more than other executives to transform the IT function's role, resource model, and core systems, and to bring about the cultural and organizational changes that such transformations involve. In the following section of this article, we lay out the ten questions that CEOs should ask their chief

information officers (CIOs) and management teams to determine how capable their IT function is and how closely it is aligned with the business. We then lay out one CEO's successful approach to modernizing his company's IT function. Together, these insights offer CEOs a guide to shaping a technology function that's fit for the digital age.

The modern IT function: Concepts to know, questions to ask

Based on our extensive work with CEOs and top executives at large companies, three concepts define today's most effective IT functions: a new role that calls for collaboration with the business on strategy and operations; an updated resource model offering the talent, methods, and tools to accelerate innovation; and a future-proof technology foundation of flexible, scalable systems that speed releases of IT products. To help CEOs assess where their companies stand with respect to these three concepts, we have included ten key questions that CEOs can ask (exhibit).

Exhibit

Ten questions can help CEOs determine whether their companies' IT functions possess the qualities that make IT effective.

	Modern IT function	What the CEO should ask to accelerate technology transformation
Role	Collaboration with the business on shaping strategy and streamlining operations • Alignment between IT and the business • Targeted technology investments • Advocacy for end users	**1.** How are we making key technology decisions at all levels of the company? **2.** How do we track and maximize the value produced by our major technology investments? **3.** How often do our tech teams seek input from users?
Resource model	Talent, methods, and tools to accelerate innovation • Ample engineering talent • Agile working methods • Leading-edge tools • Targeted vendor partnerships	**4.** Have we placed high-caliber engineers in IT roles that contribute the most value to the company? **5.** How many projects has IT shut down because they weren't providing value? **6.** How long does it take for our company to deploy new applications? **7.** Which of our IT capabilities do vendors provide, and why?
Technology foundation	Flexible, scalable systems that speed releases of IT products • Modular architecture • Enterprise-wide data and artificial intelligence (AI) • Integrated cybersecurity	**8.** How much custom development work goes into building new IT solutions? **9.** What % of business decisions are we making with help from AI? **10.** For our developers, is cybersecurity a hindrance?

A new role for IT: Collaboration with the business on shaping strategy and streamlining operations
Many IT functions have trouble matching their priorities with those of the business. The problem often starts at the top: CIOs aren't included in strategic discussions, where they can shape other executives' thinking on how the business can best use technology. CEOs are ideally positioned to correct this. At the successful companies we know, CEOs have defined a strategic role for the technology function according to the following principles:

Alignment between IT and the business. We're seeing companies make organizational changes specifically to promote seamless collaboration between the tech function and other units and functions. CEOs are adding CIOs to their leadership teams and asking CIOs to report directly to them.[1] Some companies form unified business and technology teams that each support one technology product (for customers or employees) or one IT platform (a component, such as a customer-relationship-management [CRM] system, that supports multiple functions).[2] CEOs can test for these patterns by asking, "How are we making key technology decisions at all levels of the company?" They'll want to hear that business users and tech experts are working side by side.

Targeted technology investments. Top economic performers are more likely than other companies to develop new digital businesses in addition to digitizing their core business. Both activities require investments in technology. However, the typical company's wish list of technology investments exceeds its technology budget. CEOs must therefore commit their organizations to prioritizing high-value investments. To reinforce this discipline, the CEO should start by asking: "How do we track and maximize the value produced by our major technology investments?" An effective approach will involve not only measuring the payback from technology investments, but also reallocating capital frequently to promising opportunities—another practice associated with strong economic performance.[3]

Advocacy for end users. Modern IT functions follow design-thinking practices, by which they develop an in-depth understanding of users' needs as the basis for new products and features.[4] Such practices should interest the CEO: McKinsey research shows that they're correlated with strong financial performance.[5] CEOs can probe for them by asking, "How often do our tech teams seek input from users?" If the answer isn't "at every step," the tech function probably hasn't adopted design thinking.

An updated resource model for IT: The talent, methods, and tools to accelerate innovation
In pursuit of cost savings, traditional IT functions outsource much of their development and engineering work and focus on vendor and project management. Modern IT functions, by contrast, value innovation more highly than cost savings, and so they assemble top-notch workers and equip them with sophisticated methods and tools, along with specialized vendor support. To build a resource model that speeds innovation, CEOs should push for the inclusion of the following four elements:

Ample engineering talent. To keep mission-critical technologies ahead of the curve, companies recruit skilled engineers and entice them to stay with quality training and appealing incentives, including nonmanagerial career tracks where engineers can concentrate on technical work without sacrificing the chance to earn manager-level salaries. To gauge the IT function's talent mix, CEOs should ask, "Have we placed high-caliber engineers in enough IT roles that contribute the most value to the company?" A number less than 70 percent is a red flag.

---

[1] McKinsey research shows that companies with the best-performing IT organizations are more likely to say that their CIOs are involved in shaping overall business strategy. For more, see "Can IT rise to the digital challenge?," October 2018, McKinsey.com.
[2] Oliver Bossert and Driek Desmet, "The platform play: How to operate like a tech company," February 2019, McKinsey.com.
[3] McKinsey research shows that top economic performers divide digital capital evenly between creating new digital businesses and digitizing the core business and also reallocate capital expenditures more frequently than other companies. For more, see "A winning operating model for digital strategy," January 2019, McKinsey.com.
[4] "The power of design thinking," March 2016, McKinsey.com.
[5] Fabricio Dore, Garen Kouyoumjian, Hugo Sarrazin, and Benedict Sheppard, "The business value of design," *McKinsey Quarterly*, October 2018, McKinsey.com.

Agile working methods. Agile working methods produce good results quickly by having technology teams develop starter versions of new products, share them with users, and make round after round of improvements that users want.[6] CEOs can test IT's agility by asking, "How many projects has IT shut down because they weren't providing value?" If IT hasn't shut down some projects, then the function hasn't truly embraced agile. That's because agile practices call for ending projects as soon as it's clear that they aren't working out—and for celebrating the discretion of the people involved.[7]

Leading-edge tools. Modern IT functions create software and artificial-intelligence (AI) tools that automate routine software development, testing, and deployment tasks, thereby shortening time to market for tech products. They gain more efficiency by shifting systems into the cloud.[8] To assess their IT functions' tools, CEOs can ask, "How long does it take for our company to deploy new applications?" It should take only minutes if infrastructure is being automatically configured in the cloud.[9]

Targeted vendor partnerships. Leading IT functions build their expertise and capabilities in areas where they seek strategic advantages and form outsourcing partnerships to obtain capabilities that are nonstrategic (think "commodity" IT services) or too specialized to recruit for. CEOs can investigate their IT partnership models by asking, "Which of our IT capabilities do vendors provide, and why?" Vendors should provide few if any strategic capabilities—and IT leaders should have a plan for reducing vendors' share of the work to administer or enhance those capabilities.

A future-proof technology foundation: Flexible, scalable systems that speed releases of IT products
Many longstanding companies have a core of aging enterprise-wide applications (enterprise-resource-planning [ERP] systems and the like) running on their own on-premises infrastructure (hardware, such as servers, plus basic software resources). Adding features is cumbersome, and the legacy systems cost a lot to maintain. Successful companies run on flexible, scalable software foundations that let IT teams bring out products quickly and efficiently—a valuable practice for any business. With that practice in mind, CEOs should insist that their companies' IT foundations exhibit the following features:

Modular architecture. "IT architecture" describes a company's assembly of IT systems. Modern architectures consist mostly of compact, self-contained software components that are linked with easy-to-configure application programming interfaces (APIs) and stored in the cloud.[10] CEOs should make sure their companies have versatile, innovation-friendly architectures by asking, "How much custom development work goes into building new IT solutions?" A well-designed architecture lets IT teams build solutions by repurposing a lot of previously installed software and writing modest amounts of original code.

Enterprise-wide data and AI. Today's analytics applications give users a detailed understanding of business situations so they can make better decisions. For example, think of segmenting customers into several dozen precisely defined groups, rather than a few broad categories, and precision marketing to these groups. This approach works only if the company's IT foundation provides decision makers with AI tools that draw on data from across the business as well as from external sources.[11] CEOs can test the penetration of data and AI capabilities by asking, "What percentage of business decisions are we making with help from AI?"

Integrated cybersecurity. To streamline cybersecurity work and make it more effective, modern IT functions follow two practices. They apply lower or higher levels of protection to

---

[6] "How to create an agile organization," October 2017, McKinsey.com.

[7] For more, see Wouter Aghina, Karin Ahlback, Aaron De Smet, Christopher Handscomb, Gerald Lackey, Michael Lurie, and Monica Murarka, "The five trademarks of agile organizations," January 2018, McKinsey.com.

[8] For more, see Mark Gu, Krish Krishnakanthan, Anand Mohanrangan, and Brent Smolinski, "The progressive cloud: A new approach to migration," August 2018, McKinsey.com.

[9] For more, see Santiago Comella-Dorda, Peter Dean, Vito Di Leo, Nick McNamara, and Pankaj Sachdeva, "Transforming IT infrastructure organizations using agile," October 2018, McKinsey.com.

[10] For more, see Oliver Bossert and Jürgen Laartz, "Perpetual evolution—the management approach required for digital transformation," June 2017, McKinsey.com.

[11] Adrian Booth, Jeff Hart, and Stuart Sim, "Building a great data platform," August 2018, McKinsey.com.

information assets based on their importance and risk exposure, rather than protecting all assets equally. And they integrate security protections with the software-development process, rather than applying protections after development concludes.[12] CEOs should explore their companies' cybersecurity programs by asking, "For our developers, is cybersecurity a hindrance?" If so, it might be time to consider the practices described above.

Transforming the technology function: One CEO's approach

The CEOs we work with agree that their heightened efforts to guide the technology function have paid off, because so many of their companies' strategic priorities now depend on technology capabilities. CEOs cannot, and should not, take over the CIO's job, but they can use their unique influence to assist with the most valuable aspects of a technology transformation. Setting priorities is key: CEOs and their leadership teams should focus the CEO's efforts on tech-transformation activities that the CEO is best positioned to lead—particularly, the organizational changes required to promote better collaboration between IT and the business as well as to deliver innovative IT products. Here is a look at how the newly appointed CEO of one healthcare company changed his approach to technology, in close partnership with the CIO, to suit the organization's strategic needs.

Establishing a strategic role for the technology function

The CEO knew well that technology was profoundly changing how his company carried out crucial activities such as drug discovery and drug development—and that his company's strategic direction didn't properly reflect these trends (see sidebar, "A CEO's technology education"). Working closely with the CIO and the other members of the company's leadership team, he began by developing a five-year vision for his company that not only laid out a new strategy and business targets but also redefined the IT function's role in creating technology capabilities that would support value creation and operational efficiency.

Developing this vision was a different effort from the company's prior strategy-setting exercises. Rather than creating a business strategy first and then developing a technology strategy to match, the leadership team planned a unified strategy covering business and technology priorities.

The new strategic vision helped the CEO and the management team recognize that the company would need to transform its technology function. The CEO and CIO turned their attention to developing a plan for redirecting most of the IT function's efforts to delivering digital and digitally-enabled products and services, as well as technology solutions, that would help the business to greatly lower its operating costs. As part of the plan, the CEO and CIO chose to place extra emphasis on change management. They understood how important it would be to reorient the mindsets of IT staff toward developing IT products that would be intuitive to use and easy to adopt. Accordingly, they called for new investments in communication and skill building, with a focus on agile, user-centered ways of working. To ensure that the IT function would be well equipped to fulfill its new expectations, the CEO and CIO also called for renewing the company's core IT systems and adding technology talent.

Elevating the CIO

The CEO knew that the organization's business units and functions would achieve their strategic goals only if they aligned their activities closely with those of the technology function. Tech would need to become their partner in pursuing innovations and seeking operational efficiencies. The CEO resolved to strengthen the working relationships between the company's business units and functions and the tech function, starting in the company's uppermost ranks.

The company's previous CEO had established a leadership team consisting of the heads of the company's main business units, the head of human resources, and the head of supply-chain management. The new CEO added the CIO to this leadership team and invited him to all leadership meetings. At those meetings, the CIO began

---

[12] James Kaplan, Wolf Richter, and David Ware, "Cybersecurity: Linchpin of the digital enterprise," July 2019, McKinsey.com.

learning firsthand about the business's aspirations and framing how technology could support progress toward those aspirations.

Joined by the CIO, the leadership team also became a forum for engaging the business in technology decisions and for explaining why certain technology changes were necessary. For example, after the IT department determined that productivity and collaboration would increase if the company consolidated its multiple communication platforms, the IT leader explained the opportunity to business leaders firsthand and sought their support for pursuing it. Together, the leaders developed a plan for promoting the new communications platform and encouraging employees to use it. As a result, employees adopted the new communications platform more readily than they had adopted other new technology tools.

Another important change the CEO made was sharing the company's technology plan with the board. He knew it was unusual for a board of directors to sign on to a technology plan, but he also knew that the company's technology plan would have as much strategic importance as the other plans that the board was accustomed to considering. He also felt that making a commitment to the board would motivate him and the leadership team to remain focused on the technology transformation.

Rebalancing technology investments and tracking their business value

Like many a CEO, the chief executive of the healthcare company had risen as a leader partly because of his ability to deliver value, closely monitoring the funds that were being disbursed and the cost savings and revenues associated with those investments. He knew that the company's stepped-up technology program would pay off only if leaders applied the same discipline to tracking its value. The CEO asked his CIO for help devising a system to link technology investments to business value—both the value from selling new tech-enabled products and services and the operational efficiencies from embedding technologies into business processes.

Tracking investments in IT and the resulting returns proved to be more difficult than the CEO expected. The costs of running core systems and developing new applications weren't consistently divided among business functions. That made it hard to determine which functions were the heaviest consumers of IT services and whether investments were properly divided between technologies to sell and technologies to streamline operations. And when the IT function created new applications or features, business functions didn't always record the revenues or cost savings that resulted from their use.

Nevertheless, the CEO and CIO were determined to try measuring the payoff from at least some tech investments. In one instance, they focused on the technologies that would support a strategic goal of enabling patients to access and order the company's products and services online. A few quarters after setting that goal, executives discovered that IT spending allocated to it fell short of what would be needed to implement all the

A CEO's technology education

Even before the CEO initiated his company's tech-focused strategic-planning effort, he realized that his personal knowledge of IT wasn't up to the task of leading a tech-powered organization. And so, for six months, the CEO devoted several hours per week to meeting with IT leaders and staff so he could hear directly from them about the company's technology capabilities, achievements, and challenges. For each get-together, he asked the CIO and other technology leaders to invite the company's most knowledgeable experts on the topic he wanted to learn about—regardless of their job titles or seniority within the business. These master classes soon brought him up to speed on subjects such as cybersecurity, data management, IT infrastructure, and machine learning.

business-process changes they had outlined—and was much less than the planned IT spending in nonstrategic areas.

To accelerate improvements in key patient-access processes such as tracking inventory and dispatching supplies, the team reallocated IT investments toward changes to the patient-access platform and to underlying systems such as ERP. They also set up key performance indicators (KPIs) and objectives and key results (OKRs) to measure how much business value resulted from investments in patient-access technologies.

Once the team could gauge the value of tech features to improve patient access, they began to release additional investments only for features that showed a positive return, rather than funding them with an up-front, no-questions-asked budget allocation. The new investment approach helped the company achieve a 28 percent increase in sales in less than a year and made the software-development process more agile and patient-centric, leading to improved customer-satisfaction scores and a 30-percent reduction in time to market.

Building a world-class tech workforce
As the CEO, the CIO, and the leadership team realigned the tech function with the company's other functions and raised its strategic importance, the CEO realized that IT would need a new resource model as well—a resource model more like that of other functions, which recruited and trained employees to support the business's strategically significant capabilities. Traditionally, the IT function had relied on external vendors to perform software-development projects. IT staff largely oversaw those vendors and managed vendor-created technologies after they'd been implemented. And the caliber of its in-house tech talent wasn't as high as it was for other functions.

The CEO made it one of his priorities to strengthen the tech function's resource model by assembling an in-house cohort of skilled technology workers. He called for hiring dozens of proven engineers and experts in technology disciplines, such as design and user-interface (UI) and user-experience (UX) development, that the company formerly obtained from vendors. He also approved investments in training and on-the-job apprenticeships. Finally, the CEO saw to the creation of incentives that reflected the value of tech workers, along with career paths that would supply them with interesting business problems to work on.

Today, the company's IT workforce has a better appreciation of the company's strategic needs and a stronger association with colleagues in other business units and functions than vendors ever did. Continuity in staffing has been a major factor: tech specialists spend longer periods working with the same business peers than vendor-provided staff, who were frequently reassigned to other accounts. Overall, improvements to the company's tech workforce have increased collaboration between the business and IT, supercharged innovation, and reduced the costs of hiring, onboarding, and training.

———

The potential for technology to deliver winning business capabilities and change a company's fortunes is simply too great for CEOs not to lead technology's integration with the wider business. CEOs who actively influence and shape their companies' technology functions can position their companies for greater success in an economy where digital savvy is at a premium.

Reimagine role of technology

The CIO challenge: Modern business needs a new kind of tech leader

As technology becomes increasingly important, an organization's success depends on whether the CIO can move from being a functional to a strategic business leader.

by Anusha Dhasarathy, Isha Gill, and Naufal Khan

"**There's no worse time than now** to be an average CIO." These words, uttered by an executive at a recent conference, neatly capture the intense pressure on chief information officers (CIOs). For years, executives have stressed the need for CIOs to move beyond simply managing IT to leveraging technology to create value for the business. This priority is now a requirement. New technologies have been at the center of trends—from mobile-first consumer shopping preferences to the promise of artificial intelligence in critical decision making—that have reshaped the competitive landscape and disrupted business models. For this reason, companies need to be tech forward: technology needs to drive the business.

Despite this pressing need, of the organizations that have pursued digitization, 79 percent of them are still in the early stages of their technology transformation, according to McKinsey's 2018 IT strategy survey.[1] Legitimate factors are delaying progress, from the scale of the change to the mind-boggling complexity of legacy systems. We believe, however, that one of the biggest issues is that many CIOs have not accepted the degree to which their role needs to expand beyond cost and performance responsibilities in order to transform IT into a core driver of business value.

Three vectors of a comprehensive transformation

Before understanding the responsibilities of the new CIO, it's important to understand the nature of tech transformations themselves. In most cases we've observed, tech transformations are implemented as a set of disjointed initiatives across IT. That leads promising developments to stall out or underdeliver. We have found that a tech transformation must be comprehensive to deliver full business value. Creating powerful customer experiences, for example, requires a data architecture to track and make sense of customer behavior. Architecting modular platforms needs revamped approaches to hiring in order to get top-flight engineers.

This reality requires a CIO to first come to terms with the scope of the transformation itself. In our experience, it's been helpful to think about it along three vectors:

1. Reimagine the role of technology in the organization. This vector includes establishing the role of technology as a business and innovation partner to design a tech-forward business strategy (for example, tech-enabled products and business models), integrate tech management across organizational silos, and deliver excellent user experiences.

2. Reinvent technology delivery. IT needs to change how it functions by embracing agile; improving IT services with next-generation capabilities such as end-to-end automation, platform as a service, and cloud; building small teams around top engineers; and developing flexible tech partnerships.

3. Future-proof the foundation. To keep pace with rapid technological advancements, organizations need to implement a flexible architecture supported by modular platforms, enable data ubiquity, and protect systems through advanced cybersecurity.

Five traits of a transformative CIO

For IT to become a driver of value, the transformative CIO also needs a new set of skills and capabilities that embody a more expansive role. In working on tech transformations with hundreds of CIOs, we have identified five CIO traits that we believe are markers for success.

1. Business leader

To help technology generate business value, the transformative CIO has to understand business strategy. Findings from our 2018 IT strategy survey reveal that companies with top IT organizations are much more likely than others to have the CIO very involved with shaping

---

[1] "Can IT rise to the digital challenge?," October 2018, McKinsey.com.

Questions for the CIO

- Can I clearly articulate the business's goals?

- Are the most important technology initiatives delivering quantifiable business value to the company?

- What percentage of technology resources is focused on work that drives business goals versus maintenance?

the business strategy and agenda, and strong performance on core IT tasks enables faster progress against a company's digital goals.[2] CIOs who can make this leap tend to take the following actions.

Learn the business inside and out. The scope of an IT transformation means that CIOs must be prepared to interact with the business in different ways. We have found, for example, that the best CIOs go far beyond meeting with the C-suite or attending strategy meetings. They invest time with functional and business-unit leaders and managers to gain an in-depth understanding of business realities on the ground and go out of their way to develop a nuanced and detailed understanding of customer issues. CIOs do this by continually reviewing customer-satisfaction reports, regularly monitoring customer-care calls, and participating in user forums to hear direct feedback.

As one large financial institution set out to build its digital products, the business and technology teams jointly led user listening and feedback panels early and often throughout the development process. Both technology and business leaders made it a priority to attend these panel discussions so that they could effectively guide their teams on developing products that would best address the needs of end customers. The CIO of a B2B technology-services company, meanwhile, meets customers on a regular basis to get firsthand feedback on both products and the

customer's experience of doing business with the company. He uses these perspectives to inform his technology decisions.

Take responsibility for initiatives that generate revenue. CIOs can further develop business acumen by taking responsibility for initiatives that generate business impact, such as building an e-commerce business or by working with a business-unit leader to launch a digital product and then measure success by business-impact key performance indicators (KPIs), not technology KPIs. Such efforts allow CIOs to build a deep understanding of the business implications of technology, such as customer abandonment because of slow download times on a site or other poor user experiences.

As part of a digital transformation, for instance, the CIO at a large financial institution committed to developing digital products to help the business scale its presence in a new market. While the CIO already understood how to build systems to support financial products, he and his team had limited experience in creating new digital products to sell directly to consumers. So the team created a program built on rapid test-and-learn cycles to identify what mattered to customers and meet those needs. Subordinating tech decisions to customer needs was crucial in allowing the CIO and his team to develop a digital offering that succeeded where it mattered: with consumers.

---

[2] "Can IT rise to the digital challenge?," October 2018, McKinsey.com.

Get on boards. Developing a deeper well of business knowledge often requires CIOs to extend their networks beyond the organization. One of the best ways to do that is by joining the board of another company. A third of the boards of companies within the Fortune 500 today include a former CIO or CTO, and that number continues to increase.[3]

2. Change agent

A full technology transformation is not only about moving to the cloud or embracing new IT solutions. It also involves infusing technology into every strategy discussion and process throughout the organization. Driving a transformation around the three vectors we laid out earlier (reimagining the role of technology, reinventing technology delivery, and future-proofing the foundation) starts with a CIO mindset that both acknowledges the need for transformative change and commits to a multiyear journey.

Partner with business leaders. Generating support for a transformation among business leaders across the organization requires creating true partnering relationships with them based on common goals, mutual responsibility, and accountability. According to a McKinsey survey on business technology, in fact, the companies in which IT plays a partner role in digital initiatives are further along in both implementation and achieving business impact.[4]

To kick-start the transformation journey, the CIO of a transportation-and-logistics company made it her first priority to meet with every single business leader to understand their goals and issues and to set expectations on how they could best work together, by clarifying, for example, what the business side could expect to get from IT in a consultant role versus IT as a service provider or partner. This effort to understand what mattered to each leader established trust, and from each of these discussions it became clear that the business wanted a true partnership with technology and understood what it meant. The CIO further built on the relationship with the business by prioritizing initiatives in the tech transformation that addressed business needs and by working closely with business leaders to drive progress. This active collaboration ensured that the products and services IT developed were adopted.

---

[3] "The digital CIO has arrived," MIT Sloan CIO Symposium, 2016, searchcio.techtarget.com.
[4] "Partnering to shape the future—IT's new imperative," May 2016, McKinsey.com.

Questions for the CIO

- Do leaders in the C-suite have a clear understanding of why a tech transformation is important?

- Do you have partner-level relationships with people in the C-suite in developing the vision and plan for both business and IT?

- Is your tech transformation actively incorporating each of the three vectors of change?

- Do you have a "war room" to manage the transformation that can solve problems as well as track progress?

The CEO's role in making the CIO successful

The stage is set for CIOs both to lead a successful technology transformation and to influence business strategy. They can't do it alone, however. The CEO must create an environment where the CIO can thrive. Here are a few things CEOs can do:

- Establish a strategic role for the technology function

- Elevate the CIO to report directly to the CEO

- Rebalance technology investments and track their business value

- Prioritize the development of a world-class tech workforce

For more on this topic, see "The CEO's new technology agenda" in this compendium.

Articulate the 'why.' Gaining support for a transformation requires stakeholders to understand that true change will come only from tackling all three transformation vectors in a strategic, interlinked manner. That means not just explaining how this three-pronged approach is better for IT but also clarifying how it drives business goals and how it can be implemented. When considering a shift to cloud, for example, executives tend to understand it first as a cost-saving opportunity. But in helping executives understand the full range of cloud benefits— improved speed to market, better developer productivity, and improved resilience and disaster recovery—CIOs can help them see how the cloud can unlock new revenue models and services tied to business priorities.

Have an integrated plan that highlights risks and dependencies beyond IT. Large IT initiatives have always required detailed planning, but business-oriented CIOs ensure that transformation plans account for dependencies outside of IT, such as marketing campaigns or legal implications. They approach planning as a dynamic process

rather than something static, which allows transformation teams to better remove roadblocks and to allocate people and spend when and where they are needed. To actively manage this process, such CIOs also put in place a "war room," a dedicated team that ensures transformation initiatives are delivering value by actively tracking progress and helping to break through root-cause issues.

This was the approach taken in a large global retailer's digital and technology transformation. The CIO set up a transformation war-room team that worked jointly from the beginning with leaders outside the IT function, including marketing, operations, sales, and e-commerce. Together, they created detailed work plans. This detailed early planning revealed which systems needed to be upgraded and when. The war-room team actively tracked progress and quickly escalated issues for speedy resolution. The results were clear: a fivefold jump in digital sales, and project delivery four times faster than projects of similar scope had previously taken.

3. Talent scout

Nearly half of respondents to McKinsey's 2018 IT strategy survey cite skill gaps on traditional teams as the top obstacle to a successful digital transformation.[5] So CIOs need to focus not just on recruiting top people but also on retaining them. Two solutions have proven effective.

Reimagine how to attract tech stars. Companies can reap tremendous benefits from outsourcing. In the oil and gas industry, for example, the outsourcing of application development grew 50 percent between 2014 and 2018.[6] But that needs to change, especially around the most crucial capabilities. CIOs who want to reinvent tech's role need tech stars, particularly the best engineers. By hiring the best tech people, we've seen companies reduce their technology costs by as much as 30 percent while maintaining or improving their productivity.[7] CIOs need to move quickly. In just 18 months, one CIO at a transportation-and-logistics company radically reshaped its talent profile. All the direct reports and approximately 50 percent of tech employees were new, and 80 percent had transitioned to different roles.

The head of technology and analytics at a large retail organization set up a talent war room to hire data scientists and engineers. As part of this effort, the war-room team revamped recruitment and onboarding processes by using different talent sources, such as HackerRank and General Assembly, and by updating candidate screenings and interviews with appropriate assessments of technical and other skills, such as coding and collaboration. In addition, they led weekly check-ins to track the talent funnel and adjust the process as needed.

Build up internal talent. Getting good people doesn't matter if you can't keep them. Top CIOs, therefore, develop diverse career paths so that top talent can advance in their own areas of strength— for example, by letting a top-notch software engineer advance while continuing to code design software rather than forcing her to manage others in order to succeed.

Retraining the existing tech workforce also needs to be an important element of this platform. The CIO of a large consumer company made

---

[5] "Can IT rise to the digital challenge?," October 2018, McKinsey.com.
[6] Dhingra, Sverre Fjeldstad, Natalya Katsap, and Richard Ward, "A new mandate for the oil and gas chief information officer," November 2019, McKinsey.com.
[7] Klemens Hjartar, Peter Jacobs, Eric Lamarre, and Lars Vinter, "It's time to reset the IT talent model," *Sloan Management Review*, March 5, 2020, sloanreview.mit.edu.

Questions for the CIO

- Are the top people in IT really stars in their field?

- Do you rely exclusively on HR to find your talent?

- Do you have a clear view of the talent you need in the next three years—and a plan to develop it?

- What percentage of the best people you hire are still with you two years later?

digital and analytics upskilling one of the company's key strategic priorities, launching an enterprise-wide program, in tandem with HR's learning team. The program invested in an online learning portal to create personalized online learning experiences based on an employee's goals and learning needs. These were supplemented by other programs, including in-person training, top management immersion sessions, and the cultivation of an in-house expert network that people could tap on specific topics.

4. Culture revolutionary

An effective talent strategy requires a culture that supports talent.

Build a true engineering community. Pay matters, of course, but top people want to go where they're valued. One way to create that kind of environment is to provide engineers with more autonomy by reducing the number of managers and often-bureaucratic processes, such as time-consuming reports and multiple rounds of approval.

Creating ways for cohorts of similar skill sets to get together can be a powerful way to share best practices and foster a sense of community. The CIO of a software company established various community-building and knowledge-sharing efforts—hackathons, "dev days," tech spotlights, brown-bag lunches—where product managers, developers, data engineers, and architects could meet on a weekly basis to share details about their projects and bring up ideas or issues for discussion. The CIO attended and actively participated.

Model and support true collaboration. Promoting collaboration across technology teams and between the business and technology is one of the most crucial prerequisites for a successful transformation. Top-quartile IT organizations are more likely to have an integrated or fully digital operating model, according to McKinsey's 2018 IT strategy survey.[8]

In practice, CIOs can enable collaboration if they're willing to relinquish some control. One CIO at a financial-services firm realized that for his people to increase their impact, they had to be more closely tied to business teams. So he embedded them into cross-functional teams aligned around specific products, relying on informal networks of guilds and chapters to provide guidance and light oversight. The most effective CIOs ensure this

---

[8] "Can IT rise to the digital challenge?," October 2018, McKinsey.com.

Questions for the CIO

- Do you meet or speak with IT employees who are on the front lines at least once a week?

- Do you have a way to accurately measure and track people's attitudes across the IT department?

- Are your top engineers happy with their work?

- How often do you publicly celebrate success and support noble failures?

Questions for the CIO

- Do the questions about technology that leaders in the C-suite ask reflect a true understanding of the impact of tech decisions?

- When you explain the ramifications of tech decisions, do leaders really understand you?

- How often do company leaders reach out to you for substantive guidance about how tech can improve their business?

level of collaboration is the norm within IT itself as well. This is particularly important around cybersecurity. IT can radically reduce cycle times and maintain effective security by incorporating security early into development and working closely with the cybersecurity team on an ongoing basis.

5. Tech translator

In the past, IT transformations have often proven expensive, time consuming, and short on value, and this has made some companies leery of undertaking them again. To address this issue and build trust, the best CIOs play an active role in educating leaders about technologies and their applications for the business.

Make the business implications of tech decisions clear. Many tech decisions don't get sufficient business scrutiny beyond cost and high-level strategy discussions. Transformative CIOs don't settle for that kind of interaction, articulating instead how a proposed solution solves the underlying business problem, what alternative approaches exist, and the pros and cons of each. The CEO of a B2B technology-services company

found this level of insight so important that he asked the CIO to present periodically to the board on technology-led business models.

This role was particularly important when a retail giant was looking to acquire an analytics company. The CIO and his leadership team were involved from the very beginning in determining the data and analytics capabilities needed to fulfill the company's business strategy. They performed deep-dive technical assessments, system and data-platform compatibility reviews, and tests of vendor capabilities. The CIO ran a pilot with a business unit and operations team for three months to determine whether the final vendor could deliver on its capabilities. At the end of the process, the business was able to make an informed decision.

———

These skills are the tools that enable a CIO's ability to transform IT. And in an increasingly tech-driven business landscape, they position CIOs as legitimate contenders to lead businesses as well.

Commercial lines insurtech: A pathway to digital

Rather than fear the disruptive potential of insurtechs, commercial insurance executives should view them as a catalyst for digitization.

by Ari Chester, Nick Hoffman, Sylvain Johansson, and Peter Braad Olesen

Companies across industries are seeking to embrace digital technologies—to support new business models, improve efficiency, and gain a competitive advantage. Commercial insurance executives clearly recognize the benefits of digital but face some obstacles in making headway. Large incumbents lag behind because the complicated nature of their work often requires human judgment and interaction, transactions are typically low volume and bespoke in nature, and legacy IT systems and processes make the transition resource intensive and complex. What's more, commercial insurance has historically been slow to change, and a lack of companies with clearly demonstrated impact from digital has left many executives focused on their own plan of action.

Enter insurtechs. Most insurtechs are not currently seeking to completely transform commercial lines but instead are more focused on enabling or extending the insurance value chain. In personal insurance, insurtechs played the role of digital attackers and captured market share at specific points in the value chain. Lacking the scale and expertise needed to excel in commercial, insurtechs are viewed by executives not as competitors to be feared but as potential partners that could accelerate their digitization efforts.

The rapid proliferation of commercial insurtechs has created a challenge for large incumbents: how to identify worthy candidates for collaboration. Due to this uncertainty, many commercial insurers have been sitting on the sidelines.

The urgency to embrace digital will only grow in the coming years, however, so commercial insurers would be wise to get in the game—and the sooner, the better. As a first step, executives should become more familiar with the areas in the value chain where insurtechs are concentrating their efforts. Armed with this context, insurers can prioritize their engagement toward insurtechs in ways that can add value to their own strategy. This strategic collaboration can help usher in new, tech-enabled approaches that should inspire commercial incumbents and accelerate the digitization of their enterprise.

Insurtechs at the gate

Over the past few years, global investment in insurtechs has grown by leaps and bounds—from $250 million in 2011 to $2.3 billion in 2017. Although the United States was the pioneering market for these companies, only 38 percent of all insurtechs are currently headquartered there. According to the latest figures, there are more than 1,500 insurtechs globally, and 37 percent are based in Europe, the Middle East, and Africa (EMEA)—in particular, Germany and the United Kingdom. An analysis from McKinsey's Panorama Insurtech database shows that around 39 percent of insurtechs are focused on the commercial segment, mostly in small and medium-sized enterprises (SMEs), as shown in Exhibit 1. (See sidebar, "About the research.")

How insurtechs will affect incumbents

As the number of commercial insurtechs grows, their influence will take different forms. Some insurtechs will partner with incumbents to provide innovative new products and services, and others will be acquired and integrated into incumbents. The majority of commercial insurtechs (63 percent) are focused on enabling the insurance value chain and partnering with incumbents. Only a small number of insurtechs (9 percent) are attempting to fully disrupt the insurance market (Exhibit 2). These companies don't currently pose a serious threat to incumbents, but in the coming years they might be

Exhibit 1

Insurtechs are entering the commercial-lines space, especially among small and medium-size enterprises (SMEs).

Insurtech focus by customer segment, %
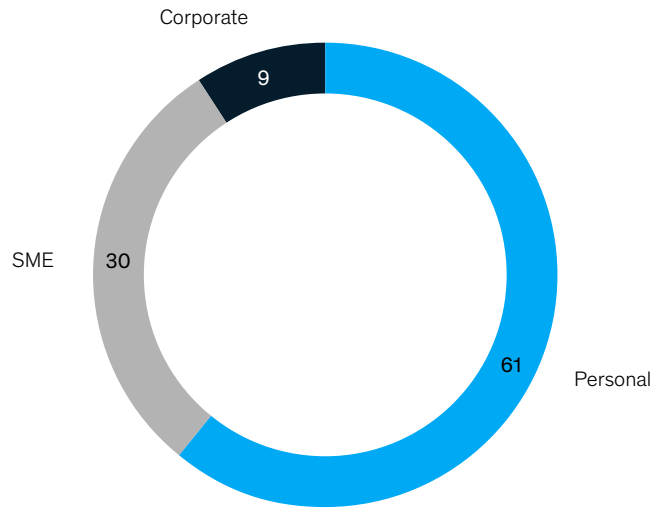
Source: McKinsey Panorama Insurtech database

able to make inroads in certain segments or niches and take market share.

Despite significant digital advances, commercial lines still rely heavily on human judgment—particularly in underwriting. This manual model not only increases operating costs but also limits the ability of incumbents to provide superior customer service (such as risk prevention and loss control) for a select few customers, specifically those with large accounts or where change in risk behavior would have considerable impact. Insurtechs, however, can help scale and expand services, using digital to enable greater interactivity and enhance human judgment with technology. In doing so, companies can extend their services beyond the largest accounts while significantly improving performance and efficiency.

Commercial insurtechs are currently focused primarily on two areas: digital interaction and core insurance capabilities (Exhibit 3).

Digital interaction models. Inspired by the success of digital brokers and advisers of insurtechs in personal lines, a number of commercial insurtechs, such as Finanzchef24, Insureon, and Zensurance, are providing new and seamless digital customer experiences. Others are inspired by the digital peer-to-peer (P2P) models seen in the retail segment, such as Gather. The new digital interaction models also lower the cost to serve customers and increase transparency in pricing and coverages. Furthermore, some of the digital brokers interact directly with reinsurers and other capital providers while outsourcing insurance processes such as claims handling. These practices might ultimately reduce the role of the traditional insurers. Notably, the digital interaction models used by commercial insurtechs will most likely have the greatest value in the SME segment.

As the customer decision journey for the lower end of commercial lines starts to resemble personal lines, North American traditional companies and

Exhibit 2

Insurtechs are both friends and foes, raising strategic questions on competition and collaboration.

Insurtech role, %

Disrupt full value chain
Capturing value
from incumbents

9

Disintermediate customers
Enabling new channels
for incumbents
but potential pressure
on margins

28

63

Enable value chain
Making a positive
impact on incumbents'
top line, indemnity, and
administration costs
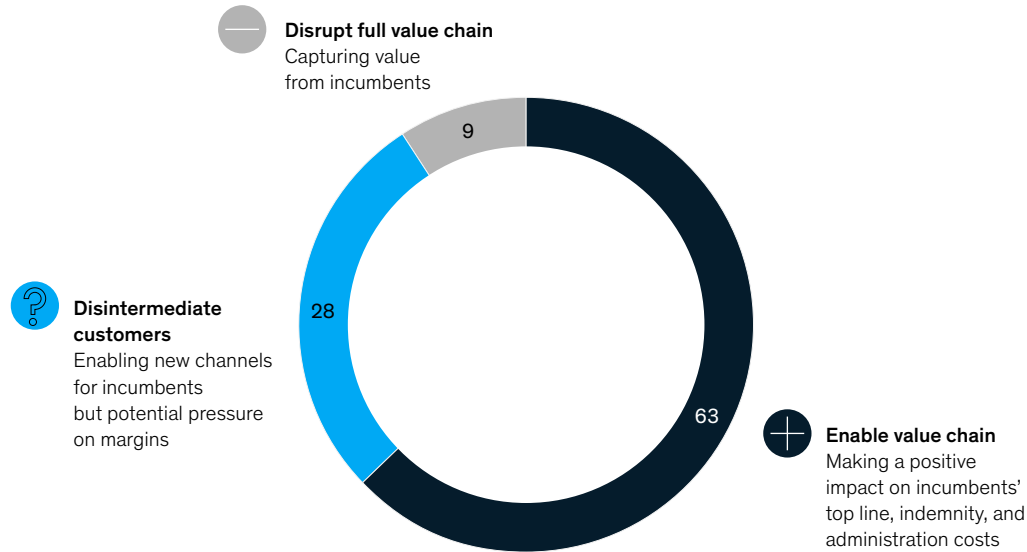
Source: McKinsey Panorama Insurtech database

insurtechs are actively pursuing commercial SMEs using digital solutions. Key trends include more automated or streamlined underwriting, a shift from brick-and-mortar to digital service and delivery, the replacement of intermediated with "direct" customer engagement, and the development of aggregator solutions.

Digital core insurance capabilities. By adopting new technologies, insurtechs in commercial lines are at the forefront of reducing human involvement and enhancing human judgment in key insurance processes, such as certain areas of underwriting and claims. The increased dependence on technology lowers costs and allows insurers to adjust their approach from "art" to "science" in key disciplines, including underwriting, risk selection, and claims leakage prevention.

Furthermore, insurtechs are using approaches with the potential to provide new services to their customers, better enabling them to monitor, prevent, and mitigate their own risk at an affordable cost. For example, the following use cases

are relevant to both SMEs and more complex commercial lines segments:

— *Virtual reality and drone technology* to improve underwriting and claims inspection data and decisions. Insurtechs such as Aerobotics and Airware have built enhanced inspection capabilities in property and agriculture.

— *Blockchain technology* to assess the provenance of items and thereby avoid claims leakage. Examples include Everledger for diamonds and BlockVerify for electronics and pharmaceuticals, among others.

— *New data sources for underwriting and claims prevention.* Meteo Protect, for example, uses weather data, Augury Insurance captures status data from Internet of Things (IoT) machinery, and Windward for marine data and analytics.

— *Advanced analytics.* Adapt Ready, for instance, deploys machine learning to reduce business interruption by improving risk selection.

It is still too early to tell exactly where digital models will have the greatest impact on commercial lines. However, recent McKinsey analysis found that administrative costs for greenfield insurers are, on average, half those of incumbents—sometimes even less.[1] Their cost leadership is partially due to a monoline focus and the absence of legacy IT systems, processes, products, and mindset, as well as digital-by-design products. While these results are primarily related to personal lines, the impact on commercial lines, starting within the SME segment, will over time become as significant.

Developing a plan of action

When the fintech movement started in financial services, the banks that adapted quickly to meet the challenge formulated a strategy in three phases—understand, engage, and act. Commercial insurers would do well to follow a similar approach to determine the best way to partner with insurtechs (Exhibit 4).

— *Understand.* While some of the larger insurers and reinsurers have made progress across all three stages of engagement, many insurers are currently in this phase. Commercial executives must become more familiar with the evolution of the insurtech ecosystem as well as gain an understanding of the research in insurtech databases or publications and participating in insurtech accelerator programs, which are run by a third party. Other insurers have launched hackathons with insurtechs. Zurich, for example, held a two-day event called "Insurhack" that focused on software innovation. It offered €75,000 in cash prizes to participants in challenges focused on areas such as open data and everyday insurance.[2]

— *Engage.* This phase involves interacting with players in the insurtech ecosystem to seek out partnerships or inspiration.

---

[1] Tonia Freysoldt, Sylvain Johansson, Christine Korwin- Szymanowska, Björn Münstermann, and Ulrike Vogelgesang, "Evolving insurance cost structures," April 2018, McKinsey.com.
[2] Held in Germany, Insurhack is a two-day "hackathon" challenge for coders.

Exhibit 3

Commercial lines insurtechs focus on digital distribution and core insurance capabilities.

Share of insurtechs in database

● <10%   ● 10–20%   ● >20%

Number of insurtechs as percent of total in the database

	Marketing	Distribution and sales	Product development	UW[1] and pricing	Claims
All insurtech	8	43	16	20	13
SME[2] and corporate insurtechs	9	36	18	22	15

Digital interaction models

Digital core insurance capabilities
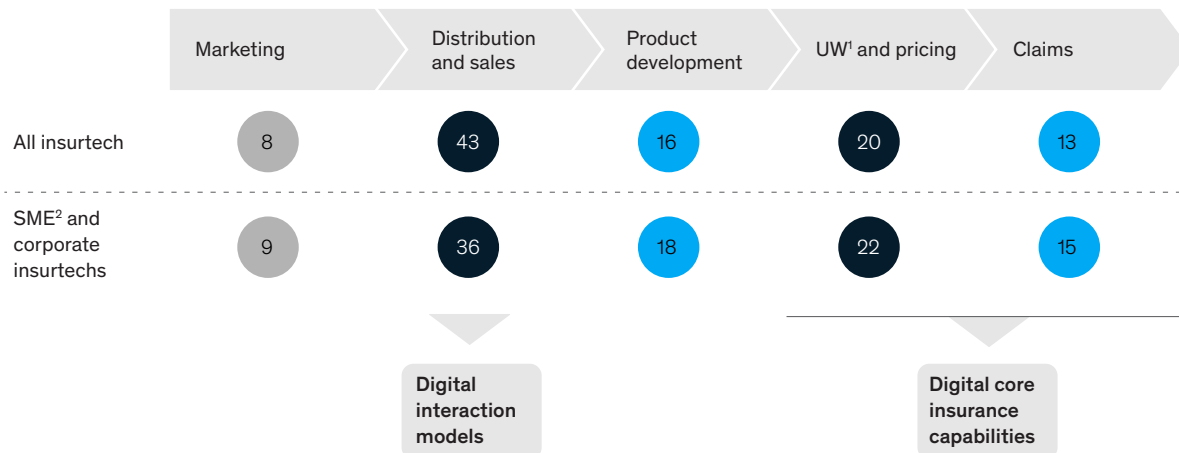
[1] Underwriting.
[2] Small and medium-size enterprises.

Source: McKinsey Panorama Insurtech database

Exhibit 4

Insurance incumbents have started following three phases of digitization.

	A. Understand	B. Engage	C. Act
Goal	Understand what is going on and gain awareness of the value at stake	Engage with insurtech community to seek inspiration and investigate partnerships	Acquire or invest into insurtech and adopt an "insurtech style" of working

← Internal focus ——————————— External focus →

| **Actions** | • Participate in insurtech accelerator programs

• Launch insurtech hackathons | • Partner with insurtech to develop proof of concept

• Launch an insurtech incubator | • Wait and see

• Direct investments

• Partnerships

• Establish a venture-capital fund

• Adopt an insurtech way of working

• Become an ecosystem orchestrator |

Commercial insurers can conduct more formal scouting, partner with insurtechs to develop proof-of-concept solutions, or launch incubator programs. Incumbents such as AIG have launched incubator programs in an effort to provide a springboard to promising insurtechs. Likewise, Allianz established a subsidiary, Allianz X, which seeks to develop and scale new business models in the commercial space.[3] Its 100-day "entrepreneur in residence" program enables small business leaders to collaborate with the company's experts to establish a start-up. Participants have access to mentors as well as to a range of resources.

— *Act.* Commercial executives can use their firsthand knowledge of the opportunities to partner with insurtechs to determine whether to invest, collaborate, adopt an insurtech approach, or wait and see. A few large multinational

primary insurers and reinsurers are also actively investing and seeding opportunities in the insurtech space using a multitude of interaction models, ranging from investments to partnerships and reinsurance cover.

Some insurers have launched venture capital funds in the insurtech space. AXA Venture Partners, for instance, has $450 million in funding and invests in enterprise software and technologies, AI, and cyber-security.[4] Allianz Corporate Ventures has made seven investments since 2015, and part of its strategy is to view insurtechs as partners that can accelerate its digitization.[5] MunichRe has made investments in excess of $68 millon in insurtech, especially focused on getting access to IoT ecosystems. Its leaders view the investments as long-terms partnerships where they bring not just money to the insurtech but also domain expertise, clients, and brand.[6] Similarly, XL Catlin Ventures

---

[3] Elena Mesropyan, "Thirteen InsurTech accelerators & incubators supercharging the evolution of the insurance industry," MEDICI, June 9, 2017, gomedici.com.
[4] "AXA Strategic Ventures rebrands as AXA Venture Partners," AXA Venture Partners, April 10, 2018, axavp.com.
[5] Hugh Terry, "Allianz: In action summary," The Digital Insurer, accessed May 11, 2018, the-digital-insurer.com.
[6] "Driving digital transformation," Munich Re Investor Day, November 21, 2017, munichre.com.

has both invested in US sharing economy insurtech Slice and cocreated a new product—an on-demand cyber insurance solution for SMEs.

Some commercial insurers are active in all three phases. Since the insurtech space is changing rapidly, approaching the "understand" and "engage" phases as ongoing efforts rather than one-off activities can ensure that executives stay up to date on the latest developments.

Identifying insurtech partners

Finding the right insurtechs to engage with requires a structured approach. Executives should consider several parameters when evaluating an insurtech for a more formal arrangement (Exhibit 5):

Degree of innovation. The analysis should include activities from improving the current value chain (for example, through the introduction of advanced analytics or artificial triaging of quotes), extending the current value chain (by providing adjacent services for risk prevention and mitigation), and exploring completely new risk pools and business models (for example, through ecosystems).[7]

Placement along the insurance value chain. Insurtechs have emerged at each step of the value chain, from marketing and sales to administration and claims.

Strategic relevance and value for the company. This measure seeks to determine the importance of the innovation across the insurance value chain.

---

[7] Tanguy Catlin, Johannes-Tobias Lorenz, Jahnavi Nandan, Shirish Sharma, and Andreas Waschto, "Insurance beyond digital: The rise of ecosystems and platforms," January 2018, McKinsey.com.

Exhibit 5

Prioritizing insurtech engagement based on value chain, degree of innovation, and strategic fit.

● Low relevance   ● Medium relevance   ● High relevance

Value chain

	Marketing	Distribution and sales	Underwriting	Policy admin	Claims	Target
Improve current value chain	Low	Medium	High	Medium	Medium	−x% admin cost
Extend current value chain	Medium	Medium	Medium	Low	High	+y% revenue
Explore new risk pools and business models	Medium	Medium	Medium	Medium	Medium	X% of future revenue
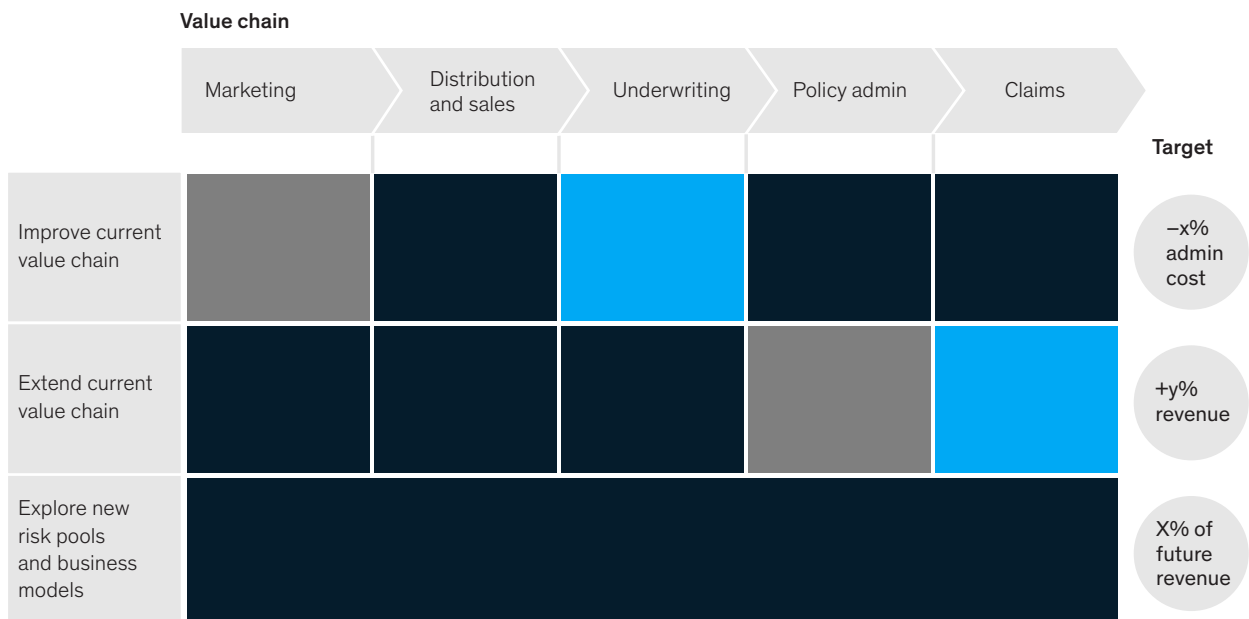
Relevance and value can vary at each part of the chain. For example, insurers seeking to extend the value chain should focus on claims, which has the highest relevance and impact for this value driver.

———————

Insurtechs are entering the commercial lines space: many of these start-ups will fail, and a few will succeed. The most important impact of commercial lines insurtechs is that they provide a source of inspiration for the incumbent commercial lines insurers and reinsurers and a way to leapfrog into digital.

Commercial insurers that are able to find the right insurtechs to engage with could improve margins, expand their client base, and extend their services. Forging such partnerships may allow them to break free from constant cost pressures and eroding margins once new technologies mature. To reap these benefits, commercial players must manage their partnerships effectively and expand IT capabilities to implement the solutions provided by insurtechs. All of these moves will require investment into understanding and engaging with insurtechs, defining the right business models, and integrating insurtech solutions into IT architecture and core systems. The payoff could include not only increased digitization and new ways of generating value but also a stronger competitive position in the coming years.

The platform play: How to operate like a tech company

For tech to be a real driver of innovation and growth, IT needs to reorganize itself around flexible and independent platforms.

by Oliver Bossert and Driek Desmet

"**The question is not** how fast tech companies will become car companies, but how fast we will become a tech company." This is how the board member of a global car company recently articulated the central issue facing most incumbents today: how to operate and innovate like a tech company.

The tech giants of today have been some of the most innovative companies in the past generation. A handful of industry leaders, such as Ping An and BMW, are fast joining their ranks by reinventing their core business around data and digital. What distinguishes these tech companies is that their technology allows them to move faster, more flexibly, and at greater scale than their competitors. IT is not a cumbersome estate "that gets in the way," but an enabler and driver of continuous innovation and adaptation.

The reason this is a competitive advantage for tech companies is because their IT is organized around a set of modular "platforms," run by accountable platform (or product) teams. Each platform consists of a logical cluster of activities and associated technology that delivers on a specific business goal and can therefore be run as a business, or "as a service," as technologists say. These platforms are each managed individually, can be swapped in and out, and, when "assembled," form the backbone of a company's technology capability. Just as important is that the business and tech sides of the company work closely together and have the decision-making authority to move quickly.

This modular, platform-based IT setup of tech companies is what enables them to accelerate and innovate. They can experiment, fail, learn, and scale quickly: they can get products to market 100 times faster than their more lumbering peers (think weeks instead of months). With this kind of speed and flexibility, IT can and should become a focus for innovation and growth at the executive committee and board level. With new technologies and ways of working coming online, tech should be a competitive advantage, not a burden as it is in far too many companies today (see sidebar, "Why now?").

What a platform-based company looks like in practice

One of the global leading banks created about 30 platforms. One such platform was payments, which consisted of more than 60 applications that previously had been managed independently from each other. The top team decided to bring the 300-plus IT people working on development and maintenance of payments together with the corresponding people on the business side. Under joint business/IT leadership, this entity was empowered to move quickly on priority business initiatives, to modernize the IT structure, and to allocate the resources to make that happen.

The team shifted its working model and started running the payments platform as an internal business that served all the different parts of the bank (think payments as a service). This approach made it clear where to focus specific tech interventions: removal of nonstrategic IT applications; modernization and accelerated shift of the target applications into the cloud; connectivity to enable swapping solutions in or out easily; and, most important, a major step-up in feature/solution development for the internal business clients. This platform-based way of running the business was then progressively rolled out across the group. Prioritization is set by the top team (because empowerment does not mean anarchy), and all IT interventions are run the same way, to ensure consistency and replicability.

This is in stark contrast to the way large organizations normally act. Just establishing a business unit to manage a new offering or running a typical large IT project generally becomes a multiyear endeavor.

A closer look at the platform-based company

Think of a platform not just as technology but as a service, or what Silicon Valley calls a "product."

Platforms focus on business solutions to serve clients (internal or external) and to supply other platforms. They operate as independent entities that bring together business, technology,

Why now?

The notion of flexible, modular IT has been in vogue for ten years or so. But it largely remained a concept on paper, at least for many large incumbent companies. That has now completely changed because IT itself has changed, and important management practices such as agile and cross-collaboration are increasingly mainstream.

Modular IT is now technically possible.

	Before	Today
Connectivity	• Lack of well-established connectivity protocols	• Application programming interfaces allow blocks of functionality to talk easily
Deployment	• Slow and physical effort	• Cloud enables instantaneous deployment
Software language	• Static and hard to change	• New languages that are clean, structured for data usage, and easy to adjust
IT solutions	• Big monolithic solutions, which were hard to change even within explicit parameters	• Discrete blocks of functionality (eg, microservices), enabling much faster build and delivery
IT architecture	• Overly complex "spaghetti of systems" (often managed by independent business units)	• Technology ecosystems (internal and external), making it easy to pick and choose

governance, processes, and people management and are empowered to move quickly. They are run by a platform owner, who takes end-to-end responsibility for providing the solution and operating it like a service. Platform teams are cross-functional, with business, IT, and anything else that is needed, such as analytics, risk management, and so on. (Some companies call this a "tribe.") They work in an agile manner, delivering the solution itself, enabling continuous business-led innovation, and developing and running all necessary IT.

A platform-based company will have 20 to 40 plat-forms, each big enough to provide an important

and discrete service but small enough to be manageable. To simplify platform management, it helps to group them into three broad areas: customer journeys, business capabilities, and core IT capabilities (Exhibit 1).

For example, in personal banking, the customer-journey platforms cover the customer experiences of searching, opening an account, getting a mortgage, and so on. The business-capability platforms deliver the banking solutions, such as payments and credit analytics, and the support capabilities, such as employee-pension management, visual dashboarding, and

Exhibit 1

Platforms are grouped into three broad areas.

Customer-journey platforms ("journeys as a service") — Customer proposition and experience platforms built on reusable code (internal and external)

Business-capability platforms ("company as a service") — Business-solution platforms, designed to be modular and run as a business (internal and external)

Core IT platforms ("IT for IT") — Core IT provisioning, eg, cloud, data, automation (internal and external)

Mission control — Provides oversight, coordinates, allocates resources, sets standards

management information systems (MIS). Finally, the core IT platforms provide the shared technology on which the journeys and business capabilities run, such as the cloud platform, the data analytics environment, and the set of IT connectivity solutions (Exhibit 2).

Mission control to manage across platforms

Platforms are distinct units, but their value is based on how effectively they work together. Most companies overlook the criticality of making all IT components work together seamlessly because their attention is focused on individual projects. While most organizations understand the need to coordinate, the best ones develop a mission control capability with the resources and authority to lead and manage across platforms in three ways:

1. Make strategic and allocation decisions. The best mission control teams take a "clean sheet" approach to allocation decisions every year, prioritizing spend and effort on those platforms that can best support business goals and/or are in most urgent technical need. This means much more radical reallocations in budgeting and resourcing across platforms (and business units) than the

typical 5 to 10 percent increase or decrease that dominates allocation decisions at many companies. Mission control needs to work directly with the executive committee to secure resources and make these difficult trade-offs, while diving deep enough into the IT to manage critical path dependencies (cloud migration may require application rationalization first). In one case, the executive committee reduced the IT budget for one business unit by a third to prioritize platforms in the other two business units, based on the understanding that the following year's allocation would be a clean sheet again.

2. Set and enforce standards for speed and interoperability. The team establishes business standards, such as how teams work together in an agile way. It also sets technology standards, such as platform and application interfaces for seamless connectivity, the way code is written and logged in service libraries to ensure easy access, and what IT tools should be used for agile team management. Clear standards empower teams because they no longer have to worry about redoing work, miscommunication, or wasted effort in creating applications that will not work well with other applications. Mission control has the authority

to enforce the use of standards by, for example, not releasing any budget for project elements that deviate from them.

3. Manage and coordinate programs that cut across platforms. This function is more critical than previously understood, because working in a more agile and iterative way means that many requirements and dependencies, such as data access for a given business platform, for example, become clear only as work progresses. This reality is the blind spot of program managers and systems integrators because they understandably focus only on their own tightly defined mandate and project. Mission control acts as the design authority and oversight team to drive consistency and critical path delivery. Our research shows that not doing this severely slows down IT programs and wastes 30 to 40 percent of IT project spend.

How to take a platform approach

Becoming a platform-based company goes a step further than what most think of as traditionally transforming IT. It is a fundamental organizational and operational change to create an IT environment that runs as a set of platforms. As with any major transformation, it requires strong CEO leadership, quality teams, strong project management and communication, as well as value assurance. We have found that the following four actions have an outsize importance to successful completion of the shift to platform-based IT:

1. Assess the fitness of the platform portfolio. Business and IT should together quickly cluster the company's activities and associated IT into a set of 20 to 40 platforms that cover customer journeys, business capabilities, and core IT.

Exhibit 2

Retail and banking examples show the services offered on each platform.

	Retail example	Banking example
Customer-journey platforms	• In-store browsing and shopping for weekend • Clicking and collecting • Same-day home delivery • Subscribing	• Searching • Account opening • Transacting • Buying house (from valuing house to getting mortgage)
Business-capability platforms (to enable journeys)	"Retailer as a service" • Store- and warehouse-inventory management • Merchandising • Employee-pension management	"Bank as a service" • Payments • Real estate valuation • Credit underwriting • Employee-pension management
Core IT platforms	• In-store live video data-management platform • In-store face recognition • Cloud platform • Access and identity management	• Omnichannel IT platform-development environment • In-branch face recognition • Cloud platform • Access and identity management

This does not have to be definitive, just a useful starting point. Then conduct a fitness check on each platform: "fit" platforms are in good shape and only need investment to innovate and capture more value; "healthy" platforms work now but need modernization to prepare for future requirements; and "sick" platforms are no match for what competitors can do. They need a complete overhaul. DBS, one of Asia's leading banking groups, used a similar approach and communicated the assessment to the whole market at the end of 2017. Visualizing the fitness of all platforms is powerful because it enables an executive team to have the right debate on tough trade-offs and priorities and to then assertively reallocate resources (Exhibit 3).

2. Set up the initial platform teams and mission control. A successful transformation is about putting the right people in place at this stage. Establish teams for two to three priority platforms. Typically, a platform team will start with 20 to 30 people, which can then quickly ramp up to hundreds. It includes specific roles:

Platform leader—either a business or IT executive, or sometimes both as coleaders; a platform leader should be able to act like a real "product owner," a mini-business CEO with an IT engineering mind

Business members, who share responsibility with the technical team for all the design and the ongoing management as a business

Technical members, who manage all the IT applications associated with the platform and take full responsibility for modernization, renewal, ongoing feature development, and day-to-day operations

People with necessary functional skills, from analytics to finance

Exhibit 3

Companies need to perform a fitness assessment of their platforms.

The platform play: How to operate like a tech company
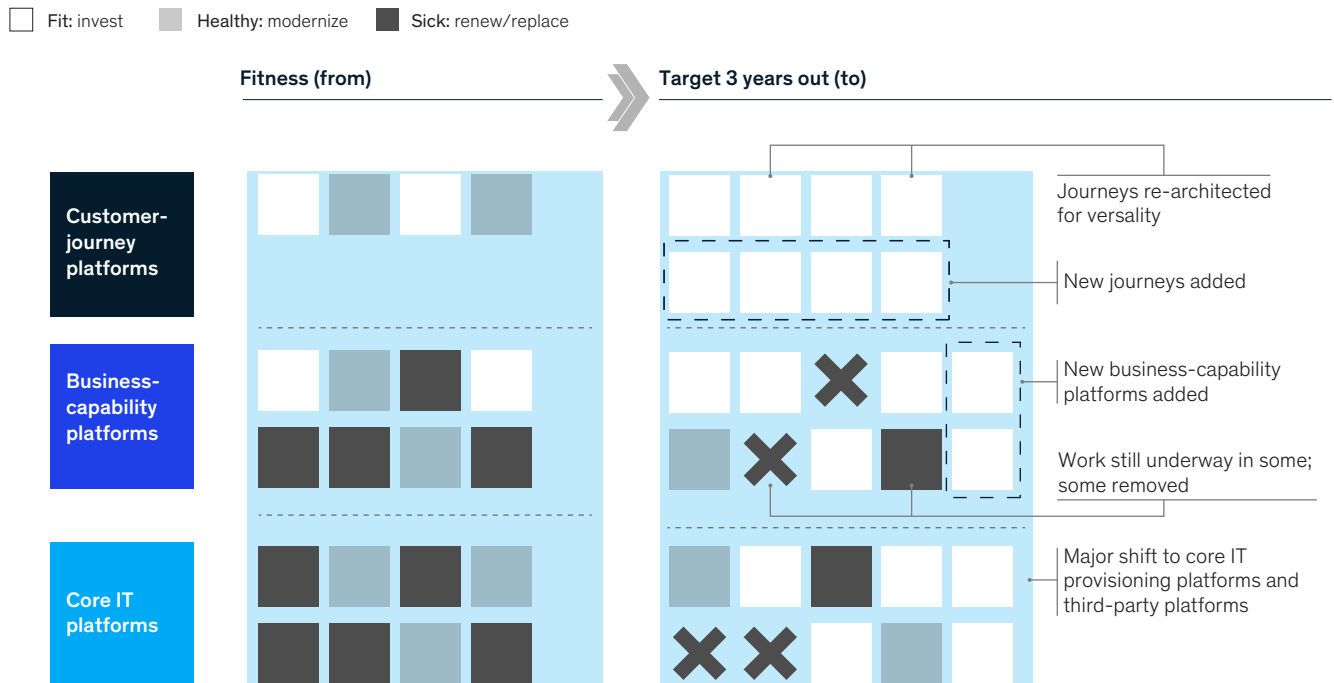
In parallel, start building out mission control with eight to ten of your very best finance, IT architecture, and program-management people. They need to constitute the most influential team working directly with the chief information officer, sometimes even reporting directly to the CEO. Mission control needs to have decision rights (or at least veto rights) on all IT spend and all platform budget requests.

3. Transform platform by platform. The transformation approach should progress platform by platform, focusing on top priorities. Platform teams take full responsibility for their work. They move quickly, using agile to carry out fast iterations of discrete pieces of work. With guidance from mission control and following prescribed standards, they are spared traditional alignment meetings, formal approvals, and other dependencies that slow everything down and create unnecessary complexity. Platform teams generally focus on a few core activities:

Converting platform capabilities to serve customers and other platforms. Affecting this shift requires a complete focus on the user experience through design thinking and digitization/ automation, and on interoperability by putting in place application programming interfaces (APIs) based on established standards and by creating service catalogs.

Evaluating and managing existing and necessary applications. This means decommissioning old and infrequently used applications; updating, renewing, or replacing core applications; and building value-added features outside of old applications. This is often where most of the work is needed. In conjunction with this effort is an acceleration into the public–private cloud.

Injecting data analytics into all possible activities of the platform. This means piloting and scaling use cases and explicitly accessing the company's analytics and data platforms (or starting to build them).

Writing (or rewriting) code as self-contained blocks or modules that can be easily swapped out and replaced wherever possible. Extensive use of APIs can help to provide the necessary flexibility to existing code.

4. Manage through the executive committee. While mission control plans and tackles the platform transformations day to day, allocating resources (the best people and the total IT budget) away from less productive platforms to those that are more productive and critical, the executive committee enforces the big decisions, sets a high business bar for transformation goals, and mediates all group-level issues. For example, during the transition, mission control may decide to deprioritize a platform but be overruled by management on the business side. This is when the executive committee needs to intervene.

Becoming a platform-based company is ultimately a question of mindset. It requires both the determination to stay the course and the flexibility to change and adjust based on what platform teams learn. By committing to this approach, IT can stop slowing down change and start accelerating it.

This article was originally published on McKinsey.com in February 2019.

Oliver Bossert is a senior expert in McKinsey's Frankfurt office, and **Driek Desmet** is a senior partner in the London office.

How to extract maximum value from a zero-based design approach to customer journeys

Companies finding success in transforming their customer journeys are discovering that four practices are critical.

by JP Higgins, Elixabete Larrea, Swapnil Prabha, Alex Singla, and Rohit Sood

In recent years, the business landscape has undergone massive changes thanks to shifting economic conditions, heightened customer expectations, and technological innovation. This reality has put additional pressure on businesses to improve performance and redesign their products, services, and even organizations. Zero-based design has emerged as a potent approach.

If done right, the principles of zero-based design—which essentially encourages people to cast aside assumptions to expand the scope of discovery—will help organizations achieve step changes in performance compared with traditional approaches. Typical results include an increase of 30 to 50 percent in operational productivity and a rise of ten to 20 points in customer-satisfaction scores, fueled by enhanced responsiveness of up to 80 percent.

Given that impact, many organizations in the financial-services industry have tried to use zero-based design to transform customer journeys. But in practice, those efforts have often fallen short of their full value potential because organizations tend to narrowly define what zero-based design actually is. For this reason, they do not put in place the necessary building blocks so that great ideas lead to great solutions.

In our experience, four issues are the primary culprits: incomplete or unclear definitions of end-to-end journeys (both customer facing and internal),[1] lack of the right skill sets on the journey-redesign team, constrained ideation, and regimented and inflexible ways of working.

To address these issues, we find it helpful to ask the following questions.

1. Are all processes in your organization mapped against end-to-end customer journeys?

Companies often believe they have worked across departments to define end-to-end customer journeys by assembling members of different departments or aligning the organization to resolve a single pain point. This approach, however, doesn't provide the necessary clarity needed to define an end-to-end journey. What's needed is for companies to identify and reframe all processes throughout the organization into a comprehensive set of end-to-end journeys. This means accounting for processes that directly touch the customer as well as the supporting middle- and back-office functions. This is crucial because it is important to have the right definition of journeys to which the zero-based design approach can be applied. Otherwise, companies will risk delivering incomplete and inconsistent experiences to their customers.

A good journey definition includes the following:

— *Places the customer at the center and uses the customer's language.* Taking this perspective will help the journey team work with the customer in mind. For example, an insurance sales customer's journey definition might be, "I want to protect myself from the unexpected."

— *Identifies a clear beginning and end.* Defining the outlines of the customer journey will force the team to think comprehensively about the customer experience instead of trying to arrive at point-by-point solutions. In insurance, a sales journey may start when a customer begins to evaluate options and end when he or she receives the policy.

— *Crosses departmental boundaries.* By considering the multiple functional groups that touch the customer journey, teams can solve for the customer's integrated experience. In the insurance sales example, the journey will involve a minimum of the sales, pricing, policy-issuance, and even claims departments.

To define a set of end-to-end customer journeys, teams will need to invest significant effort and apply the right resources and capabilities, such as analytics and workforce management. When

---

[1] For more, see Albert Bollard, Elixabete Larrea, Alex Singla, and Rohit Sood, "The next-generation operating model for the digital world," March 2017, McKinsey.com.

Applying the 'art of the possible' with ideation sessions

Imagine that a commercial-lines insurance carrier wants to reimagine the journey by which a newly acquired customer sets up his or her account. Here is what an "art of the possible" ideation session could look like across the four elements:

Aspiration. The CEO and senior leader responsible for this journey kick off the "art of the possible" workshop together with the relevant journey team. They remind the team of the carrier's strategic vision and explicitly link it to measurable goals for the journey in question, such as targets to increase revenue by 10 percent, reduce overall costs by more than 30 percent, and improve already excellent customer-satisfaction scores. The CEO underscores the vision with a challenge to the team to achieve these results within 12 months. The team has clear goals they can shoot for and a way to measure whether they have succeeded.

Inspiration. Next, the team sees and hears about examples of innovative processes and approaches from outside the insurance industry. The group, for example, learns about how e-commerce companies create dynamic shopping experiences that cater to multiple shopper personas and how companies use cognitive agents that can have humanlike interactions, complete with natural-sounding voices.

The participants then debate how these innovations apply to the journey they are redesigning. As a result, they start thinking about how to reinvent the process, drawing on the examples they've reviewed.

Education on next-gen capabilities. The team then learns about specific new technologies, capabilities, and practices, with a goal of demystifying them and understanding how these levers solve specific problems. For example, participants gain an understanding of the solutions that different elements of automation can provide and when to use each capability.

The inspiration element continues as the team learns about, for example, how retail and consumer industries apply geospatial capabilities to optimize their network of stores or how the healthcare industry applies a value-based care approach to measure and compare provider performance. Participants now have a basic knowledge of the building blocks—advanced analytics, performance measurement, new technologies—they need to assemble to reinvent their customer journey.

Ideation. With their creativity primed, participants draw on practices used at some of the most innovative companies in the world. The team works, for example, in 30-second ideation sprints to record ideas quickly, without time to filter or judge their output. This yields a spectrum of creative ideas, which could include chatbot-enabled support for customers to set up accounts or advanced-analytics-enabled loss control and mitigation plans as additional services for customers.

---

properly done, the outcome will be unprecedented visibility into every aspect of the customer journey. For example, a personal lines property-and-casualty (P&C) carrier defining its end-to-end journeys would quickly realize that a customer who has been in an accident and is now recovering from an injury and getting his or her vehicle repaired would perceive that entire experience as a single journey. Therefore, even if the carrier's claims organization separates the vehicle-damage and injury adjustors into two different groups, they will need to come together to redesign the claims-customer journey.

2. Do you have people with diverse skill sets on your journey-redesign teams?

Many organizations bring together IT employees and business experts to redesign customer journeys. This collaboration helps, but it is not enough.

The success of a zero-based design effort depends on the journey team having a mix of skill sets to help generate ideas, create prototypes, test them, and then iterate on them. Following are two nontraditional but critical roles that need to be part of those teams:

— Experienced *designers* are adept at interpreting multiple stakeholder perspectives and translating them into an optimized possible journey design for the customer.

— *Customer anthropologists* can help the team understand customer insights more deeply. They interpret quantitative and qualitative research data and reconcile nonintuitive inputs to form a coherent narrative around the customer experience.

Financial-services firms and traditional organizations don't necessarily have such nontraditional skills in-house. When they do exist, the skills can vary significantly, and attracting the right external talent is a challenge. Companies that are serious about pursuing zero-based design must invest in updated, innovative recruiting strategies to identify, hire, and develop employees with the right skill sets for these nontraditional roles.

3. Are your ideation sessions sparking true innovation or derivative ideas?

Many proactive organizations are learning the basics of design thinking and ideation sessions. Companies often start with inspiring videos, integrate customer perspectives into ideation sessions, and include subject-matter experts in them as well.

While these steps are an important start, they don't maximize the potential of zero-based design. An "art of the possible" approach can amplify creative thinking by releasing participants from constraints and inspiring them with possibilities.[2] An effective ideation session should include four critical elements (for more, see sidebar, "Applying the 'art of the possible' with ideation sessions"):

— *A clear, bold aspiration in line with the company's overall strategy.* Members of the ideation team must have complete clarity on the company's overall vision, strategy, and

goals (both financial and nonfinancial) that they are addressing. To achieve this clarity, senior leaders must be present at ideation sessions to articulate and credibly communicate the vision.

— *Inspiration from outside innovators.* Cross-functional teams that are exposed to examples of creative thinking in action from other sectors are more likely to challenge their own insular thinking and produce creative ideas.

— *Next-generation capabilities.* Zero-based design participants who become familiar with new capabilities such as automation, advanced analytics, and digital are better able to make connections between potential innovative solutions and existing business problems.[3] As a result, "art of the possible" workshops frequently incorporate overviews of advanced capabilities and other relevant educational programming.

— *Ideation in rapid sprints.* All zero-based design sessions require team members to brainstorm. However, "art of the possible" workshops jump-start the process by leading participants through a series of rapid-fire exercises designed to challenge them to take on different points of view. The result is an exciting environment that stimulates creative visions of redesigned journeys.

4. Is your organization as agile as your journey team?

Many organizations that apply zero-based design believe it is sufficient for just their journey-redesign teams to adopt an agile way of working. To get results, however, the entire organization needs to adapt to the pace, flexibility, autonomy, and transparency of the journey teams.

Organizations can achieve the full potential of zero-based design only if they evolve their governance models and infrastructure to enable fast-paced, distributed, and accessible decision

[2] The "art of the possible" is our approach for implementing zero-based design principles in organizations and teams to spark unconstrained ideation.
[3] Albert Bollard, Elixabete Larrea, Alex Singla, and Rohit Sood, "The next-generation operating model for the digital world," March 2017, McKinsey.com.

making. Successful organizations adopt a test-and-learn mindset and diligently measure success by results and outcomes. Companies that have been successful at zero-based design share some common traits:

— Leadership updates and steering-committee meetings that focus on discussions and demonstrations in the work area instead of presentations in boardrooms.

— Frequent and rapid investment decisions based on start-up-like pitches supported by rigorous but not cumbersome business cases that can be evaluated and approved to keep pace with the ideation team.

— Adoption of "agile" routines such as regular huddles, brief work sprints focused on output, and regular retrospective evaluations. This mode of working allows organizations to be nimble and respond to market changes quickly.

———————

A fundamental redesign of end-to-end customer journeys is not the place for half measures. Zero-based design can help organizations transform processes, mindsets, and operations, but only if they fully commit to four essential areas where organizations have traditionally missed the mark.

This article was originally published on McKinsey.com in January 2019.

JP Higgins is an associate partner in McKinsey's New York office; **Elixabete Larrea** is a partner in the Boston office, where **Swapnil Prabha** is an associate partner; **Alex Singla** is a senior partner in the Chicago office; and **Rohit Sood** is a senior partner in the Toronto office.

Reinvent technology delivery

The journey to an agile organization

You know what an agile organization is, and why it's important. But figuring out how to pull off an agile transformation is another question.

by Daniel Brosseau, Sherina Ebrahim, Christopher Handscomb, and Shail Thaker

Agility is catching fire, and there is growing recognition of its transformational benefits. But moving to an agile operating model is tough, especially for established companies. There are several paths to agility and many different starting points, yet successful agile transformations all share the common elements described in this article.

Agile organizations are different. Traditional organizations are built around a static, siloed, structural hierarchy, whereas agile organizations are characterized as a network of teams operating in rapid learning and decision-making cycles. Traditional organizations place their governance bodies at their apex, and decision rights flow down the hierarchy; conversely, agile organizations instill a common purpose and use new data to give decision rights to the teams closest to the information. An agile organization can ideally combine velocity and adaptability with stability and efficiency.[1]

Transforming to an agile operating model

Any enterprise-wide agile transformation needs to be both comprehensive and iterative. That is, it should be comprehensive in that it touches strategy, structure, people, process, and technology, and iterative in that not everything can be planned up front (Exhibit 1).

Exhibit 1

A comprehensive transformation touches every facet of the organization, including people, process, strategy, structure, and technology.

Workforce size and location model: take a mission-oriented approach to workforce sizing and location

Reporting structure: simplify and delay your reporting structure

Role and responsibilities: build roles and responsibilities up from the businesses and limit HQ to the minimum necessary to run the businesses

Governance: streamline decision making

Supporting systems and tools: ensure the enterprise has the right tools to support an agile way of working

Architecture evolution: enable the design and evolution of architecture based on requirements

Delivery pipeline: automate your testing and integration processes to enable fast and continuous delivery

IT infrastructure and operations: ensure you have the appropriate infrastructure and operations to support rapid changes

Leadership: train managers to provide vision, inspire, model, and coach rather than direct

Talent management: be ready to attract and retain the best talent

Culture: challenge existing culture and mindsets

Informal networks and communication: create opportunities for employees to form organic networks across the organization

Team processes: free up a team's time to work on value-creating activities

Linkage mechanisms: create means for resources from different functions to collaborate

Planning and decision processes: recognize that even the best plans can fail, and design planning and decision making to rapidly test and learn

Performance management: structure performance management based on outcomes

Structure · People · Technology · Processes · Strategy

[1] Wouter Aghina, Aaron De Smet, and Kirsten Weerda, "Agility: It rhymes with stability," *McKinsey Quarterly*, December 2015, McKinsey.com.

There are many different paths to enterprise agility. Some organizations are born agile—they use an agile operating model from the start. As for others, broadly put, we see three types of journeys to agile: all-in, which entails an organization-wide commitment to go agile and a series of waves of agile transformation; step-wise, which involves a systematic and more discreet approach; and emergent, which represents essentially a bottom-up approach.

Born-agile organizations are relatively common in the technology sector (for instance, Spotify or Riot Games[2]), with rare examples in other industries (Hilcorp, a North American oil and gas company, is a case in point[3]). Most organizations must undergo a transformation to embrace enterprise agility. Such transformations vary in pace, scope, and approach, but all contain a set of common elements across two broad stages (Exhibit 2).

Exhibit 2

Two components make up an iterative approach that requires the organizations to continuously test, learn, and course correct.

Aspire, design, and pilot	Scale and improve
Agree on end-state vision, develop blueprint, and learn through agile pilots	Roll out agile cells and transform the organization backbone, supported by a systematic approach to build capabilities

Top-team aspiration
Align and commit to the vision and scope of the agile transformation, informed by assessment of the organization today

Blueprint
Identify how agile can unlock most value and design corresponding operating model

Agile pilots
Launch pilots to test the agile operating model in a defined area

Agile cell deployment and support
Design and roll out agile units wave by wave, including moving people to new roles

Backbone transformation
Rewire core processes and systems of the organization to support agility

Capability accelerator
Build the new capabilities required to sustain agility

Culture and change team
Coordinate and communicate transformation, remove roadblocks, and start culture refresh

[2] Stephen Denning, *The Age of Agile: How Smart Companies Are Transforming the Way Work Gets Done*, New York: AMACOM, 2018.
[3] "Digging deep for organizational innovation: An interview with Greg Lalicker," *McKinsey Quarterly*, April 2018, McKinsey.com.

To build the top team's understanding and aspiration, nothing beats site visits to companies that have undergone an agile transformation.

First, successful transformations start with an effort to aspire, design, and pilot the new agile operating model. These elements can occur in any order and often happen in parallel. Second, the impetus to scale and improve involves increasing the number of agile cells. However, this involves much more than simply rolling out more pilots. Organizations may iterate among these stages as they roll out agility across more and more of their component parts.

Aspire, design, and pilot

Most transformations start with building the top team's understanding and aspirations, creating a blueprint to identify how agility will add value, and learning through agile pilots. These three elements inform one another and often overlap.

Top-team aspiration. Successful agile transformations need strong and aligned leadership from the top. A compelling, commonly understood and jointly owned aspiration is critical for success. Adopting an agile operating model can alleviate challenges in the current organization (such as unclear accountabilities, problematic interfaces, or slow decision making). Yet a desire to address pain points is not enough; there is a bigger prize. As one CEO observed, "I'd never have launched this agile transformation if I only wanted to remove

pain points; we're doing this because we need to fundamentally transform the company to compete in the future." This aligns with McKinsey research showing that transformations emphasizing both strengths and challenges are three times more likely to succeed.[4]

To build the top team's understanding and aspiration, nothing beats site visits to companies that have undergone an agile transformation. For example, the entire leadership team at a global telecommunications company contemplating an agile transformation invested a week to visit ING (a Dutch bank), TDC (a Danish telecommunications company), Spotify, Entel (a Chilean communications company), and others prior to launching an agile transformation.[5]

Blueprint. The blueprint for an agile operating model is much more than an organization chart and must provide a clear vision and design of how a new operating model might work (Exhibit 3). An agile transformation fundamentally changes the way work is done and, therefore, blueprinting also needs to identify changes to the people, processes, and technology elements of the operating model. The blueprint should, at first, be a minimum viable product developed in a fast-paced, iterative manner that gives enough direction for the

[4] Scott Keller, Mary Meaney, and Caroline Pung, "What successful transformations share," March 2010, McKinsey.com.
[5] Bo Krag Esbensen, Klemens Hjartar, David Pralong, and Olli Salo, "A tale of two agile paths: How a pair of operators set up their organizational transformations," February 2019, McKinsey.com.

Exhibit 3

The blueprint provides a clear vision and design for a new operating model.

Iterative process to derive agile operating model

Value	Structure	Agile teams	Backbone	Road map
Understand where value is created in the industry and where company needs to be distinctive	Design the overall structure (eg, organizational axes, reporting lines)	Identify teams and define missions to deliver value streams	Outline requirements on the core processes, people, and technology to enable agility	Decide on implementation approach
Define end-to-end value streams	Identify organizational groupings, informed by value streams to create an organization map	Select best agile way of working for each mission, eg, cross-functional, flow to work	Identify required changes in culture and mindsets	Develop high-level road map
Identify elements that can benefit from greater agility, either more dynamic or stable	Define the "capability" axis, eg, chapters or disciplines			Create backlog
				Prioritize for immediate next steps

organization to start testing the design. The first step in blueprinting is to get clear on where the value lies. All operating-model design must be grounded in an understanding of how value is created in the industry and how the individual organization creates value. This fundamentally links to strategy.

Next comes structure. An agile organization does not deliver work according to a classic organization chart; rather, it can be thought of as a series of cells (or "teams," "squads," or "pools") grouped around common missions, often called "tribes." The blueprinting element should produce a "tribe map" to illustrate how individuals that are grouped get work done, as well as a more recognizable organization chart to show the capability axis along which common skill sets are owned and managed (Exhibit 4).

Individual agile cells are defined by outcomes or missions rather than by input actions or capabilities. Teams performing different types of missions will likely use different agile models. However, three types of agile cells are most common. First, cross-functional teams deliver products, projects, or activities. These have the knowledge and skills within the team and should have a mission representing end-to-end delivery of the associated value stream. The "squads and tribes" model developed by Spotify and used by ING, among others, is one example.[6] Second, self-managing teams deliver baseload activity and are relatively stable over time. These teams define the best way to set goals, prioritize activities, and focus effort. Lean-manufacturing teams or maintenance crews could be examples of this agile approach. Indeed, more broadly, lean-management tools and practices are highly complementary with enterprise agility. Third, flow-to-work pools of

---

[6] "ING's agile transformation: An interview with Bart Schlatmann," *McKinsey Quarterly*, January 2017, McKinsey.com.

Exhibit 4

The blueprint combines a 'tribe map,' illustrating how individuals are grouped, with a 'capability' axis along which common skill sets are owned and managed.

Example tribe map
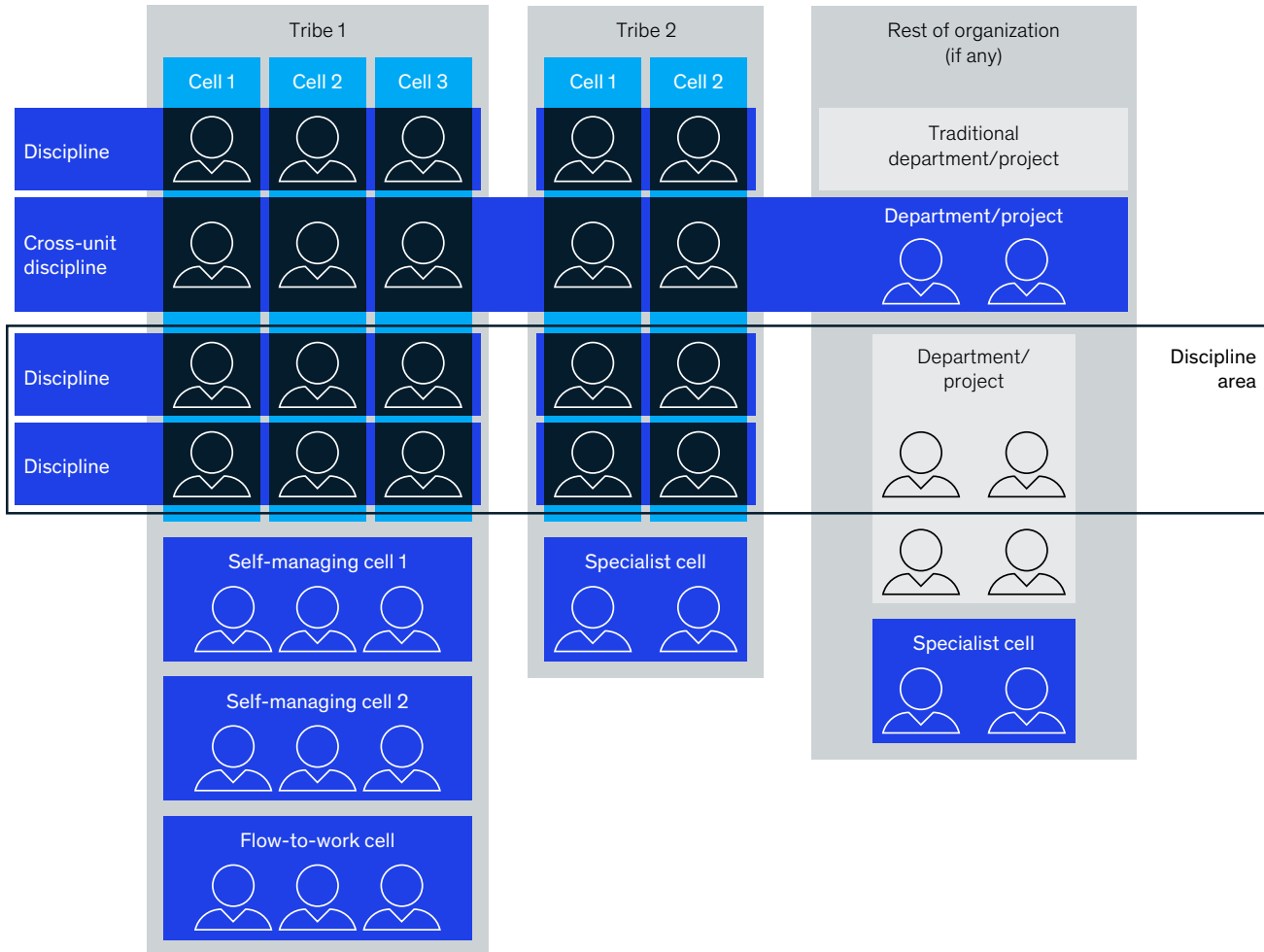
individuals are staffed full time to different tasks based on the priority of the need. Functional teams like HR or scarce resources like enterprise architects are often seen as "flow" resources.

One telecommunications company identified five major activities across their business and selected an agile approach for each: channel and delivery units (for example, stores) were organized as self-

managing teams to increase local flexibility with joint accountability; segment ownership, product development, and enabling teams were organized in cross-functional squads and tribes; and centers of excellence for all other activities (including subject-matter experts and corporate support activities) combined flow-to-work and temporary cross-functional teams for specific tasks.

Working in teams may sound familiar, but at scale this requires change across the whole operating model to provide appropriate governance and coordination. The organizational backbone comprises the stable components of an agile operating model that are essential to enable agile teams. Typically, these backbone elements include core processes (for example, talent management, budgeting, planning, performance management, and risk), people elements (including a North Star,[7] core values, and expected leadership behaviors), and technology components. In trying to scale up, many agile transformations fail by simply launching more agile teams without addressing these backbone elements.

The final step of blueprinting is to outline the implementation road map. This road map should contain, at minimum, a view on the overall scope and pace of the transformation, and the list (or "backlog") of tasks.

The five steps of the blueprint form a coherent approach. A commercial insurer in North America used an agile blueprint to accelerate innovation of digital and business processes. It defined a chapter-based organization structure and created a new organization of product managers (who played product-owner roles in agile teams) to guide teams toward business outcomes. They defined a team structure mostly aligned to customer and internal user journeys, with dedicated teams to grow selected businesses. They created a stable planning and performance-management backbone, as well as a culture of risk taking, and they used an 18-month road map to create all the new positions, train personnel in the new roles, and implement the change in full.

Agile pilots. The purpose of a pilot is to demonstrate the value of agile ways of working through tangible business outcomes. Early experiments may be limited to individual teams, but most pilots involve multiple teams to test the broader elements of enterprise agility. Nothing convinces skeptical executives like teams of their own employees having verifiable impact through agile working. For example, one oil and gas company launched a series of agile pilots through which cross-functional teams managed to design wells in 50 to 75 percent less time than the historical average.

Initially, the scope of the agile pilot must be defined and the team set up with a practical end in view; this might include deciding on team staffing, structure, work space, facilities, and resources. Next, the way the agile pilot will run must be outlined with respect to structure, process, and people; this is typically collated in a playbook that forms the basis for communications with those in the pilot.

Scale and improve
Scaling beyond a few pilots is no small feat; this is where most agile transformations fail. It requires recognition from leadership that scale-up will require an iterative mindset: learning is rapidly incorporated in the scale-up plan. In this, enough time is required—a significant portion of key leaders' time—as well as willingness to role model new mindsets and behaviors. Agile transformations acknowledge that not everything can be known and planned for, and that the best way to implement is to adjust as you go. For example, a leading European bank first deployed four "frontrunner" tribes to test the blueprint in action and adapted important elements of the blueprint across the delivery enterprise. Such an iterative rollout approach enables continuous refinement based on constant feedback and capability building for key roles across the organization, including agile coaches, product owners, scrum masters, and leadership.

Agile cell deployment and support. Agile scale-up first and foremost requires standing up more agile cells. However, an organization can't pilot its way to enterprise agility. The transformation should match the organizational cadence, context, and aspiration. But at some point, it is necessary to leap toward

---

[7] To give coherence and focus to their distributed value creation models, agile organizations set a shared purpose and vision—"the North Star"— for the organization that helps people feel personally and emotionally invested. For more, see Wouter Aghina, Aaron De Smet, Gerald Lackey, Michael Lurie, and Monica Murarka, "The five trademarks of agile organizations," January 2018, McKinsey.com.

the new agile operating model, ways of working, and culture. For large organizations, this need not be a day one for the entirety but will likely progress through a series of waves.

Many chose to start by transforming their headquarters and product-development organizations before touching frontline, customer-facing units (call centers, stores, or manufacturing facilities). It is possible to transform one factory or one end-to-end customer journey at a time, but highly interconnected functions in the headquarters may need an all-in transition approach.

The size and scope of waves depend on the context and aspiration. For example, a large Eastern European bank designed waves of nine months, where the diagnostic, design, and selection for ten tribes, 150 squads, and 1,500 roles were performed in the first three months and then deployed over a six-month period, launching a new tribe every two weeks. Furthermore, the scale-up effort was a top priority for C-suite executives, which dedicated more than 10 percent of their time to the transformation.

Resources to support new agile cells—for example, availability of agile coaches or appropriate work space—can often limit the speed of scale-up. Failure to address the support of new agile cells can cause friction and delay in the transformation.

Backbone transformation. Reflecting on its agile experience before scaling up, one executive observed: "Most of our agile pilots are working despite, rather than supported by, our broader organizational 'wiring' [processes, systems, and even beliefs and values] that forms what we call the backbone of an organization." The backbone governs how decisions get made; how people, budgets, and capital get deployed; and how risk gets managed. Taking an organization to an agile operating model requires that this backbone be transformed (Exhibit 5).

Capability accelerator. Successfully scaling an agile operating model requires new skills, behaviors, and mindsets across the organization. This is vitally important and constitutes an intensive phase of an agile transformation. Most organizations require existing staff to take on these new roles or responsibilities, and as such, need a way to build new skills and capabilities. Specifically, any successful agile transformation will invariably create a capability accelerator to retrain and reorganize staff, make the agile idea common to all, and develop the right skills across the organization.

A typical capability journey may well have distinct phases. First, organizations need to identify the number of trainers (agile coaches) required, and then hire and develop them; a failure to do so can cause delay and blockage when the agile transformation extends across the whole organization. Second, as part of building capabilities, the organization must define the new agile roles (agile coaches, product owners, tribe leads, chapter leads, and product owners, for example), along with a clear idea of what success looks like in each role. Third, learning and career paths should be set for all staff, making clear the opportunities that the agile transformation opens up. Fourth, the organization needs to enable continuous learning and improvement across the organization (this will entail a large-scale digital and communications program). Finally, it's necessary to design and run a whole-organization effort to raise agile skills (often by means of intensive boot camps) and ensure that new staff are onboarded appropriately. Larger organizations often set up an academy to consolidate and formalize these functions.

Focusing on culture and the change team

A culture and change team is an essential coordinating element of an agile transformation. But it is not a traditional project-management office; rather, the emphasis should be on enabling the other transformation elements, helping to remove impediments and catalyzing culture change.

As an example, Roche, a global healthcare company, launched a global leadership initiative as a central component of its transformation to become a

Exhibit 5

The organization's backbone must be transformed for an agile operating model.

Backbone components

Decision making and governance setup

The governance and decision-making process is simplified—for example, a set of ring-fenced decision rights that need to be taken at the executive-committee level (typically a subset of decisions made today by those bodies), while everything else is pushed down the organization

Business planning and budgeting

The methods of strategic decision making change significantly in agile, as organization-wide goals need to be set, aligned, and reviewed through more fit-for-purpose processes; budgeting becomes a flexible process that seeks to reprioritize and reallocate capital as necessary

Funding decision making

Funding decisions are made more frequently (from annual cycles), and a continuous review of capital allocation can be done through approaches similar to venture capital and based on quarterly business reviews

Performance management

Performance management moves from optimizing individual key performance indicators to assessing performance based on results achieved by teams, or so-called objectives and key results

Roles and career paths

Agile roles need to be defined initially to ensure coverage of strategic priorities and alignment; it is also critical to define the career path through a flatter organization to sustain the transformation and to lay out how roles are initially selected to enact the new operating model

Risk management and assurance

Done well, an agile operating model can strengthen control around risks and assure technical quality by removing layers, increasing transparency around what is happening, and preserving technical competency—especially critical for organizations in high-hazard industries

Workforce location and work space

Agile team members will likely need to be on-site and will require a work space to enable agile ways of working and collaboration with other cells

Technology

Deploying technology foundations will enable short time to market and high quality, for instance, via architecture evolution and the use of a self-service delivery pipeline and infrastructure (eg, cloud)

more agile enterprise.[8] It designed a four-day program with a combined focus on personal and organizational transformation. More than 4,000 leaders have now been touched by the effort, helping to shift the collective consciousness and capabilities for leaders to deliver the change.

The importance of investing in culture and change on the journey to agility cannot be overstated. Agile is, above all, a mindset. Without the right mindset, all other parts of the agile operating system can be in place, and yet companies will see few benefits. In contrast, when leaders and teams have a strong agile mindset, then a clear aspiration alone is often enough for a successful agile operating model to emerge.

[8] "How a healthcare company is pursuing agile transformation: An interview with Tammy Lowry," January 2019, McKinsey.com.

Understanding transformation archetypes

All successful enterprise-wide agile transformations include the elements described above, but there are several different ways in which the elements can be combined and sequenced. As introduced earlier, there are three major transformation archetypes:

1. *Step-wise.* Transforming to an agile organization often feels like a step into the dark for senior leaders. Perhaps understandably, then, the most common transformation archetype shows a clear distinction between the aspire, design, and pilot phase and the scale and improve phase. Many companies will run multiple rounds of pilots and iterate their blueprint several times before fully committing to scaling up across a large part of the organization. It is not uncommon for this process to take one to two years, as leaders and the organization build familiarity with agility and prove to themselves that agile ways of working can bring value to their organization. Organizations may well go through several subsequent rounds of aspire, design, and pilot before scaling up elsewhere.

2. *All-in.* Although less common, an increasing number of organizations gain strong conviction early on and fully commit up front to move the whole organization to an agile model. Leaders from these organizations define a plan to execute all steps of the transformation approach as quickly as possible. Even in these types of transformation it is rare for the whole organization to transform to an agile model in a single "big bang"; rather, it is more common for the transformation to proceed through a number of planned waves.

3. *Emergent.* It is impossible—and not very agile—to plan out an agile transformation in detail from the start. Instead, most agile transformations have emergent elements. Some organizations have chosen to progress their entire agile transformation through an emergent, bottom-up approach. In this archetype, an aspiration from top leaders sets a clear direction, and significant effort is spent building agile mindsets and capabilities among leaders.

———————

"It's like this," one CEO explained. "We are 3,000 people on a giant cruise ship. But what we need to be is 3,000 people in a few hundred yachts. So, how do I get my people safely into those smaller boats?" As is increasingly common, the discussion had moved from if an agile operating model was applicable to how leaders could help their organization transform. Navigating an organization to an agile operating model is not easy. The elements of an agile transformation described in this article provide a guide.
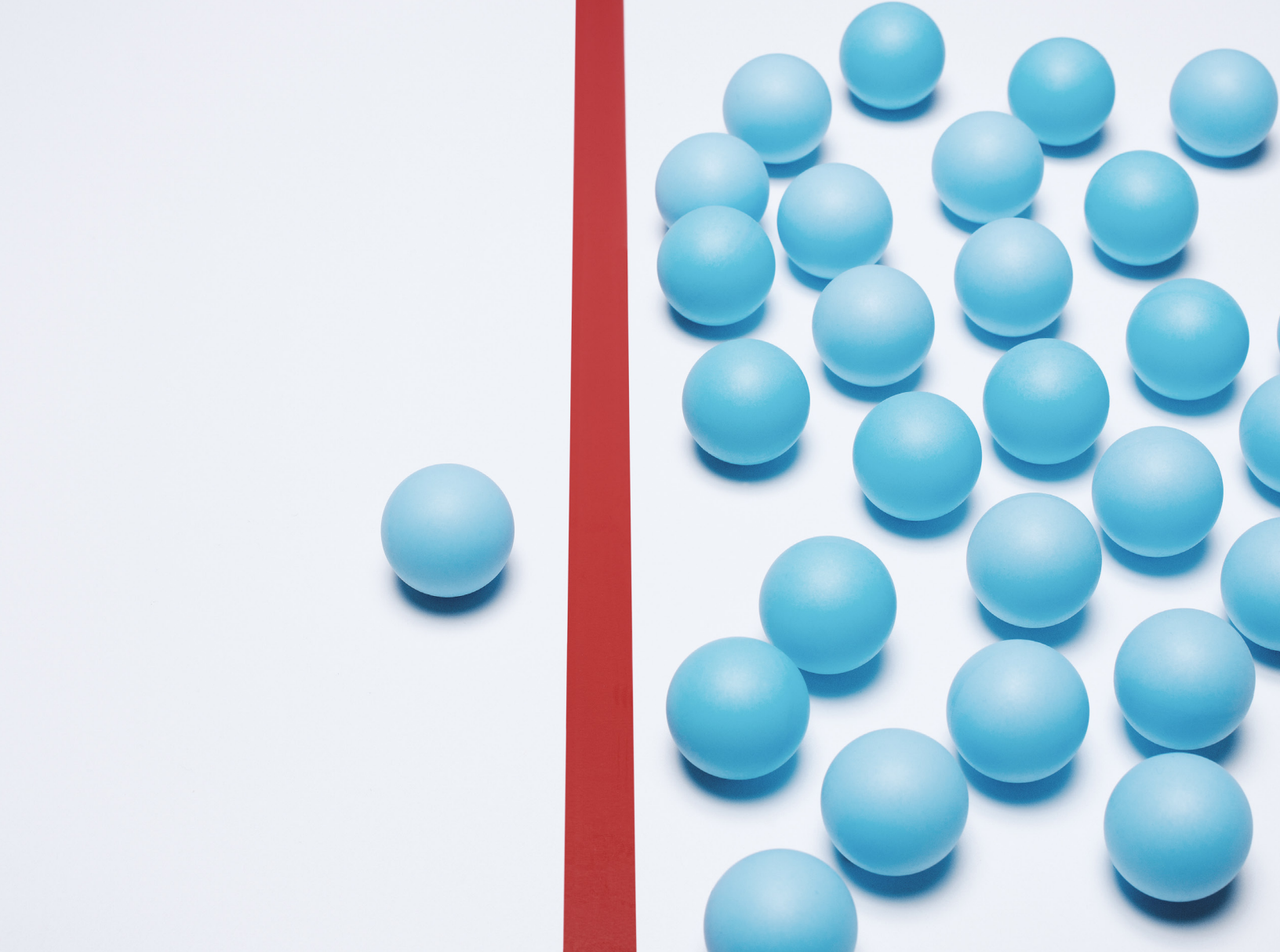
Flip the ratio: Taking IT from bottleneck to battle ready

A new way to focus on outcomes and results can free IT organizations to spend more time on business priorities.

by Nagendra Bommadevara, Steve Jansen, Lauren Klak, and Maneesh Subherwal

What if an investor managed your IT? One thing it would likely hit on quickly is an important detail: for many companies, a larger proportion of the IT organization is focused on support and administrative work that is often manual and inefficient—testing, deployment, maintenance, code fixes, and so on. At two financial services organizations we analyzed, a stunning 90 percent of the IT organization was focused on these kinds of tasks. That left just 10 percent of technologists' capacity for business priorities and market-differentiating work (Exhibit 1).

This state of affairs partly explains why IT is often viewed as a cost center and a bottleneck by the business. It also highlights one of the reasons that incumbents are struggling to keep up with tech companies. With just 10 percent of IT allocated to generating new business value, incumbents are not battle ready when it comes to contending with nimble tech players.

As any investor would tell you, place your resource bets where you believe there is value. For IT, that means flipping the ratio, so that the great majority of IT resources are working on products that build value for the business. As simple as that may sound, few IT organizations have been able to do it. Some companies have managed to pull it off, however, by following a specific recipe that allows them to

Exhibit 1

Too little of IT's resources go toward business-differentiating activities.

What business wants from IT

Business-oriented software development

All other IT

What IT provides

Business-oriented software development

Other software development

Support for software development

Administrative IT

- **~30% of IT organization is developers**
  - <30% development on truly market-differentiating business features
  - >70% development on repeat/non-value-add work (eg, lack of application programming interfaces)

- **Significant support for developers to get code into production (eg, testers, deployment specialists)**

- **Administrative and maintenance**
  - Application maintenance
  - IT infrastructure

work better and smarter. Typical payback in making this shift—freeing as much as 30 to 40 percent of IT labor costs—occurs within 18 to 24 months. Flipping the ratio can improve time to market and quality. The framework also allows organizations to quickly evaluate the business value of new technologies (cloud, microservices, automation, AI) and then rapidly scale adoption.

How to escape the trap

IT leaders have been trying to increase the productivity of their teams, and many have made good progress. But too often, cloud and other solutions languish in proof-of-concept stages with little funding and, in many situations, no business case. Meanwhile, the day-to-day pressure of running an IT shop—improving service levels while lowering costs for existing systems—continues.

To flip the ratio, four things need to happen.

1. Extend agile to back-end IT

One of the main reasons back-end systems demand so many resources is that they do not take advantage of agile ways of working that have become second nature to most software developers. Either back-end teams confuse "doing" agile rather than actually "being" agile, running waterfall projects using the scrum method but not working in small teams rapidly iterating on small chunks of code, or agile doesn't even make it to the back-end teams. Even application maintenance and IT infrastructure can benefit from agile principles, which is significant, since these areas often make up 40 to 60 percent of the IT organization. By introducing true agile methods— small, cross-functional teams or squads working in rapid iterations—to relevant enterprise IT work, companies can radically reduce the resources needed to support those systems while substantially improving service quality and the potential for automation.

One midsize US-based financial services company discovered just how much value using agile for back-end IT functions could be realized. At first, application-maintenance and IT-infrastructure functions—about 40 percent of the organization—

did not use agile. Making matters worse, most of the demand on this group was reactive, handling incidents—data fixes and batch updates, for example—that required handoffs across multiple product teams and caused frequent interruptions, significantly reducing productivity.

The company decided to move to an agile operating model. It started by rigorously quantifying demand to improve transparency and looking at products based on how they fit into the end-to-end value chain, which allowed the company to better understand the dependencies across multiple products.

With better insight into demand, the company created small, self-sufficient teams to not just meet demand but figure out how to reduce it. By better understanding business needs, teams eliminated some demand by providing self-service options. Cross-functional teams had the people needed to not only identify the root cause of incidents but correct them immediately. They also focused on preventive maintenance and predictive monitoring to address issues before they became significant problems (Exhibit 2).

Within six months, the company had reduced application operations spend by more than 30 percent and improved system stability (reduced incident volume and elimination of false alerts) by more than 20 percent. Further, the company was on track to reduce capacity dedicated to administrative IT by another 20 to 30 percent and improve system stability by 30 to 50 percent over the following six months.

2. Measure the things that create value

You are what you measure. That old adage still applies, and it is one of the keys to improving how IT works. IT collects an overwhelming volume of data and metrics but often struggles to use them to drive business value. For example, the common metrics of product-delivery time and budget encourage teams to release products quickly and under budget. There's nothing wrong with that, of course, except that it can mask a very real issue: a product could perform well against these metrics but still be a bad

Exhibit 2

An agile operating model can reduce IT administration.

Head count focused on administrative IT

Application operations

Infrastructure

Starting point	6 months (interim state)	18 months

- Well-defined, business-oriented services with high visibility into incoming demand
- Small, self-sufficient teams with end-to-end ownership for each service being provided
- OKR[1]-based self-governance of each team for improvements

- Root-cause elimination of recurring incidents
- Self-service for most common requests
- Proactive monitoring, predictive maintenance, and self-healing solutions for next level of improvements

[1] Objectives and key results.

product that demands lots of time to fix its defects or maintain it.

IT leaders need instead to measure the performance and health of the organization based on the desired outcomes. In the case of the financial services company's application-operations team, elimination of reactive demand was the desired outcome, and percentage of false alerts was a key metric. The best metrics not only show progress but also are specific and useful enough to be tracked every day, easy to measure, and highlight what changes are needed. YouTube, for example, realized that the amount of time people viewed a video (viewed hours) was the

most important determinant of increasing revenue, so it focused all activities on improving that metric.[1] The right metrics can also be measured at the squad, tribe, and organizational level, which allows for higher levels of self-governance through objectives and key results (OKRs) while providing the transparency that leadership needs (Exhibit 3).[2]

3. Harness market dynamics to develop 'IT for IT' solutions and drive their adoption

There are typically multiple improvement opportunities that cut across many teams or products in IT—for example, a platform for the creation of application programming interfaces

---

[1] John Doerr, *Measure What Matters: How Google, Bono, and the Gates Foundation Rock the World with OKRs*, New York: Penguin, 2018.
[2] For a good introduction to OKRs, see John Doerr, *Measure What Matters*.

Exhibit 3

Use the right metrics to measure what matters.

	Key question(s) being addressed	Likely top-level metric(s)
Business relevance	• Are the stories/features being worked on by IT considered "business relevant" or "market differentiating"?	• Percentage and volume of stories/features that are considered "market differentiating" by the business
Flexibility	• How flexible is IT in changing directions with changes in the market/business needs?	• Percentage and volume of stories that can be deployed into production standalone
Technology debt	• How much technology debt (currency, defects, etc) can be a business risk or preclude IT from working on business-relevant stories/features?	• Indexed technology debt of the applications underlying a service/product, eg, — Currency of the technology stack — Defect backlog
Customer satisfaction	• How satisfied are the business users/owners with the stories/features being delivered?	• One-click surveys to the business users/owners after deploying story/feature
Team-member engagement	• How excited are the team members (employees or contractors) to be part of the team?	• Anonymized pulse survey conducted at the team level

(APIs). These "IT for IT" solutions can help teams work more efficiently and effectively by standardizing processes and making code easy to reuse, for example. However, one of the big issues contributing to IT administrative bloat is that these sorts of IT-for-IT solutions often end up languishing unused. Not only are resources tied up in developing them, but further work is often needed because they don't work as expected.

At one insurance company, this became a glaring issue. The API enablement team had done what it was asked to do: establish an API platform to

let developers build new APIs more efficiently. Yet after investing in the platform, fewer than 100 APIs had been created on it, and worse, fewer than ten of those had been referenced more than five times—and this was in an organization of 500 developers. Why weren't they using the platform? It turned out that it was just too difficult to use. Developers had to submit a manual request, which took a week to fulfill, so they found it easier to just write new code.

A better solution relies more on market-demand mechanisms. Agile teams create demand for tools and solutions they need to help hit their OKRs. As

developers spot these needs, they propose a solution (such as developing a platform for API development or a portal for developers to find existing code) to meet the demand, which is quickly reviewed and funded (or rejected) by an oversight team. If approved, an enablement team is formed, made up of people with the right skills. IT organizations provide incentives for enablement teams to form, such as bonuses and recognition. The key difference, however, is that enablement teams have specific OKRs for not just delivering the product but showing that it works and is adopted. Developed tools and solutions

need to solve the problem, be easy to use, and easily deployed (Exhibit 4).

We have found that a venture-capital (VC) funding model, in which IT leadership acts as the venture capitalist, works well to fund IT-for-IT solutions. In this system, anyone in the IT organization can submit an idea for creating a new enablement team; if an idea is deemed attractive, IT leadership provides seed funding and sets OKRs. Quarterly assessments show progress, and leadership decides whether to allocate another round of funding to that enablement team and what OKRs to pursue next (Exhibit 5).

Exhibit 4

Enablement teams can be set up to design and drive the adoption of solutions common for multiple agile squads.

Typical goals for an enablement team

- Lay out the strategy, design, and impact of the technology innovation

- Create guardrails and tool kits ("backpack") needed by the other IT teams to adopt the technology

- Act as evangelists, promoting the solutions to other teams

- Self-govern the enablement team through OKRs focused on adoption of the technology

Illustrative example: API enablement team

Rationale for setting up the API team

APIs (and their reuse) free up developer capacity to focus more on new, market-differentiating features; in addition, reuse reduces the potential for rework

Elements of API solution	Evangelism with other teams
1. Self-service platform to create APIs 2. Portal to search for existing APIs	1. "Dojo" sessions with teams to learn and launch 2. Community channels for cross-learning and celebrating success 3. Connecting with other enablement teams (eg, APIs in cloud)

Metrics for measuring success and driving OKRs

1. Number of (static) references per API

Exhibit 5

A VC-style funding mechanism ensures that enablement teams' OKRs are aligned with the goal—to flip the ratio.
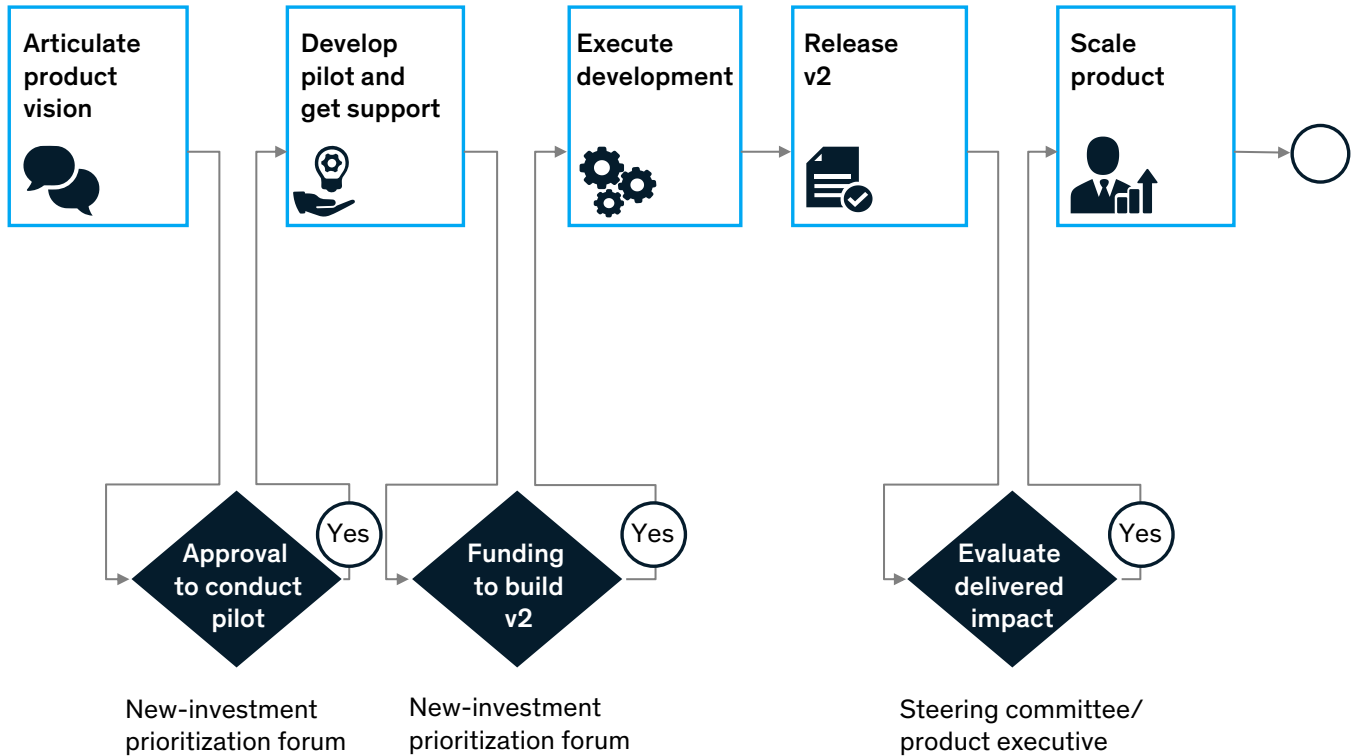
In this model, the company's executive committee acts as investors in a VC fund, so IT leadership goes to them annually (or more often, depending on the need) to demonstrate impact from the enablement teams and request VC funds for the next year. The effect is to force the teams in the tribe to behave like start-ups, moving quickly to demonstrate the value of their work.

4. Stay focused on driving the program
As in any transformation, time is the enemy. After an initial set of wins, progress often bogs down because teams run into problems, issues become more complex, or leadership simply loses interest. Without firm leadership and guidance, the full

value potential of the resource allocation isn't met, or—worse—the organization slides back to the old way of working. But too much leadership control stifles enthusiasm and the sense of autonomy that's necessary for teams to be successful.

We have found that a thoughtful and disciplined quarterly IT review (QIR) process can be helpful (Exhibit 6). Similar to the quarterly business review at most highly mature, agile organizations, the QIR process allows IT leaders to take stock of the progress, resolve issues, reallocate budgets as needed, and provide guidance on the next quarter's priorities for pushing forward to flip the ratio. For their part, each agile squad/tribe assesses its

Exhibit 6

A quarterly IT review governs the journey to flip the ratio.
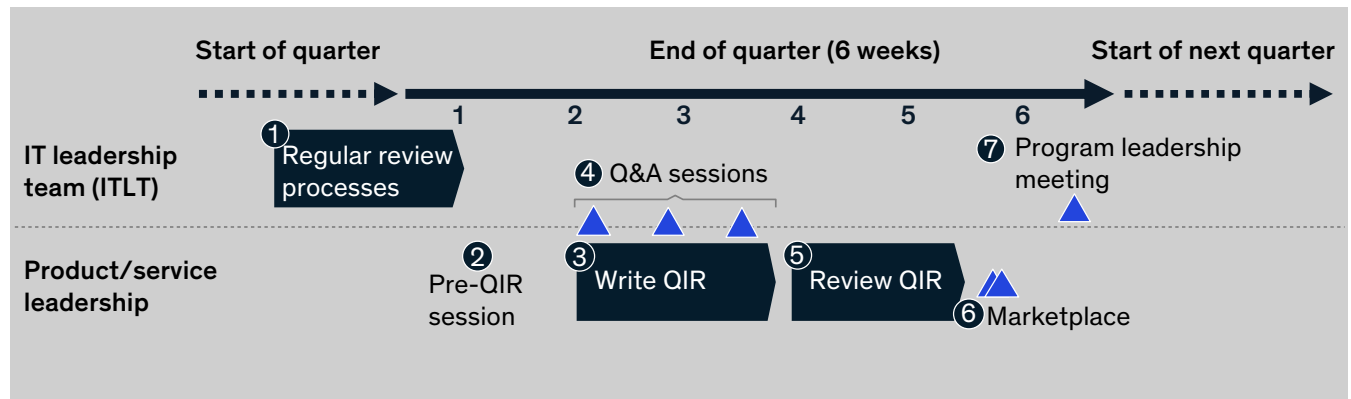
① ITLT, with support from the executive committee, sets the budget for enabling on a yearly basis and adapts quarterly within the QIR.

② ITLT sets what needs to be accomplished next quarter by providing tribe leads with priorities.

③ Tribe leads draft and publish a 5–10 page QIR memo, which includes a retrospective of prvious quarter as well as the OKRs for the next quarter.

④ Q&A sessions with ITLT are set up to provide tribe leads the opportunity to receive extra guidance on their objectives, road map, or impediments.

⑤ Tribe leaders read and comment on the QIR memo drafts of other tribe leaders.

⑥ A 1-day QIR marketplace event resolves dependencies and finalizes QIR memos.

⑦ A joint meeting with ITLT and tribe leaders resolves constraints/dependencies and validates that the current budget (resource) level is adequate.

progress on its top-level metrics, sets aspirational OKRs for the next quarter, and submits them to their peers and leadership for review.

To be sure, flipping the ratio is not easy. But if IT organizations want to help build business value, they can only do so if their resources are allocated to value-creating activities.

This article was originally published on McKinsey.com in August 2019.

Nagendra Bommadevara is a partner in McKinsey's New York office, **Steve Jansen** is an associate partner in the Charlotte office, **Lauren Klak** is an associate partner in the Cleveland office, and **Maneesh Subherwal** is an associate partner in the New Jersey office.

Cloud adoption to accelerate IT modernization

The cloud is a means, not an end. Success in modernizing IT through the cloud is driven by a complete standardization and automation strategy.

by Nagendra Bommadevara, Andrea Del Miglio, and Steve Jansen

Cloud-computing adoption has been increasing rapidly, with cloud-specific spending expected to grow at more than six times the rate of general IT spending through 2020.[1] While large organizations have successfully implemented specific software-as-a-service (SaaS) solutions or adopted a cloud-first strategy for new systems, many are struggling to get the full value of moving the bulk of their enterprise systems to the cloud.

This is because companies tend to fall into the trap of confusing simply moving IT systems to the cloud with the transformational strategy needed to get the full value of the cloud. Just taking legacy applications and moving them to the cloud—"lift-and-shift"—will not automatically yield the benefits that cloud infrastructure and systems can provide. In fact, in some cases, that approach can result in IT architectures that are more complex, cumbersome, and costly than before.

The full value of cloud comes from approaching these options not as one-off tactical decisions but as part of a comprehensive strategy to pursue digital transformation. Such a strategy is enabled by the standardization and automation of the IT environment through an open API model, adopting a modern security posture, working in an automated agile operating model, and leveraging new capabilities to drive innovative business solutions. While cloud is not a prerequisite for any of these features, it does act as a force multiplier. Companies that view cloud capabilities in this way can create a next-generation IT capable of enabling business growth and innovation in the rapidly evolving digital era.

Lift-and-shift is not enough

Cloud services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud appeal to many organizations because of their stated features: pay-per-use, ability to scale up or down based on usage, high resilience, self-service, and so on. All these benefits are expected to lead to much lower IT costs, faster time-to-market and better service quality compared with traditional IT offerings.

However, traditional enterprises run into two major issues when moving to cloud:

— The existing business applications were created using the traditional IT paradigm. As a result, these applications are typically monolithic and configured for fixed/static capacity in a few data centers. Simply moving them to the cloud will not magically endow them with all the dynamic features of the cloud.

— The typical technology workforce of an enterprise is well versed in developing business applications in the traditional IT framework. Most of them need to be reskilled or upskilled for the cloud environment.

IT security is a good example. Most traditional IT environments adopt a perimeter-based "castles and moats" approach to security, whereas cloud environments are more like modern hotels, where a key card allows access to certain floors and rooms. Unless the legacy applications that have been developed and deployed for a castles-and-moats security model are reconfigured for the new security model, migrating to the cloud may have an adverse impact on cybersecurity.[2]

Enterprises have been successful in adopting SaaS solutions mainly because SaaS addresses these constraints in a simple fashion: they replace the existing business applications and leave the development of new features to the SaaS provider. SaaS solutions have therefore become very popular for business functions such as marketing and sales, back office (HR), and communication and collaboration. However, in most sectors, there are no mature SaaS solutions for core business functions such as billing for the utilities sector and core/online banking for financial services.

As a result, despite overall increased cloud investment, enterprise cloud adoption is maturing slowly.[3] Many enterprises are stuck supporting

---

[1] IDC, "The Salesforce economy," September 2016, salesforce.com.
[2] "Benchmark your enterprise cloud adoption," Forrester, January 3, 2017, reprints.forrester.com.
[3] The overall cloud security model is more complicated than the above analogy—we are simply making the point on why lift-and-shift is not likely a good strategy for cloud adoption.

both their inefficient traditional data-center environments and inadequately planned cloud implementations that may not be as easy to manage or as affordable as they imagined. While some forward-thinking companies have been able to pursue advanced enterprise cloud implementations, the average enterprise has achieved less than 20 percent public or private cloud adoption (Exhibit 1).

Benefits of automating IT processes through the cloud

Historically, enterprise business applications have been designed to run on custom-configured IT systems, each application requiring its own heavily customized configuration of computer storage and network resources. As a result, IT needed armies of administrators just to keep systems updated and running, to manually add new capacity when demand is high, or apply quick fixes for issues such as low performance. As the number of IT solutions has increased, so has the overhead necessary for testing, integration, and maintenance. In a typical enterprise, just a fraction of IT personnel is focused on designing and developing the market-differentiating solutions the business cares about; the rest are working simply to keep the lights on.

Standardizing system configurations and automating IT support processes can reverse that ratio. By enabling enterprises to better manage their infrastructures, companies can not only save on costs but also shorten times to market and improve service levels.

Exhibit 1

Cloud adoption has matured at varying rates.

● Fin services ● Insurance ● Healthcare ○ Other

% of server images deployed in private or public cloud

Bubble size represents volume of server images

Median adoption rate is 19%

Virtualization+   Basic Cloud   Advanced Cloud

Maturity of cloud capabilities
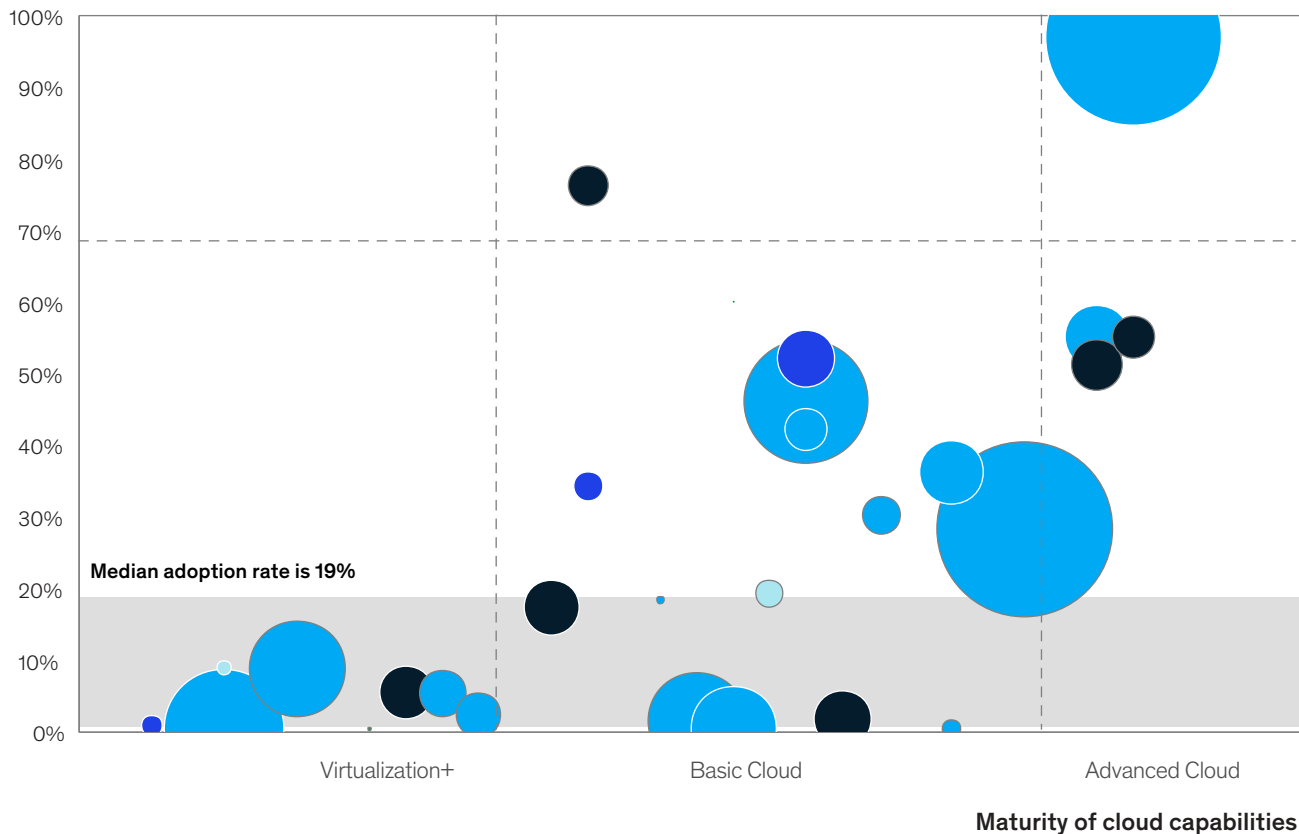
Adopting the cloud is a massive enabler of the necessary standardization and automation. With the cloud, companies can:

— Reduce IT overhead costs by 30 to 40 percent

— Help scale IT processes up and down as needed, optimizing IT asset usage

— Improve the overall flexibility of IT in meeting business needs such as more frequent releases of business features; cloud providers are increasingly offering much more sophisticated solutions than basic computing and storage, such as big-data and machine-learning services

— Increase the quality of service through the "self-healing" nature of the standard solutions (for example, automatically allocating more storage to a database); we have seen enterprises reduce IT incidents by 70 percent by using cloud computing as an opportunity to rethink their IT operations

Capturing these benefits from cloud adoption requires more than just lift-and-shift when the business-application system configurations are heavily customized and IT processes are mostly manual. It requires a certain level of remediation to make IT systems more cloud-oriented.

Netflix is one of the most public examples of this kind of commitment to and investment in cloud-enabled, next-generation infrastructure. It spent seven years on its transformation, adopting a cloud-native approach, rebuilding all its technology, and restructuring the way it operated. It employed application program interfaces (APIs) to reduce its monolithic legacy applications into smaller components, make them more flexible, and then move them to AWS. As a result, service availability has increased, nearing the company's stated goal of 99.99 percent of uptime. And Netflix has seen IT costs for streaming fall to a fraction of what they were in its own data center.

Recently, many established companies have made aggressive moves to adopt public cloud solutions. Capital One is running the bank's mobile app on AWS; GE Oil & Gas is migrating most of its computing and storage capacity to the public cloud; Maersk is migrating its legacy systems to reduce cost and operational risk while enabling advanced analytics to streamline operations.

Pioneer organizations are also actively seeking ways to leverage the new services on cloud to create innovative business solutions. Progressive Insurance deployed its Flo chatbot on public cloud; NASCAR is leveraging machine-learning solutions on cloud to analyze real-time and historical race car data to improve performance and simulate scenarios.

Even "born digital" companies that initially chose, for strategic reasons, to have their own IT infrastructure and systems are now opting to move to cloud to leverage the scalability and the higher order functionality it offers. Spotify is a prime example.

How to approach the cloud transformation

Fully embracing cloud can have a significant upside but also requires substantial upfront investments in what is often a multiyear journey. For this reason, an all-in transformation approach needs active commitment and a clear mandate from the CEO and board over the long term (see sidebar, "A tale of all-in transformation").

Specifically, there are four key topics companies should address for successful cloud adoption at scale:

1. *Decide on sourcing.* It's difficult for most companies to build their own cloud technology stack and even harder to maintain it. Partnering with public cloud providers to build and manage the cloud stack is the more typical approach. In most cases, the pragmatic way to start is with a single cloud service provider while adopting the necessary guiding principles to avoid being locked into one provider. After achieving a certain scale and level of maturity—in our experience, a good rule of thumb is to plan for an annual run rate of $30 million with the primary cloud service provider—an enterprise can explore a second or third service provider for scaling up.

A tale of an all-in transformation

A Fortune 100 company with a $2.2 billion annual IT spend ($800 million on infrastructure costs alone), was struggling with the cost and complexity of its legacy IT environment. Its IT department was supporting 8,000 applications (including 150 instances of SAP) and 20,000 workloads. Not surprisingly, provisioning was slow. It took more than 45 days to set up a server, and the company knew this was not sustainable.

Consequently, the company invested more than $200 million in aggressive digital transformation. It was a significant effort, but the company achieved a return on its investment in less than four years.

The company first defined its cloud sourcing strategy, grounding it in an aggressive move to a hybrid (public and private) cloud model as public cloud options were still maturing in late 2013. It opted for a single strategic partner for each cloud and recently added a second public cloud partner. It then created a cloud operating model, setting up a new 100-person team working within an agile operations framework.

Then, beginning in 2015, the company began its legacy-remediation work, moving all its applications to a private cloud, heavily incentivizing its application teams. It took an opportunistic approach to upskilling IT: every application team that wanted to use cloud had to go through an in-house training program.

Within the first six months, the company had moved its complex SAP environment to private cloud and adopted a cloud-first policy for all new applications. It replaced expensive colocated contracts and moved its systems to a software-defined data center.

Less than three years in, the company has moved more than 2,000 workloads and two petabytes of data to the public cloud. The company reduced costs by $90 million at the two-year mark and is on track to cut another $60 million. Automation also significantly improved performance and agility. With the transformation on track to completion in 2018, the company is now one of the largest enterprises operating on cloud.

2. *Create a public-cloud operating model.* Unlike traditional operating models, the public cloud requires IT to manage infrastructure as code. This requires software engineers who understand the compute, storage, and security protocols of public cloud (as opposed to network engineers or system administrators). For most enterprises, this translates to a massive upskilling of the infrastructure organization and the operating model in which they work. Specific teams need to be assigned to configure and manage the production environment.

3. *Legacy-application remediation.* Existing applications will need to be refactored at the infrastructure and application layers to align with the security and capacity requirements of the public cloud. Security must be baked into these applications, and they must work in a more automated fashion. This requires significant attention from application teams, which can be hard to get.

Companies can address this hurdle by creating a clear business case for legacy-application modernization, aligning the migration schedule with major application upgrades or replacements, and adopting foundational solutions (such as API frameworks) to make the remediation easier.

4. *Cultivating the right skills.* Professionals must be able to develop applications on the cloud (specifically on the vendor's system) securely and quickly. To do this, companies will need to hire and train cloud experts and then introduce them into development teams, retrain or upskill the existing workforce, and set up digital-innovation labs as needed with an emphasis on cloud development.

This aggressive approach relies on true commitment from leadership in the form of money (one financial-services business is investing $300 million in a cloud transformation) and time (these programs can take two to three years). That's because, in executing a cloud transformation, multiple things need to happen at the same time. In many cases, for example, a core group of cloud engineers preps for the cloud migration by setting up the cloud environment, hardening it, looking at applications to move, and creating tools for migration. Meanwhile, the main IT team is being trained in how to work in an agile way. This approach has significant management challenges, but with strong leadership, it's the fastest path to transformation.

Many enterprises, however, are not yet ready to take the full plunge into cloud, perhaps because organizational buy-in is lacking, or there is a reluctance to invest the required resources in a multiyear effort, or in some cases due to regulatory constraints. These organizations can achieve significant benefits in the short-to-medium term, albeit on a smaller scale, by adopting the cloud's agile and automated operating model within their traditional IT. This approach builds important organizational capabilities and prepares the business for a cloud transformation when it is ready.

Companies have eagerly adopted agile methods for application development and are actively pursuing automation/DevOps (such as continuous integration and continuous delivery), but the same approach can have an even greater impact on IT operations and infrastructure. By organizing the infrastructure function into tribes of small cross-functional, self-directed squads with product owners to prioritize work and scrum masters responsible for removing barriers, IT can prioritize work in ways that increase productivity, quality, and speed. In addition, the continuous automation program, over time, can further infuse cloudlike capabilities into traditional IT, such as APIs for interactions between developers and infrastructure (Exhibit 2).

With the goal of improving service levels and reducing costs, one major life insurance company adopted an agile approach within its 250-person IT operations groups. The company began by assessing the state of its current infrastructure—its

core processes, organizational model, metrics and KPIs, and historical demand—and developed a hypothesis about what it might achieve with a more agile approach. It created a leadership program appropriate to agile methods, adopted the necessary tools, and conducted an agile-for-infrastructure boot camp for stakeholders.

Within six weeks, the IT infrastructure group started planning for ongoing projects, conducted training sessions for senior leaders and infrastructure teams, and set a goal for what ongoing operations should look like. It fully leveraged scrum methodology for planned work such as projects, and Kanban, a methodology for managing the creation of products emphasizing continual delivery, for unplanned work such as incidents and service requests. By the end of the second month, the company had achieved the operational model it envisioned and was able to begin designing service-management processes and launching automation initiatives.

It completed the initial transformation in six months, cutting IT costs by more than 35 percent and doubling productivity. The insurer plans to automate up to 80 percent of its operations work, driving costs down even further and significantly improving its service levels. Today, it is well positioned to move more aggressively to the cloud in the future.

The rules of the cloud game

There are many actions enterprises can take that have proved valuable to early adopters of cloud-enabled next-generation infrastructure. These include, but are not limited to:

— *Evaluating the current IT portfolio.* Before beginning any cloud development or migration, take a dispassionate look at the existing IT portfolio to determine what is suited for public cloud platforms or SaaS alternatives.

— *Choosing your transformation approach.* Involve all key stakeholders in determining whether your enterprise will be an aggressive or opportunistic transformer.

— *Articulating IT and business goals.* Create a well-defined set of outcome-oriented

Exhibit 2

The agile/DevOps operating model is proving to be even more applicable in infrastructure than in application development.

Projects (internal and external), audit, patching, non-standard requests, etc

Planned demand

Agile squads (scrum)

Incoming work for a product/service

Story pointing and understanding of incoming demand allows for data-informed:

- Productivity improvements
- Automation investments
- Understanding of demand drivers

Automation and DevOps

When systems are stable and operations work is mostly automated, a DevOps style of operating model can be implemented (single team owning both the planned and unplanned demand for a given product/service)

Unplanned demand

Incidents, service requests, changes and housekeeping work (eg, log reviews)

Operation teams (Kanban)

aspirations for both the short and long term in line with your approach.

— *Securing buy-in.* Ensure commitment and investment from senior management, particularly finance leaders, who must support the transfer from capital to operations and maintenance investments/accounting.

— *Addressing change management.* A heavily automated agile operating model will require significant shifts in IT behaviors and mindsets. Invest in both change management and

the development of cross-functional skills across infrastructure, security, and application environments.

— *Adopting new KPIs.* Measure and reward your technology team for standardization and automation rather than, say, for availability.

By viewing cloud computing as a starting point for IT automation, companies may be able to have it all: scalability, agility, flexibility, efficiency, and cost savings. But that's only possible by building up both automation and cloud capabilities.

Unlocking business acceleration in a hybrid cloud world

Companies that have moved operations to the cloud still are not achieving the desired operational agility. A renewed focus on people, processes, and policies can unlock the cloud's full potential.

by Arul Elumalai and Roger Roberts

Abstract

Across industries, CEOs share a top priority: harness technology to jump-start growth, accelerate time to market, and foster innovation. Chief information officers (CIOs) recognize that the C-suite depends on them to achieve growth and meet rising expectations for agility. They increasingly view IT modernization—including migrating to the cloud, adopting new application architectures, and building on cloud-native services—as a way to sustain these goals. To date, however, most companies have not captured the anticipated agility benefits because a number of challenges hinder technology leaders as they push ahead with modernization initiatives. While many of these challenges are valid, we also find some are false trade-offs that can be avoided.

CIOs need to promote the transformation mindset of focusing on differentiated business value by adopting agile processes, automating policies, and upskilling talent across the entire organization. They need to look beyond technology to change the way their IT organization operates across three foundational elements: people, processes, and policies. Priorities include upskilling existing talent and creating new roles (such as site reliability engineers, full-stack engineers, and data scientists), revamping procedures by adopting agile development processes with security integrated into every step, and enforcing policies through automation. The research delves into the practices of leaders versus that of laggards and distills the key "unlocks" that can help organizations move to higher levels of business agility as they pursue increased cloud adoption.

McKinsey & Company has published this report based on its independent research. McKinsey does not endorse any technology vendor, product, or service.

Digital technologies continue to transform every facet of business. Across industries, CEOs have a consistent top priority—harness technology to jump-start growth, speed time to market, and foster innovation. Several factors are ratcheting up pressure: investors are valuing top-line revenue growth; rising customer expectations for simple cross-channel experiences are compelling companies to systematically tear down silos; and an organization's ability to respond to market shifts is becoming a core differentiator. Meanwhile, digital leaders across sectors have changed the competitive landscape by demonstrating that agility and velocity can beat scale.

Senior technology leaders are feeling this pressure. In recent McKinsey research, when chief information officers (CIOs) or equivalent tech leaders were asked about their CEO's top priorities (see sidebar, "About the research"), 71 percent pointed to agility in reacting to changing customer needs and faster time to market, while 88 percent of respondents cited revenue acceleration (Exhibit 1).

These priorities are playing out across every industry, with huge implications for business models.

— A clothing company, for example, traditionally had several weeks between the introduction of a new product line in stores and when competitors could get their cheaper versions to market. That cushion has dropped significantly thanks to digital channels: the company indicates that it now has just 48 hours to launch a new design and gain buyers through digital, direct-to-consumer routes, and rapid (sometimes same-day) delivery.

— A digital-media company regularly saw spikes in viewership upon releasing new content, so its need to ramp up infrastructure in order to accommodate increases in demand has suddenly become critical to satisfy its subscribers.

— In financial services, a line-of-business leader at a large retail bank cited tremendous pressure

Exhibit 1

To stay relevant and ahead of the competition, CEOs across industries are prioritizing growth and speed of innovation over cost.

"What would you say are the top 3 priorities for your CEO?"
Chief information officers who mentioned this as a top 3 CEO priority, %

CEO priorities

Revenue acceleration	88
Improved agility and faster time to market	71
Cost reduction	47
Better management of regulatory and compliance risks	29
Increased customer satisfaction	29
Other (eg, brand reputation, other financial goals, strategic initiatives)	41
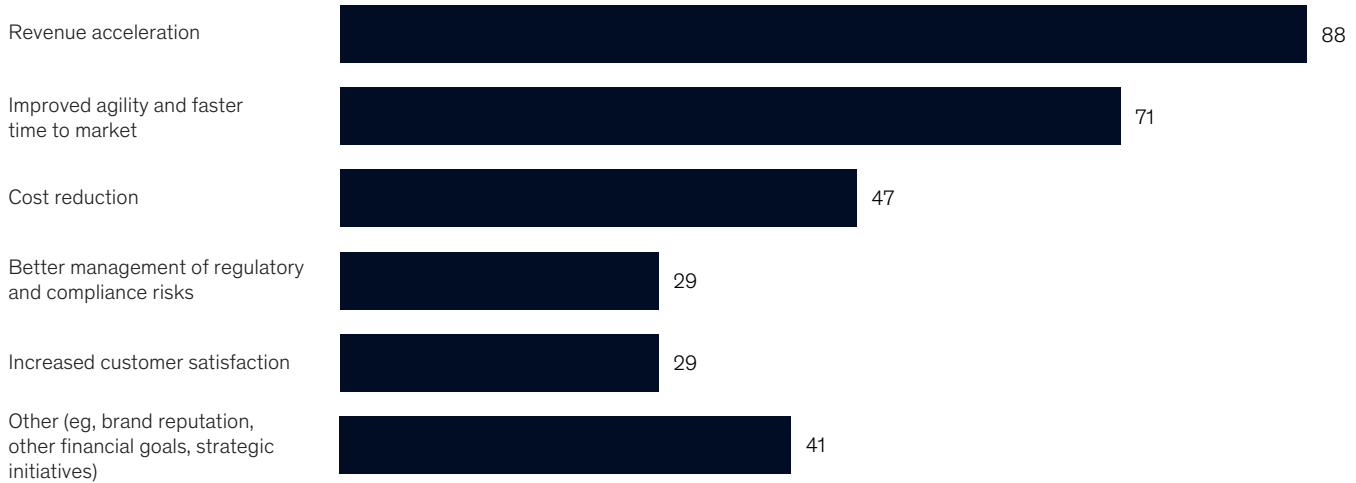
Source: McKinsey expert interviews (N = 52)

to shorten product-development cycles. The industry's average product release time has ranged from nine to 24 months—a glacial pace compared with that of fintech companies, which can deploy code daily and run dozens of A/B tests a month.

The common thread running through these examples is the ongoing, urgent need to gain market advantage through business acceleration.

Role of digital and the ever-increasing reliance on technology leaders

IT strategy has long been part of business strategy, but C-suite executives (CxOs) are increasingly seeking a larger impact from investments in digital technologies. Digital innovation has become central to the full range of business transformation initiatives and is no longer just one category among many. Since technology is integral to a company's performance and competitiveness, identifying prudent investments in IT modernization becomes

even more critical. CEOs recognize the importance of getting it right: good choices establish a favorable course, and the business soars; however, poor choices will siphon away much-needed organizational energy and resources and undermine competitiveness.

The task of translating ambitious tech-driven strategies into accelerated performance falls to CIOs and chief technology officers (CTOs). Nearly 60 percent of CIOs indicated that their CEO depends on them to achieve the organization's top three business priorities (Exhibit 2).

As a CTO at a large US insurance company points out, "I think all CEO priorities depend on the office of the CTO. It is all about bringing products to market faster. We have to innovate on new policies and change our business model rapidly." And the CIO of a retailer indicates that the IT team is mutually accountable with the chief marketing officer (CMO) to achieve the growth objective: "The CIO and CMO

About the research

To gain a better understanding of the challenges organizations face in modernizing their IT infrastructure, McKinsey conducted in-depth interviews with the tech leaders (chief information and technology officers) at 52 enterprises in the spring of 2019. The sample studied companies from 17 industries with global operations. Of respondents, 78 percent work at organizations with at least 5,000 employees, and 44 percent work at companies with annual revenues in excess of $10 billion.

Exhibit 2

IT leaders clearly realize CxOs' dependence on them to deliver on growth priorities and agility expectations.

"Which of the top 3 CxO priorities depend on you?"
CIOs who indicated that at least 2 of CxOs' top 3 priorities depend on them, %

	None	One	Two	Three
	0	6	35	59
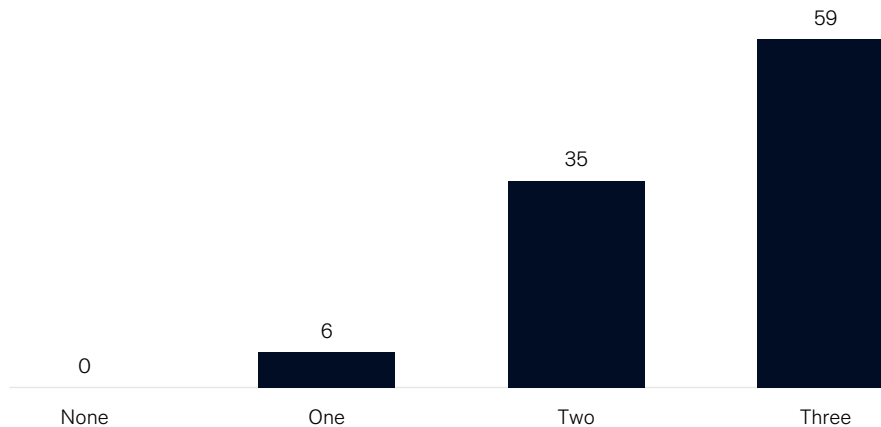
Source: McKinsey expert interviews (N = 52)

will have to work together. We have common metrics to track. If a campaign fails, both of us are on the hook. So to say that the CMO is dependent on me to deliver the objectives is an understatement. It's our joint responsibility."

The IT infrastructure modernization imperative

To meet CxO and board expectations, IT modern-ization is critical. According to our research, CIOs believe that the organization cannot capture agility benefits by simply shifting applications to cloud platforms. Instead, they recognize the need to reassess the infrastructure stack and the way it works.

Emphasizing agility while managing cost and risk
When asked about the principal benefits of infrastructure modernization, CIOs prioritize increased agility and better quality of service to customers. They are also looking to reduce costs and improve their security posture (Exhibit 3).

CIOs see the cloud as a predominant enabler of IT architecture and its modernization. They are increasingly migrating workloads and redirecting

Exhibit 3

CIOs believe that business benefits cannot be achieved by lifting and shifting applications and need to rethink the infrastructure stack.

CIO reasons for pursuing infrastructure modernization
100 points allocated across

Agility and time to market	28
Quality of services or reliability	27
Cost efficiency	20
Security and risk reduction	19
Other (eg, employee satisfaction, talent retention)	6
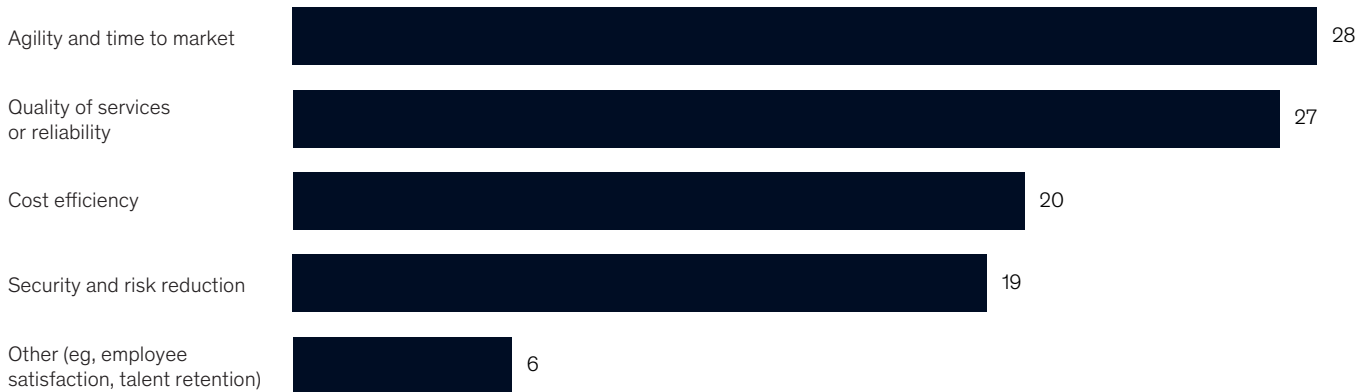
Source: McKinsey expert interviews (N = 52)

a greater share of their infrastructure spending to the cloud. The companies we surveyed currently have around 50 percent of all workloads running on public- and private-cloud platforms. By 2022, that share is projected to rise to 75 percent, with roughly two-thirds of that workload housed in shared public platforms within data centers built out by the major cloud-service providers (Exhibit 4).

While this migration represents a dramatic technology overhaul, astute tech executives also view it as a trigger to reevaluate how the IT function works. One large retail chain's CIO notes, "I need a forcing device to jolt my organization out of its old ways of working. I see cloud as that catalyst. Our current tools enable the old ways, not the new. Until we implement the tools and data, we can't reap the full benefits."

Identifying key challenges

Thus far, modernization efforts have largely failed to generate the expected benefits. Despite migrating a portion of workloads to the cloud, around 80 percent of CIOs report that they have not attained the level of agility and business benefits that they sought through modernization. Further

analysis indicates that companies are falling short of their IT agility expectations, regardless of their level of cloud migration (Exhibit 5). Even organizations that have transitioned the majority of workloads to the cloud remain within the same range of IT agility as their slower-moving counterparts.

Our research found that CIOs face several entrenched challenges when pursuing IT modernization: survey respondents indicated talent gaps were their top barrier, followed by security and compliance requirements (Exhibit 6).

The CIO of an automaker reflects on the struggle of hiring candidates with the requisite cloud expertise: "Finding someone with skills similar to engineers who are attracted by large cloud providers and software as a service (SaaS) companies is too difficult."

Notably, 28 percent of respondents cited the complexity of their current environment. The technology leader in financial services notes, "We were surprised by the hidden complexity, dependencies and hard-coding of legacy applications, and slow migration speed." Thus, it becomes critical for many applications

Exhibit 4

CIOs see cloud as crucial to modernizing technology and are increasingly migrating workloads to cloud.

Workloads distribution in 2019 vs in 2022
% of workloads

Legend: ■ Public cloud ■ Private cloud ■ On premise ⊗ % respondents

Left chart (2019 → 2022):
- 2019: 26 Public cloud, 25 Private cloud, 49 On premise
- 2022: 52 Public cloud, 23 Private cloud, 25 On premise

Increase in cloud workloads within 3 years

≥ 2x, < 35 (25% respondents):
- 2019: 16, 6, 78
- 2022: 47, 18, 35

≥ 2x, ≥ 35 (10% respondents):
- 2019: 28, 12, 60
- 2022: 63, 22, 15

< 2x, < 35 (10% respondents):
- 2019: 15, 9, 76
- 2022: 21, 13, 66

< 2x, ≥ 35 (55% respondents):
- 2019: 33, 38, 29
- 2022: 58, 28, 14

% of workloads currently in cloud

Source: McKinsey expert interviews (N = 52)

---

to refactor for modern architecture. This approach—characterized by microservices and containerization—enables companies to balance the projected cost to run against cost to modernize, focus on the pace of innovation and enhancements, and improve responsiveness to fast-changing needs and dynamic markets. We have seen CEOs seek this guidance from their IT leaders and teams.

Managing trade-offs on the IT modernization journey

The inability of CIOs to achieve greater agility is in part due to valid constraints (such as gaps in skills and training), but our research finds that avoidable compromises also hinder progress. Few organizations have the luxury of starting with a clean-sheet approach to IT infrastructure, and so CIOs are making trade-offs in the name of balancing the ideal with the practical. Our analysis identified five common compromises that IT leaders feel they are frequently forced into and that negatively affect agility (Exhibit 7). Furthermore,

some CIOs debate whether such compromises are valid or not. Some say these responses reflect real constraints, while others say that adopting new technology and operating-model innovations can easily address these constraints—hence, these are not trade-offs at all.

While a majority of CIOs indicate that they are living with these suboptimal choices, deeper analysis of companies that have successfully navigated these trade-offs highlights best practices to avoid these compromises and, in turn, increase business agility.

Giving up developer agility for the sake of control and governance. One of the top benefits of transitioning operations from legacy infrastructure to cloud-native solutions is the speed at which developers can work. However, 69 percent of organizations indicate that implementing stringent security guidelines and code review processes can slow developers significantly. According to the chief information security officer of a multinational

Exhibit 5

Analysis indicates that companies are falling short of their IT agility expectations, irrespective of migration level to cloud.

Companies with interviewed CIO, bubble size based on revenue

IT agility index[1] (achieved)

% of workloads in public- and private-cloud platforms
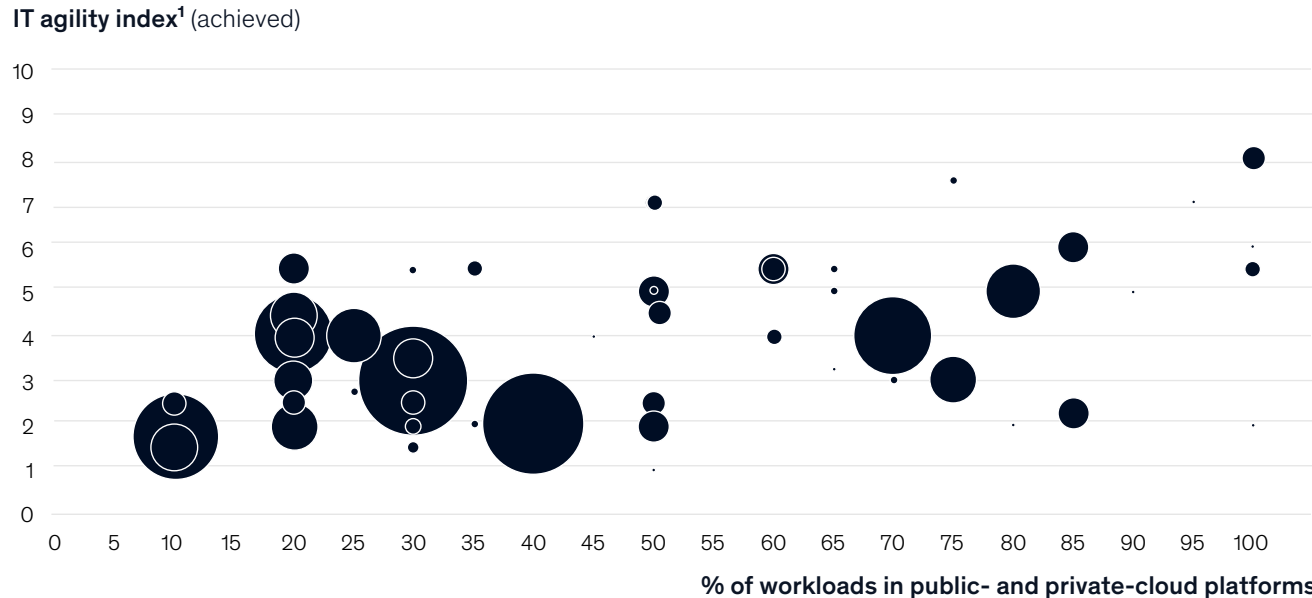
[1] Parameters used to calculate IT agility score are the following, self-reported and rated on a scale of zero to ten: speed of application and feature development, maturity of IT operations automation, and agile application-development capabilities.

cloud-based solutions provider, "In the old world, when a developer checks in bad code, I can find it and control the blast radius. But in cloud, it happens too fast—I still have those codes go through manual reviews and sign-offs." Some leaders have found a way to work around this compromise through the following approaches:

— *Acquiring and upgrading talent.* Leading companies hire developers with security architecture expertise and entrust them to design secure architectures from a project's inception.

— *Provisioning process improvements.* DevOps engineers use application programming interfaces (APIs) for environment creation, which include functions that specify secure configuration.

— *Changing development processes.* By bringing security teams more deeply into agile development and DevOps processes, companies have avoided the added complexity of cross-

team coordination and alignment across development and security teams.

— *Investing in toolchain and technology.* CIOs are integrating the right set of DevOps toolchains that can automate security policies.

— *Automating code reviews.* Security-code scanners are used to conduct automated code reviews for common vulnerability.

— *Automating test suites for code elevation.* Development teams are investing in test-driven development, and test suites are foundational to automate the elevation of code from development to test, sandbox, and production environments.

— *Implementing developer self-service.* Standardizing the service catalog for infrastructure, implementing cost guardrails, and enabling self-service can speed infrastructure procurement approval processes for developers.

Exhibit 6

CIOs' inability to deliver on agility objectives is due to valid constraints and challenges.

Top challenges CIOs are facing in infrastructure modernization
CIOs who indicated this as a challenge, %

Challenge	Value
Talent gaps (incl technical and managerial talent)	58
Security requirements and compliance constraints	52
Change management and implementation complications	33
Gaps in executives' understanding of cloud capabilities and value at stake	32
Complexity of current environment	28
High or unforeseen costs	25
Operating-model transformation complications	19

CIOs' progress is hindered by these challenges and resulting compromises. In most cases, modernization efforts run out of steam and CIOs stop pursuing the next set of progress objectives.

Source: McKinsey expert interviews (N = 52)

Exhibit 7

Some cases of compromise prove to be avoidable, according to CIOs' assessments.

■ Real trade-off ■ Contrived

Interviewees' assessment of the compromises
% of CIOs

Trading . . .	In favor of . . .	Real trade-off	Contrived
Developer agility	Control and security governance	69	31
Single-cloud-vendor economies of scale and talent focus	Leverage in vendor contract negotiation and avoiding concerns of lock-in	83	17
Best-of-breed toolchain choices best suited for each environment	Standardization and familiarity of a single tool set	77	23
Customer or employee experiences	Security lockdown	50	50
In-house talent development	Immediate outsourced talent	81	19

Source: McKinsey expert interviews (N = 52)

Forgoing single-vendor benefits in the name of avoiding vendor lock-in. Companies can realize economies of scale and build deeper expertise (especially given the cited talent shortages) if they use fewer vendors or deploy technology to allow them to scale across multiple vendors with common controls. For 83 percent of CIOs, the potential loss of flexibility from vendor lock-in can loom large, forcing them to choose multiple vendors and thereby split their focus, divide their talent to learn and work on different vendor solutions, and reduce their speed of execution. The CIO of a North American retailer notes that when it comes to picking public-cloud providers to migrate applications, "This is a true debate. Without multiple vendors, you run into technical and financial lock-in."

CIOs can also accelerate application development by using native services offered by providers. However, in some cases developers are being discouraged from creating new dependencies on native services because of concerns that it will be harder to move away from the platform if needs evolve in the future. As a CIO for a professional services company explains, "We don't see concerns of vendor lock-in with public-cloud providers by betting on a single vendor. This is not a new concept for us. However, some of our stakeholders take a different view. They hear about outages and want us to source from two or more providers." Help is coming in the form of emerging solutions that work across cloud-service-provider platforms, enabling enterprises to avoid this compromise. In the meantime, leaders are working around vendor lock-in through the following methods:

— *Abstracting infrastructure.* Seasoned architects are choosing technologies such as containerization to abstract infrastructure and to enable portability across disparate environments.

— *Minimizing dependencies on infrastructure or platforms as a service (IaaS or PaaS).* Developers at leading companies build applications that are not tied to platforms by avoiding using proprietary cloud services offered in the PaaS layer. And in cases that necessitate dependencies, developing modular code enables services to be easily swapped

out when companies move from one cloud provider to another.

— *Safeguarding contracts.* Companies concerned about future price increases from cloud providers draft and negotiate contracts that both set boundaries and offer downside protection from escalation of costs.

— *Educating executives and the board on vendor strategy.* CIOs and CTOs who prefer using a single cloud provider are making the effort to educate board members and collaborate with them to come up with solutions for vendor lock-in or service disruptions.

Missing out on the benefits of best-of-breed tool kits for the sake of standardization and familiarity. Toolchains optimized for different environments—and those with which developers and operators are most familiar—help boost productivity. In our research, 77 percent of CIOs expressed concern over having to standardize a lowest-common-denominator solution. Consequently, this trade-off means accepting reduced functionality and fit for the work at hand. Modern developers need to be free to choose combinations of languages, libraries, and frameworks that enable accelerated delivery. Leading companies are working around this trade-off in the following ways:

— *Adopting open, vendor-agnostic solutions.* Emerging cross-platform open-architecture and open-source solutions provide coverage for hybrid and multicloud environments.

— *Continuously upskilling talent.* IT organizations are adopting best-of-breed tools and investing in upskilling for developers and operators on multiple solutions.

Trading customer and employee experience for the sake of security. Providing reliable "anytime-anywhere access" of applications to users (developers or agile teams in marketing, for example) allows organizations to rapidly innovate, respond to customer needs, and scale up tests and experiments. It also enables employees to be more productive and complete tasks from anywhere. In our research, we observed leaders pursuing the

following strategies to improve customer experience without compromising security:

— *Adopting a DevSecOps approach.* IT organizations are pursuing a DevSecOps style of management for high-velocity code and model-development pipelines. Doing so not only combines the security and DevOps functions—it also blurs lines across formerly distinct roles in "waterfall" software development life cycles, simplifying the end-to-end application development and delivery process.

— *Adding layers of security.* Leaders are implementing multiple layers of security, especially for identity and access management. They are using multifactor authentication and refreshing end-point security for applications that are accessed remotely or use mobile devices.

— *Investing in data security.* IT organizations are investing to not only secure their data, the perimeter, and applications, but also to encrypt at-rest and in-motion data.

— *Remediating applications.* Companies are remediating applications opened up for external access to employees and end users.

— *Assessing security automatically and more frequently.* Leaders have increased the frequency of application scanning and penetration testing (against apps and source code).

— *Ensuring application version compliance.* Automating patch scheduling for external-facing apps ensures compliance with the latest, most secure versions.

Delaying talent development and upskilling and augmenting talent with contractors. A shortfall of tech talent is a recurring challenge for CIOs. Companies often feel they face two options: develop in-house capabilities slowly or rely on external vendors to get initiatives done quickly. Despite the best intentions to build capabilities, IT teams often compromise by outsourcing projects to contractors or partners to patch holes in their talent pipelines. The challenge is that a short-term solution often leads to long-term dependence—without a parallel

focus on promoting skills transfer, retraining current staff, and systematically backfilling contractors. Leading companies tackle this issue in several ways:

— *Hiring new talent.* IT functions are investing in the cloud operations talent and developers who bring modern full-stack skills and mindsets. These workers represent a truly strategic resource, assuring that any cloud modernization effort accounts for skill building—even if organizations need a boost from contractors to get rolling quickly.

— *Building capabilities with external help.* Companies are bringing in external expertise for skill building (such as agile team facilitators, DevOps coaches, and analytics and data science practitioners) to augment in-house talent.

— *Offering employee-education programs.* Companies are providing their employees with tuition and external-training expenses for selected continuing education, such as AI and machine-learning programs, accelerated software engineering reskilling programs, and DevOps training.

— *Partnering with technology vendors.* IT collaborates with vendors such as cloud service providers and other partners to gain expertise and educate in-house talent.

— *Freeing up capacity to invest in new skills.* Automating routine monitoring, reporting, and troubleshooting tasks can create capacity for operators to develop new skills and take on additional responsibilities.

Unlocking the full range of business benefits through an operating-model transformation

Technology leaders can avoid making these trade-offs by harnessing the right combination of IT solutions in their hybrid environment—ranging from on-premise platforms, edge nodes, and cloud services. But no matter how powerful, technology on its own is insufficient to achieve acceleration. So CIOs must transform their operating model to see material benefits, including shorter time to value, improved business agility, and reduced business

risk. Business acceleration is best achieved by extending IT modernization efforts to encompass far-reaching changes in the operating model along three dimensions: people, processes, and policies.

People
Many enterprises have IT workforces with specialized skill sets and knowledge developed over years (for example, about custom legacy systems and platform configurations). But this expertise is increasingly outdated—even if the knowledge of a business or functional domain is not. In such cases, organizations must make significant investments to retrain, upskill, or reskill their employees. In addition, the IT function typically covers a range of roles: networking engineers, capacity planners, system administrators and operators, data storage and security specialists, analysts, developers, quality-assurance engineers, database administrators, data architects, and many more.

We see an opportunity for organizations to radically simplify their IT team structures. Specifically, they can consolidate positions to a smaller set of critical roles that bring together skills formerly divided across jobs. These roles will move from structured tasks (likely to be replaced by increasingly powerful IT-management tools) toward more fulfilling ones (adapted to a world of increasing automation). Instead of supplying more resources or convening cumbersome investigations over a system instability, the best companies will develop the talent to address root problems (for example, going under the hood and changing how code consumes infrastructure resources).

Processes
Many organizations depend on ad hoc manual operations and adopt a reactive stance, building excess capacity to provide reliability. Design decisions are marked by a lack of transparency and coordination across different functions in IT, resulting in more expensive custom solutions that still underperform. And when incidents arise, they are often funneled to technology silos. These functions either are slow to respond or depend on orchestrating numerous internal and vendor resources to manage escalated incidents and resolve problems.

The ideal organization does little to no infrastructure planning and instead uses a DevOps approach and self-service to expedite the development and implementation of solutions. In other words, rather than estimating demand and planning for worst-case scenarios, a company can simply be agile in ramping up resources as needed. The IT function focuses on customer-centric journeys rather than product- or service-centered processes. After setting a course, IT automation delivers the necessary service levels to optimize the user experience despite changing conditions and surprises. For example, self-driving cars hold the potential to automate travel on even chaotic roads; however, no "IT drivers" are ready to take their hands off the wheel just yet. So the tremendous potential of process automation must be designed to complement judgment and the uniquely human capabilities needed to assure reliability, scalability, and security.

Policies
Typical organizations have policies for a wide range of issues—such as security, information access, and data management. These are often manually enforced, increasing the cost of compliance and reducing effectiveness. As such, companies can struggle to maintain consistency across existing environments and extend established policies to new environments. Slow response times to evolving internal rules and external regulations result in increased business risk. Furthermore, many of these policies were developed for older IT paradigms, serving to reinforce legacy ways of working and hindering agility and speed.

Leading organizations are characterized by policies that engage technology for automatic distribution of change as well as for monitoring and enforcement. Standard policies across hybrid environments (for example, on-premise and cloud) lead to better compliance at lower cost. These companies can quickly respond to and mitigate emerging business risks by consistently pushing policy changes out across their hybrid operating environments.

An IT modernization journey will vary, depending on an organization's starting point and its aspirations for agility. Companies may seek to shift the bulk of their operations into hybrid or public-cloud operating

environments, move discrete parts of their application portfolio, or eliminate particular legacy infrastructure platforms. Some prefer building applications based on their skills and competitive context over buying them, while others are highly selective in their build strategies and focus on integrating third-party SaaS solutions. Additional factors include a company's industry, level of maturity, tolerance for risk, and organizational readiness for pursuing agility.

Overall, we see tremendous opportunities to accelerate progress on business agility—*if* organizations are ready to take the right steps across all these elements to transform the way they work.

Central questions for IT leaders to consider as they plan their journey

CIOs can overcome the perceived trade-offs in modernization efforts and maximize the business acceleration from these investments. No matter where they start, a few primary issues must be addressed. To set the best path forward, IT leaders should consider five central questions:

1. **Do we have the right talent to support the technology transformation and needed operating-model shifts?**
   Exemplary organizations view IT as a business-acceleration partner that proactively identifies opportunities—such as those from digital, data-driven decision making, and AI—to encourage growth. These IT functions have shifted skill profiles: from project managers to product managers, from operations engineers to automation engineers. They have upskilled developers with security expertise and recruited cloud architects, security engineers, and full-stack engineers. More advanced organizations have in-house DevOps or site reliability engineer (SRE) talent. Organizations are beginning to add data scientists and AI or machine-learning specialists to integrate more data-driven intelligence into IT operations.

2. **Have we implemented the right metrics tied to business strategy so that IT can prioritize business building over just keeping the lights on?**
   IT organizations with an effective talent engine have successfully created performance metrics

and commitments aligned with business targets rather than technical objectives. Objectives and key results (objectives and key results) methodology has proven effective in conjunction with agile teams, and these metrics need to be leading indicators that link to the key objectives of modernization. Organizations are increasingly using metrics such as APIs published, test scripts created, and configuration scripts automated as metrics to improve automation. They are also implementing metrics to track how much time is spent by individuals in building new features as opposed to routine monitoring and troubleshooting tasks.

3. **Are we automating IT to the fullest?**
   Leaders that have achieved agility differ dramatically from laggards in their rate of automation. The most successful companies are increasingly adopting DevOps or SREs as part of their operations approach. As a foundation, companies are implementing test-driven development and aiming to achieve full automation of unit and integration tests. They are also baking in standardized configurations as part of deployment automation. They are then providing the setup of develop-and-test environments to developers through self-service mechanisms, eliminating wait times and enabling "one-click" deployments. Application performance tracking and troubleshooting are supported by heavily instrumented code and telemetry. Furthermore, these organizations are incorporating automation into service-request management and incidence response. They are also beginning to use machine learning and data to inform and accelerate decision making, ultimately leading with policy-based operations and control.

4. **How are we building security by design?**
   Leading IT organizations have integrated security into every aspect of planning, building, and operating. They have managed to incorporate secure thinking and design earlier in the process and automated security enforcement based on policy. DevSecOps and API-based security are core enablers in such organizations. This effort starts with hiring developers with knowledge of security architecture. In the implementation phase,

developers create modular security components that can be easily reused, thereby eliminating the need for separate design and implementation. During the review phase, automatic code scanners are used for code reviews to detect vulnerabilities. In the testing phase, security tests are automated and integrated into the functional testing process. Last, during the deployment phase, APIs for environment creation include functions to enforce secure configurations. By taking this approach, leading organizations have accelerated—rather than slowed—developer agility and innovation. In parallel, they have also created delightful customer and employee experiences.

5. **What architectural approaches are we implementing to dramatically accelerate time-to-release features?**
   Approaches that increase flexibility, abstract the infrastructure, and let organizations focus on applications in line with business use cases are the hallmarks of leading IT organizations.

They have adopted containerized and serverless architectures and built applications dependent on open standards. When using proprietary platforms, decisions are based on the clear time-to-market advantage and technical superiority. Fast-moving IT organizations have heavily invested in API-based approaches and meticulously plan for code reuse. They also have a clear migration path in mind should a superior platform emerge.

———————

We see exciting innovations coming faster and faster from technology providers. These innovations hold the potential to overcome the compromises and constraints that have held back enterprise IT. The pace by which organizations can accelerate business change through these cloud platform capabilities will be set by the pace at which they can change the way they work.

This article was originally published on McKinsey.com in August 2019.

Arul Elumalai is an alumnus of McKinsey's Silicon Valley office, where **Roger Roberts** is a partner.

The authors wish to thank Arif Cam, Lisa Donchak, Jordan Rohrlich, and Chaitali Thakur for their contributions to this article.

How Prudential Financial is tackling the future of work

Prudential Financial vice chairman Rob Falzon discusses the criticality of people to digital growth, how Prudential is preparing its workforce for the future, and partnerships with the education sector.

Automation and digitization are transforming both business strategy and workplaces. The companies and organizations that build their talent engines to meet the changing needs of the future of work will thrive in tomorrow's world. Early movers are already making headway, solidifying their advantage over those who have not yet taken action.

The question of today is, "What works?" Many organizations are experimenting with everything from setting up skills-based talent marketplaces to building large-scale skilling programs to partnering with academic institutions.

Scott Rutherford and Jon Harris of McKinsey recently interviewed Rob Falzon of Prudential Financial. In the videos and the following edited excerpts of their conversation, Rob describes how he views the "future of work challenge" and what Prudential is doing to address it.

McKinsey: *"Future of work" is a term that's being used to describe so many different things. How do you define future of work?*

Rob Falzon: I find that oftentimes when people think about future of work, they immediately translate that into cost—the cost of people versus machines doing work. My view of it is that if you're focused just on the cost component of it, you're going to lose the race here—you're missing the real opportunity. The real opportunity—the real driver of the future of work—is around customer expectations [in a digitizing world].

One of the observations is that the full digitization of our companies and our economy today is not actually inhibited by technology or by data. We have lots and lots of data. And we have lots of ability to store that data. And we have tons of computing power. The enablement of digitization is actually talent.

So at Prudential, we know our talent is actually at the center of the future of work, as opposed to being marginalized by the future. And for us, the changing customer expectations are driving the urgency, and that's why future of work is such a massive priority. If you start with that mindset, it's all about, "How do you take the combination of technology and

talent and produce better outcomes for the talent and better outcomes of the company?" I think you need to take people from critical roles—roles that don't necessarily need to be done by humans—and put them into roles that are pivotal roles. The difference between these two types is, critical roles are important to get right—they are defensive and maintain a competitive position—but pivotal is about creating competitive differentiation and enhancing the customer experience.

McKinsey: *You mentioned you are doing a number of things around talent. Can you talk more about the training?*

Rob Falzon: We're standing up something we call "the Accelerator." And we're marrying it with apprenticeships. And I think both those components are really important.

Our Accelerator is a program that's being defined by going function by function, business by business, and encouraging the leaders of those functions and businesses to look forward three to four years. We don't look any more forward than that, because if you try to look ten years forward, it becomes like boiling the ocean. It's overwhelming. But if you look three to four years forward, just sort of around the corner, what does your function look like? What does your business look like? That definition should then inform what your talent needs to look like. And that informs the skills of that talent. So we've started going through that exercise for every business and every function, and we use that to inform the types of training that we need in the accelerators.

There are multiple Accelerators. One is a series of programs that individuals will go to for the broader skills—for example, digital literacy, leadership, and other things that are very transferable, no matter what job you have. Another is very specific and aligned to the roles and skills that we need on a go-forward basis in their areas in order to allow individuals to go from jobs that they have today into skills and jobs that are needed in the future.

Now a critical component of all of this is apprenticeship. Studies have shown that 70

percent of your learning occurs on the job. So there is only so much we're going to accomplish through the formal training programs. Ultimately, people are going to learn by getting on the job—and then hopefully succeeding at those jobs. The challenge we face is that it's often hard to get them into those positions because the hiring manager is looking for the individual who's got all of the right skills today. The apprenticeship model gives employees that opportunity to try something for six months—to see if they can succeed, at a low risk to the hiring manager, so that we can create the learning on the job to complement the things that we're doing within the Accelerator.

McKinsey: *One of the things we are finding is companies realizing they can't do this on their own. And we see ecosystems being formed through partnerships to help with either future of work for the company's employee base or for the communities the companies operate in. We're seeing universities working with corporations in new ways—and even partners within the corporate world working together. What ways have you started to partner with others on this?*

Rob Falzon: So as I mentioned, we are creating learning modules, and we're creating training experiences. And there are others that have created software or other learning content. We can piggyback off of one another instead of all recreating the wheel ourselves. Everyone has different perspectives and brings different things to the table, so the opportunity to engage other companies within and outside of your own industry [on future of work] can be really enlightening. We've learned that companies can't do it all themselves but should partner. We believe that every institution and individual has a responsibility to make this a success. So individuals own their careers, but

at the same time, companies must help their employees to make transitions. And it's in the company's economic interest to do so. Academic institutions also have a role to play here—and government too. None of these players individually can make this happen by themselves. Rather, it's about coming together to create collective solutions—a concept I call "stackable institutions." One example I would give you is one of the programs we've established in Newark, where we've begun to engage with high school juniors who are math majors in order to create a program for them and provide mentorship to help them successfully get from high school to college. Then they can transition into a Rutgers [the State University of New Jersey] honors program, which is stacked on the high school program, where they've committed that half the slots from that program will go to Newark students. Finally, we have stacked on that by saying, "If you do that, we'll endow a $10 million scholarship fund to help fund kids who might get in but might not have the financial wherewithal to live at the campus and get the full experience—or even to cover the tuition."

We and other companies are now interfacing with that honors college and providing internships—and ultimately jobs. Now that talent base is well trained to come into our workforce with the skills that we're going to need for the future. So it's a way to create a pipeline. Now, again, this is good, but it's also good business. It creates a pipeline of talent for us to satisfy the needs that we have for work of the future.

It will be a challenge, I think, for all companies to meet the needs they're going to have from a talent standpoint, just given the employment situation and the dearth of the skills that we're looking for in the marketplace, unless they do these types of partnerships.

This article was originally published on McKinsey.com in October 2019.

Rob Falzon is vice chairman of Prudential Financial. **Jon Harris** is a senior partner in McKinsey's London office, and **Scott Rutherford** is a senior partner in the Washington, DC, office.

Digital ecosystems for insurers: Opportunities through the Internet of Things

The Internet of Things has entered customers' everyday lives around the globe and transformed business models across industries. This environment brings opportunities for insurers: to develop new products, open new distribution channels, and extend their role to include prediction, prevention, and assistance.

by Simon Behm, Ulrike Deetjen, Sanjay Kaniyar, Nadine Methner, and Björn Münstermann

The Internet of Things (IoT) will radically change the world in the coming years, and networked devices will be a substantial part of that change. In 2010, people owned 12.5 billion networked devices; it is estimated that by 2025 that number will have climbed to more than 50 billion (Exhibit 1). People use such devices, many of which are equipped with sensors and automatic-activation functions, in practically all areas of their life, including for both work and leisure. It has long been possible to install them quickly and easily and to wear them anywhere on the body. These devices can transfer huge volumes of data to their providers or third parties—whether for real-time analysis or to automatically trigger reactions or services—and are already altering traditional business and operating models in multiple sectors.

So far, insurers have mainly used IoT capabilities to aid interactions with customers and to accelerate and simplify underwriting and claims processing. Increasingly, however, new IoT-based service and business models are emerging that are highly attractive to insurers. In the context of these new business models, digital networking through the IoT could become a strategic component for insurers. For example, insurers could partner with companies to provide improved or new cross-industry products and services that harness IoT technologies and the new ecosystems, which are discussed further below (Exhibit 2).

IoT technologies enable insurance companies to determine risks more precisely. Auto insurers, for example, have historically relied on indirect indicators, such as the age, address, and creditworthiness of a driver, when setting premiums. Now, data on driver behavior and the use of a vehicle, such as how fast the vehicle is driven and how often it is driven at night, are available. Applications of such technology in countries where the market is already much more mature reveal that insurers can assess risk far more accurately this way.

Networked devices also allow insurers to interact with their customers more frequently and to offer new services based on the data they have collected. In the insurance sector in particular, customers often engage exclusively with agents or brokers; direct customer contact has been limited to contract extensions and the handling of insurance claims. The IoT could therefore have considerable benefits for customer relationships, allowing companies to establish more intensive and targeted customer contact.

So how can insurers develop compelling IoT offerings and a successful strategy for setting up and becoming involved in IoT-based ecosystems?

What digital ecosystems are most important to insurers

Four different digital ecosystems are emerging that are relevant and attractive to insurers: mobility/connected car,[1] smart housing, connected health, and commercial lines (Exhibit 3). While these ecosystems certainly have parallels by measure of their basic dynamics, on a granular level, they have key differences, which is why insurers need to develop a dedicated strategy for each. The degree of market maturity differs in each of the ecosystems, and they feature some clear distinctions in market dynamics, relevant players, and regulatory environment.

Overarching dynamics can be explored using two examples: the mobility/connected-car ecosystem, the most advanced of the four ecosystems, and smart housing, specifically Ambient Assisted Living, which combines smart-home and connected health services in an innovative and effective way.

Mobility/connected car
The automotive industry and the mobility/connected-car ecosystem clearly demonstrates how digital ecosystems function and what development dynamics they can reveal. It also illustrates the entrepreneurial opportunities and challenges of this new environment.

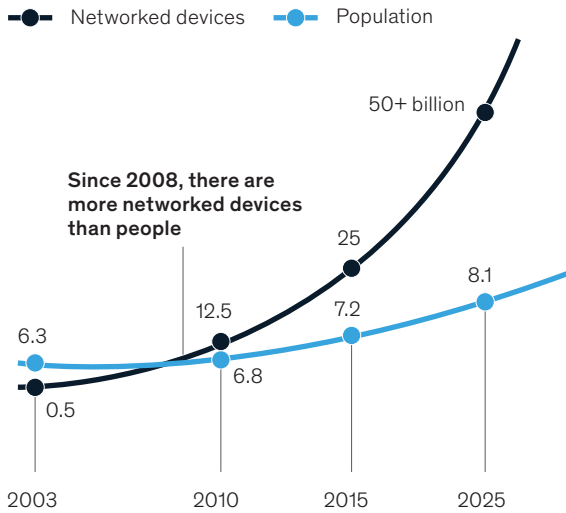Cars—and their drivers, if carrying smartphones—are increasingly outfitted with sensors that do not just monitor driving behavior and use of the vehicle but also collect other vehicle data,

---

[1] For more on connected-car ecosystems, see Markus Löffler, Christopher Mokwa, Björn Münstermann, and Johannes Wojciak, "Shifting gears: Insurers adjust for connected-car ecosystems," May 2016, McKinsey.com.
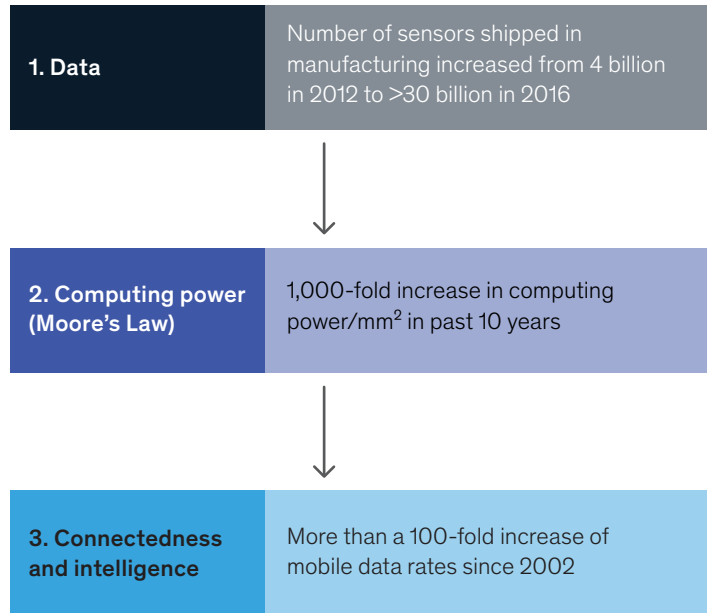
Exhibit 1

Networked devices now outnumber people and are an important component of the IoT.

An increasing number of networked devices . . .

—●— Networked devices ——●—— Population

50+ billion

Since 2008, there are more networked devices than people

25

12.5

8.1

6.3

7.2

6.8

0.5

2003   2010   2015   2025

Source: Markus Löffler, Christopher Mokwa, Björn Münstermann, and Anand Rao, "Partnerships, scale, and speed: The hallmarks of a successful IoT strategy," March 2017, McKinsey.com

. . . and three critical enablers are kick-starting the IoT

1. Data	Number of sensors shipped in manufacturing increased from 4 billion in 2012 to >30 billion in 2016
2. Computing power (Moore's Law)	1,000-fold increase in computing power/mm^2 in past 10 years
3. Connectedness and intelligence	More than a 100-fold increase of mobile data rates since 2002

from the oil temperature and wear of the brakes to tire pressure. This data forms the basis for countless new applications that contribute to customer comfort as well as to active and passive safety. The increase in applications of this kind creates a completely new ecosystem around the connected car, encompassing not just automotive OEMs. Other players in this landscape include telecommunications operators, sensor and chip manufacturers, operators of digital platforms such as Uber, research institutes, standardization centers, and, of course, insurers.

This ecosystem alters the competitive parameters for all participants—in particular, insurers. While the claims frequency of networked vehicles will decline, the numerous sensors on and in the car will increase the average claims sum due to the high repair costs. Even if high-risk customers can be distinguished

from low-risk ones using the additional data gained from the new ecosystem, overall premiums may fall due to discounts offered for telematics use. While careful drivers may justifiably expect quite considerable reductions in their insurance premiums, insurers likely won't be able to compensate for this decrease simply by increasing the rates for high-risk drivers.

To minimize the impact of any resulting decrease in premiums, it will be important for insurers to explore additional levers in conjunction with reducing claims expenditure via optimized risk selection. More effectively combating fraud, increasing use of allied repair workshops, and offering assistance and service add-ons are all initiatives that could potentially more than compensate for decreasing premiums.[2] Insurance companies could, for example, provide services for avoiding risk, point out

[2] For further details, see *Assistance & service offerings as a game changer in a transforming insurance industry*, May 2017, on McKinsey.com.

Exhibit 2

Digital networking via the IoT allows insurers to both significantly reduce costs and generate additional revenues.

Generate additional revenues

Offer new and more frequent customer interaction

Provide greater customer interaction and cross-selling, eg, via telematics apps

Develop new service and business models

Monetize data insights, eg, telematics via driving behavior and patterns

Review price models

Introduce usage-based or demand-adjusted pricing (monitoring via IoT sensors)

Reduce costs

Increase efficiency and optimize resources

Trigger automatic maintenance and therefore improve prevention mechanisms

Improve safety and pursue active prevention

Extend safety standards, eg, via immediate dispatch of ambulance services after an accident

Leverage analytics to curb fraud

Use sensor-driven decision analytics that enable the recognition of fraud

necessary maintenance work to drivers, and identify intelligent parking solutions. Insurers also can sell their data and analysis solutions to third parties, such as media agencies focusing on location-based advertising.

Various insurers worldwide have already partnered with IoT-based telematics suppliers, automotive OEMs, vehicle repair shops, telecom companies, and operators of systems that guide drivers to free parking spaces—for example, Progressive partnered with Zubie and TrueMotion. Such partnerships will provide both sides with access to

the valuable sensor data that will lay the groundwork for new hybrid insurance models.

It is possible, however, that these partners may have a better, more intensive relationship with insurance customers than the insurers themselves. Companies outside the insurance industry can also increasingly generate risk-related data and many have the requisite skills to derive relevant conclusions from it. In other words, while insurers can unlock great value from new IoT-based ecosystems, players in other sectors may be closer to the customer interface.

Exhibit 3

Four digital ecosystems are particularly attractive and relevant to insurers.

Questions to reveal key differences between IoT ecosystems

■ Private lines

Maturity	Do tried-and-true business models exist?	
	How many players are already piloting IoT projects?	
Market dynamics	What has to happen to become a pioneer in this market?	
	Is it a market in which there are barriers to entry for any key ecosystem positions?	
Relevant players	Who are the key players in this field?	
	Who is dominant at the moment?	
Regulatory environment	Are there special requirements regarding the IoT?	
	To what extent do regulations benefit or hinder innovation in the IoT area?	

Smart housing and smart health

The insurance market did not initially embrace smart housing—primarily because the potential new market was too limited for technical reasons and the solutions available on the market were slow to meet technical standards.

However, this situation has changed as the technology has matured rapidly. With the advent of Google, Amazon and other providers put their smart-home offers on the market. In recent years, the mass market has opened up by facilitating simple connections with more devices. As a result, many insurers around the world (for example, Allianz) have started cooperation models, selling integrated products via Google Nest or offering insurance discounts for people who equip their homes with smart-home devices. In addition, these insurers offer digital add-on services such as home security and convenience services (for example, Liberty Mutual).

Customers have also come to expect more and different services from insurers. To date, smart-home insurance products have largely lived under the property and casualty segment of the insurance market. Insurers have treated the product relatively defensively, as new, more modern home contents and supplementary insurance, regardless of the development of add-on services and more attractive price models for customers over the years. As insurers have also continued to sell traditional products in parallel, it has become evident that new customer segments can be addressed with smart-home insurance products.

An extension of smart housing is Ambient Assisted Living. This field connects with connected health services as well, which is particularly relevant in aging societies across industrialized countries. People with limited mobility, for instance, are increasingly seeking innovative services to aid their day-to-day activities and enable them to pursue an independent lifestyle at home. Potential customers of this segment will likely have a positive attitude toward the IoT and related technologies, as well as to insurers acting as overarching providers of this kind of new service bundle. Insurers can also position themselves as digital coordinators of nursing-care services and providers such as proptechs and general as well as specialized housing associations.

Insurers can tap into opportunities in this sector by providing customers with additional services that allow the insurers to minimize their costs.

Commercial lines
One of the areas with high value at stake is commercial ecosystems—that is, ecosystems centered on distribution to business partners (B2B or B2B2C) and on making the most of partnerships along the value chain. Whereas private lines ecosystems are primarily aimed at optimizing customer points of contact, commercial ecosystems also often focus on data and operational excellence.

Commercial lines insurers have various ecosystem plays available along the value chain: product innovation, distribution excellence, risk prevention, comprehensive service provision, supplier network management, and capital-to-risk matching. An example for product innovation involves cybersecurity, as only through additional risk management and assistance services does it become viable to insure cyberrisks—hence the rise of new partnerships between insurers and IoT cybersecurity software and hardware providers. IoT-enabled risk prevention may include, for example, sensors in warehouses to assess risk—and hence price—on a more granular level. Supplier network management has frequently been applied in (fleet) motor insurance for garages and in directors and officers liability insurance for lawyers. And capital-to-risk matching refers to an electronic platform to trade new forms of insurance-linked securities—allowing insurers to transfer risk via the markets, as is done already by some commercial lines insurers.

How insurers can improve their competitiveness and innovate
To be successful with digital ecosystems in an IoT world and develop an IoT strategy, insurers should first tackle five key tasks.

Define application areas
Insurers need to define concrete applications that customers in their market are willing to embrace and that are relevant to their business model. The potential for discounts for telematics use differs across countries, for instance, because customers' savings potentials are lower where motor insurance policies are cheaper.

While being as specific as possible in identifying attractive customers segments and promising application areas, insurers should consider the mid- to long-term potential of the application area as well as calibration factors that might unlock unrealized potential. In the German market, for example, at first glance smart housing retail insurance offerings seem to be relatively unattractive for two reasons: the market for traditional retail property insurance products is quite saturated, and roughly half of the population rents their homes, making them unlikely to invest in property tech and IoT devices. However, customer segment and behavior analyses reveal strongly growing potential for new IoT-based retail products among young and affluent renters, as well as older and more affluent property owners.

Lock in adequate strategic partnerships early
Selecting the right partner is just as success critical to defining well-shaped IoT-based insurance offerings. In mobility/connected car, these partners are OEMs, telematics providers, parking garage operators, or gas stations. In smart housing, these partners tend to be utility companies, multimedia providers, telecoms operators, and companies in the housing sector as well as specialized property tech sector players. In Ambient Assisted Living, partners include a combination of those mentioned plus connected-health providers.

To shape an adequate offering, insurers should reach out to potential partners early and actively involve them in the development and fine-tuning of the offering. This will shorten the time to market, lower the risk of sunk costs, and increase transparency on an active and rapidly expanding market. It will also increase stability of the partnership as both sides will need to invest in shaping the offering for market maturity.

Selection of candidates for successful and stable partnerships should involve certain key factors. First, partners must have sufficient experience, as well as relevant knowledge of and exposure to the target customer base. For example, IoT device providers must demonstrate mature tech operations and cybersecurity capabilities, and property-tech companies should bring an existing customer base. Second, partnerships should include an adequate commercial agreement from the start

that will appropriately provide incentives all parties to scale up the joint offering as needed. Flat rates, commission models, or volume-based incentives could all work if shaped with an appropriate risk appetite. Third, partners must be open to technical and business interoperability, to allow for other partners to step in and expand the ecosystem collaboration, as well as submit to an appropriate risk evaluation of their offerings, for example, on adequate geographical coverage or capture of relevant data needed for actual claims processing. Finally, insurers should carefully screen partnership candidates regarding their other business planned or already conducted to avoid the risk of reputation damage, sunk costs, or even accidental abuse of customer data.

Ensure scalability

Insurers can improve their ability to find the right partner by carefully positioning themselves as an attractive partner with the capabilities critical for success in the IoT ecosystem, thus ensuring the requisite scalability. An important related issue for insurers to address is consumers' reservations regarding data protection and security. Insurance companies can and should present themselves as trustworthy and reliable partners and highlight the benefits of digital networking for the consumer, such as lower premiums or a faster breakdown service. Large insurers that already operate with a tight-knit network of allied workshops have clear advantages: they can expand on possible offers with greater speed and agility. It is important for insurers to go to market with a first offer swiftly to test customer acceptance. As a second step, they can scale the offer.

Maximize rollout speed

The issue of scalability also includes the question of speed. Insurers must ask themselves if they are in the position to put their IoT offering on the market quickly. The IoT could soon reach a point where market penetration also increases exponentially for insurance products. Insurers that are not able to act fast will run the risk of losing out completely. Over time it will become ever more difficult to find a partner that both offers sufficient data and contacts and that is not yet linked to a competitor—OEMs ultimately only need one insurance partner. Data owners are likely to be choosy and to want to establish a partnership early in the smart-home market. Thus, established insurers that are best prepared and can provide a compelling IoT offering fastest will shape the market and competitive scenario, and there will be no pickings left for laggards.

Ensure a long-term perspective

Insurers should see the development of IoT services for ecosystems as a long-term investment in future capabilities. It is still not exactly clear what a positive business case for IoT offerings looks like. Reductions in premiums due to use of telematics may be significant in some markets, while there is not yet any reliable evidence of the benefits of better claims ratios. In the years to come, as maturity grows and the cost of the services continues to fall, the value for customers as well as insurers will decline considerably. Insurers should begin building their long-term capabilities now to expand their market position and develop innovative, competitive services for their customers in the years ahead.

In the end, it is important that insurers position themselves as attractive partners for existing IoT providers, ensuring that they find their role in the ecosystem and create genuine value for customers. Investing in innovative approaches will only pay off and be successful in the long term if customers understand and can see the benefits, which should include more favorable prices and rebates, additional services, and greater convenience.

This article was originally published on McKinsey.com in February 2019.

Simon Behm and **Björn Münstermann** are partners in McKinsey's Munich office. **Ulrike Deetjen** is a partner in the Stuttgart office. **Sanjay Kaniyar** is a partner in the Boston office. **Nadine Methner** is a partner in the Frankfurt office.

Future-proof the foundation

Rethinking the technology foundation for digital transformations

The McKinsey Perpetual Evolution™ approach will help established companies keep pace with digital innovation

by Oliver Bossert and Jürgen Laartz

Why are some Internet retailers able to make crucial changes to their ecommerce websites in hours while it takes brick-and-mortar retailers three months or more to do the same? How come just a few car manufacturers can rapidly make online updates to their products in the field, be they to their infotainment systems or to fuel and engine performance—a practice that is becoming crucial in a world of servitization, where manufactured products come with digital services attached to them? And how is the new wave of cloud-based enterprise software vendors able to make software updates to their products in days or weeks, rather than the months it takes traditional enterprise software vendors to do so?

Rethinking the technology foundation for digital transformations

Given that they compete front and center today with such digital natives, established companies must be able to operate with that kind of speed. But most of them can't, and to a large degree it's because of their enterprise architecture—that is, how they have designed their technology to support their business strategy. To compete against the best digital natives, traditional companies now need to adopt a much different approach to enterprise architecture. We refer to it as Perpetual Evolution™ because it allows them to continually upgrade both their digital business capabilities and the technologies underneath them.

For companies whose enterprise architectures lock them into legacy business processes and technologies, competing against pure digital companies with perpetual evolution architectures should raise red flags. Established companies in nearly every industry are racing to digitize their business models, product and service offerings, and the business processes that support them. Some are spending enormous sums to ward off companies like Amazon, Netflix, Uber, Spotify and PayPal which began life on the Internet and have rapidly gained share in sectors ranging from retail and entertainment to banking and transportation.

Unburdened of having to connect their new digital systems to aging technologies, today's digital natives can build greenfield digital business processes unconstrained from prior work, in online marketing, sales, distribution, and other areas. That is a key reason why they're thriving in this era of digitization, product servitization, and dramatically reduced software release cycles—all at a time in which those three trends thwart the incumbents.

In this article, we explain what an enterprise architecture of Perpetual Evolution™ is, how it contrasts with the architecture approaches of the past, and why it has become necessary. We then explore what companies must do to shift their enterprise architecture from the old to the new and the benefits they can get in doing so. Finally, we discuss what it takes to operate with this new architecture.

Enterprise architecture approaches, old and new

In the physical architecture, in which everything from homes to skyscrapers are mapped out, building design approaches depend on the technologies and materials available for construction. Skyscrapers, for example, couldn't be built until the arrival of high-strength steel and elevators in the late 18oos. The same principle holds true in the ways companies design products, work processes, and the information systems that support them—the ability to capitalize on new digital technologies requires new approaches to enterprise architecture.

The enterprise architecture approaches in most large companies today reflect a bygone era, a time in which it was not necessary for companies to rapidly shift their strategies, continually evolve their products and services, and constantly improve their business processes. Until this decade, digital technologies such as mobile devices, Internet of Things sensors, and big data and analytics platforms weren't crucial to being able to compete in the marketplace.

A way to think about the enterprise architecture practices of the past, current and future is to look at six core elements of the enterprise stack—business operations, business capabilities, IT integration platform, IT infrastructure services and information and communications technology:

— In designing their business operations, companies developed technology and methodology that support an inward-looking view—systems that automated and incrementally improved business processes such as order to cash, and service inquiry to resolution.

— Companies did not have an acute need to continually infuse new IT-enabled business capabilities into their operations. (By business capabilities, we mean isolated business activities that accomplish a distinct business outcomes such as an activity within a business process. Finding the product a customer would most likely buy next is one such activity.) They introduced those capabilities slowly and periodically. Even today, most companies have not rebuilt their applications as business capabilities.[1]

— Business applications such as ERP, SCM, PLM and CRM were tightly coupled systems. Making changes in one part of the application often required making big changes in other parts.

— The IT integration platform was what we call a heavyweight enterprise service bus (ESB)—heavyweight in that most business logic was written into the bus. That has turned ESBs into big monoliths that make it difficult today for companies to operate digitally in real time—e.g., to offer web visitors low latency page loading times. Customers who won't put up with such delays in the online experience are costing online retailers billions of dollars in lost revenue.

— IT infrastructure services were centrally managed by an independent team. After the developers and code testers were through with their tasks, they threw it over the wall to production, whose complex test and handover process could delay the delivery of a new system to the market for weeks or months.

— Information and communications technology was costly, and thus it had to be deployed carefully as a costly (but necessary) expense that had to be minimized. This is a key reason for the intense pressure to consolidate, outsource and offshore IT to drive costs down.

These architectural practices were successful in a world in which companies from time to time had to make major, multifaceted changes in their business and IT infrastructure. Those changes happened every 10 to 15 years, and they typically were the result of implementing a major enterprise system such as ERP, SCM, PLM and CRM.

In effect, these architectural approaches enabled what we call periodic revolution in the business and IT architecture—"big-bang" changes every decade or so. But operating in today's digital world requires a much different architecture. The new architecture must enable companies to make continual changes in their business process and IT infrastructure. As such, it is an architectural approach that we refer to as Perpetual Evolution™.

Exactly how is an architecture of Perpetual Evolution™ different? Let's examine its implications for those six core elements of the stack. (Exhibit 1)

Business operations: designed with an outward view

Business processes and digital systems must be designed with an outward view focused on the customer experience online and offline—rather than on an inward view of a company's operations. Priorities have changed. While the customer used to be an element in a producer company-centered process, today the products and services are an element of a customer journey.

To be sure, companies' inward-focused view isn't obsolete. Enterprises need to keep their core transactional processes and systems, whether they are accounts payable/receivable, order management, procurement or something else. And they must also make sure those business processes and technologies remain efficient.

However, increasingly an architecture that enables companies to perpetually evolve their businesses cannot focus only on the journey that customers use in purchasing their offerings. For many companies,

Exhibit 1

IT architectures, from periodic revolution to Perpetual Evolution™

Stack
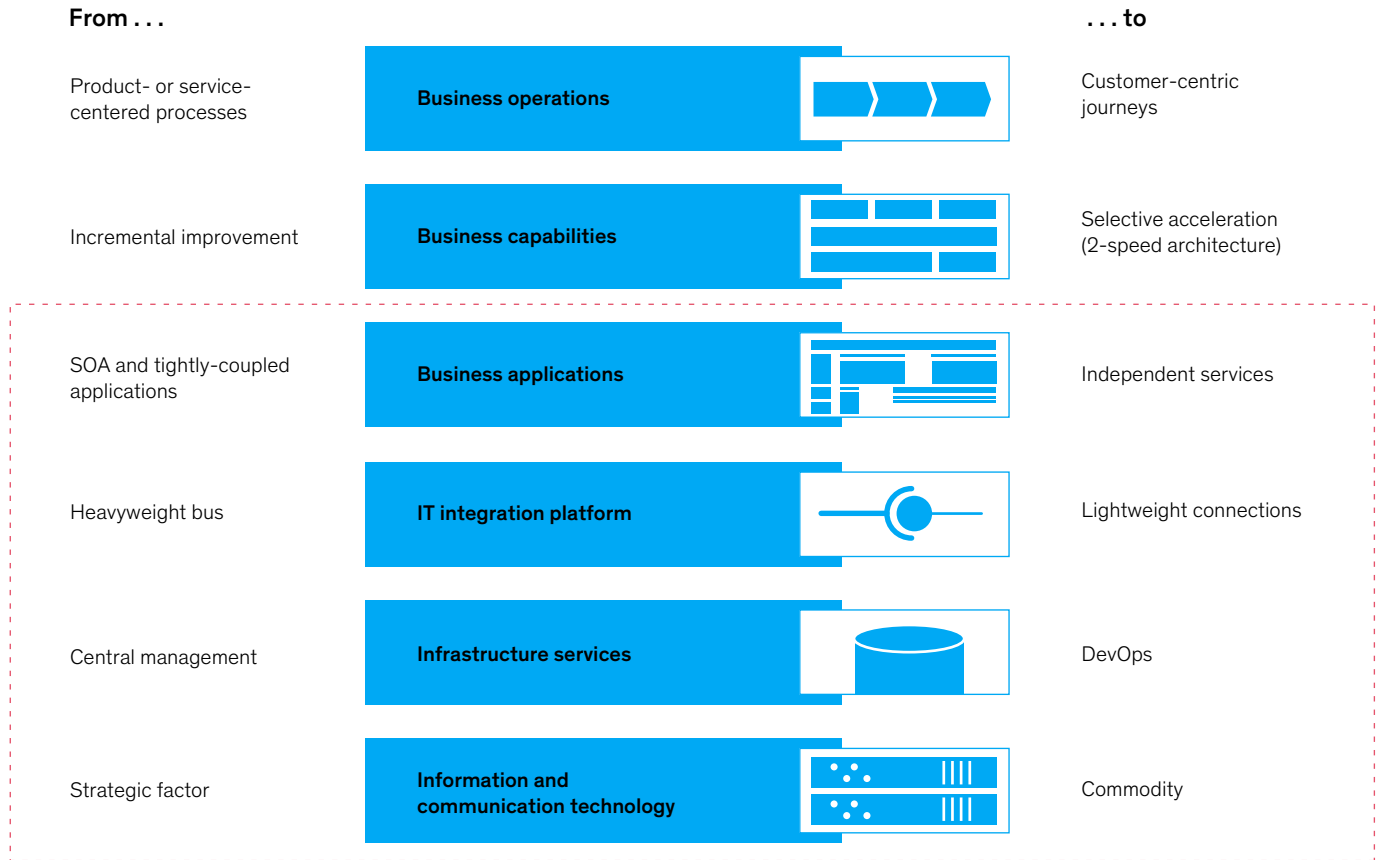
From . . .		. . . to
Product- or service-centered processes	**Business operations**	Customer-centric journeys
Incremental improvement	**Business capabilities**	Selective acceleration (2-speed architecture)
SOA and tightly-coupled applications	**Business applications**	Independent services
Heavyweight bus	**IT integration platform**	Lightweight connections
Central management	**Infrastructure services**	DevOps
Strategic factor	**Information and communication technology**	Commodity

[1] McKinsey insurance cost benchmark. Median of select P&C players in Western European peer group, enhanced by insights from client cost benchmarks/expert interviews (2016 year-end analysis).

[2] "Legacy" refers to systems that are old, outdated, and usually running parallel across different areas. Each insurers' system was classified as 1) old but stable and functionally sufficient, 2) legacy IT, 3) currently in modernization/replacement, and 4) recently modernized. Only legacy IT and recently modernized were used for the above analyses.

architecture needs to reflect a larger journey. Take, for example, an automobile insurance company's architecture. More and more policies are purchased on websites that aggregate the entire auto purchase: the car, the insurance, and more.

These larger ecosystems are end-to-end customer journeys, and you see them happening in many B2C industries in which consumers must buy several products and services to accomplish a single task: buying or renting homes, taking a vacation, and many more.

Note that B2B companies are not immune to the trend, especially those that embed digital technologies into their products (e.g., construction equipment, aircraft engines, power turbines, drilling equipment) to sell predictive maintenance, performance improvement and other services. That's the whole servitization trend we mentioned earlier. That requires a company's enterprise architecture to encompass the entire time in which customers use their products, even in real time, not just the moment of purchase.

Even B2C companies are getting into the servitization game. Take the case of manufacturers of high-definition smart televisions. In the old world of TV manufacturing, companies designed their IT systems to follow the product to the customer (in this case, to a retailer). Today's digital TVs have become platforms for manufacturers to provide a range of TV-related services to the home, such as identifying shows consumers might want based on their viewing habits, targeted advertising and more. The impact on TV makers' enterprise architecture is that they must design systems that encompass the end customer's TV viewing experience.

Business capabilities: the foundation of digital competition

Digital systems that provide the narrow functionality (such as one-stop checkout) necessary for a superior customer journey are the foundation of an architecture of perpetual evolution. In fact, the best digital native companies organize their teams of business and technology professionals by such distinct business capabilities. For example, Spotify groups teams into squads, each of which controls a set of business capabilities.

To compete in a fast-changing digital world, established companies must first move to a model for digital capabilities. They must be able to continually improve the digital business capabilities that comprise their customer journeys, and add new capabilities when necessary, by adopting an architecture of Perpetual Evolution™.

That, in turn, means grouping processes and systems into two categories: digital business capabilities that are differentiating for the customer experience, and those that are supporting transactional capabilities. We call this a two-speed architecture.[2] These digital business capabilities become the basis on which to compete in an online world.

Consider a retail chain that sells a growing proportion of its products through its website. The company cannot take months to enhance its product recommendation engine when a digital native online retailer can do that in days or weeks. The only way to do that is having an architecture that makes businesses capabilities systems-agnostic. It doesn't matter, for example, what kind of core systems the retailer has; its new or enhanced product recommendation approach can be implemented and changed easily.

So now after moving to a capability-based model in the first two levels of business operations and business capabilities, the enterprise architects need to ingrain a highly modular software skeleton in the four levels below them in the stack. We start with the business applications level.

Business applications: shifting from SOA and tightly coupled software to independent services

The goal in adopting a Perpetual Evolution™ architecture in this layer of the stack is to be able to upgrade core applications such as ERP, SCM, PLM and CRM module by module (or service by service)—without having to upgrade to a whole new version of those applications. (See Exhibit 2.) This can be explained based on three steps:

Step 1: In a monolithic architecture all elements are tightly coupled. The core platform and services are in a single release container.

Step 2: In a more service-oriented approach the functional elements, such as payment or promotion management are decoupled from one another. Still when a change does not affect a single service but the platform it will go in a longer release window.

Step 3: Perpetual Evolution™ is introducing true modularity of the underlying platform, such as deployment, data management, and analytics, so that also technical capabilities can be changed independent from one another.

IT integration platform: lightweight integration

Heavyweight buses such as an ESB no longer are the answer to all problems. Companies need lightweight connections between their services in areas where granularity and performance are of high importance. That's the only way to deal with the problem of latency—the time it takes for companies to deliver web pages to online customers who demand instant responses at every click.

Exhibit 2

Shifting applications to Perpetual Evolution™ architecture

	Monolithic	Traditional SoA	Perpetual Evolution™

Business capabilities

Technology platform
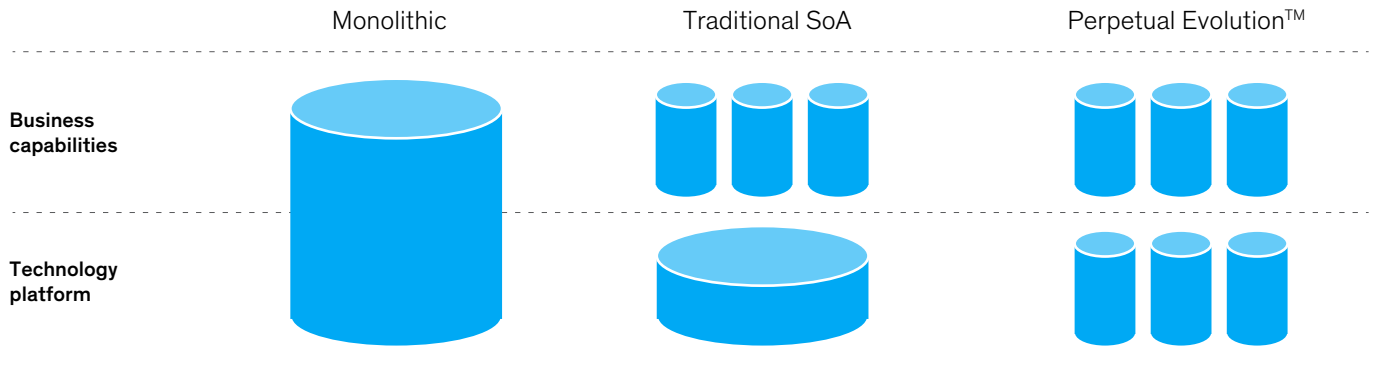
And it is the architectural prerequisite for decoupling services without making the bus a bottleneck. Without lightweight buses calling an increasing amount of Web services , IT integration platforms become big bottlenecks in the customer experience, and a major factor behind online customer defection.

Infrastructure services: DevOps takes down the wall

The concept of DevOps has firmly taken hold in many companies—grouping together IT professionals previously separated in the functions of software development and IT operations. DevOps becomes central to a firm's ability to test new digital business capabilities and bring them to market rapidly. In doing so, companies should be able to tweak business capabilities and put them online in hours or days, rather than the weeks or months it takes to develop an enhancement, throw it over the wall to testing, and then put it into a long production queue.

However, to make the DevOps model work companies need to put their DevOps team members into the teams charged with updating and building new digital business capabilities. In other words, there is one team for each business capability, and on that team are representatives from systems development and operations.

Information and communications technology: a big expense becomes a less-expensive commodity
Technology services from cloud vendors turns IT into an affordable resource for companies of many sizes.

All of a sudden, the big, costly IT infrastructure that companies have taken years to build is no longer a competitive barrier. Startup companies can climb into the game quickly, as firms like Netflix (renting computer power from Amazon Web Services for many years to support its streaming video services) and many other digital natives have done. Information and communications technology is now a commodity, and prior investments are no longer necessarily a big competitive advantage and barrier.

Binding together these six fundamental changes in the stack will enable companies to move to an architecture of perpetual evolution of their business and IT. That will enable them to loosen up their asset base of business and system capabilities—they can change out parts quickly, add new parts in no time, and replace other parts with the latest and greatest functionality.

Establishing a perpetual evolution architecture

So how do companies transition their architecture from the old to the new? How do they move from the design philosophy that guided their present IT asset base, to an approach that governs the infrastructure they need now—one by which they can make perpetual evolutions of their business in a digital world?

The obstacles are many, but all are surmountable. From our experience helping companies across industries and geographies adopt a Perpetual

Evolution™ architecture, we have found five moves to be critical:

— Freeing up the team from unnecessary dependencies

— Not overinvesting in one area by consistently eliminating dependencies

— Setting boundaries in technology—not on paper

— Maintaining freedom within capability teams through strict separation from the platform

— Regarding the platform as one of continuous change

Free up the team from having to deal with unnecessary dependencies
The concept of decoupling is a very old one in technology. However, in the past it was only applied to a limited area of the technology stack.

In the past when talking about decoupling, companies usually defined it as a technical challenge of the services or elements running on top of a rather large platform.
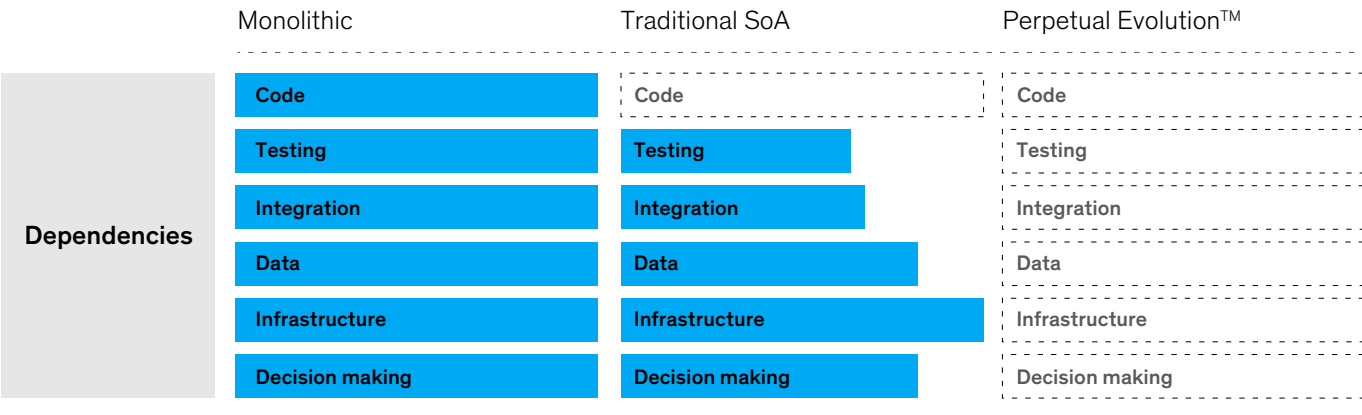
Today, all dependencies must be eliminated because it is the only way a company can change the pieces of its digital products and processes quickly, and thus keep its customer experience competitive. To do that, an architecture must eliminate dependencies among business capabilities and within the technology stack. Consider an auto manufacturer that has embedded digital technologies into its cars that enable customers to make online updates to its navigation, infotainment and other systems. If the automaker didn't design those systems in ways that it could isolate business capabilities it wants to offer customers—e.g., a certain navigation capability or a specific new feature of the infotainment system—it won't be able to change or update these elements independent from one another. Eliminating such dependencies is crucial to companies that want to design and sell new digital capabilities to small customer segments, each of which have different needs.

With this said, it is clear that dependencies need to be eliminated along all six dimensions of system development, not just in coding. (See Exhibit 3.) In a Perpetual Evolution™ architecture however the modularity and the decoupling is not limited to the functionalities. It also extends to the technology platform and the operating model.

Exhibit 3

Perpetual Evolution™ requires eliminating dependencies—not just in the technology area but also operational and decision making processes.

⸰⸰ Independent   ▪ Tight coupling

Dependencies	Monolithic	Traditional SoA	Perpetual Evolution™
	Code	Code	Code
	Testing	Testing	Testing
	Integration	Integration	Integration
	Data	Data	Data
	Infrastructure	Infrastructure	Infrastructure
	Decision making	Decision making	Decision making

Don't overinvest in one area: Eliminate all dependencies

Coding isn't the only place to worry about dependencies. Dependencies also crop up in testing, integration, data, infrastructure and decision making. By the latter, we mean who must sign off on the implementation of new business capabilities—the team chartered to build and enhance them, or senior management. If, after the capabilities are developed, senior management must approve them before they are put into the marketplace, you can bet it will take those new capabilities a long time to come to market.

These kinds of dependencies, across all six aspects of a new piece of software, have slowed companies down for years. Such dependencies are a feature, in effect, of earlier approaches to enterprise architecture. They are what forced big technology changes to be made only periodically.

In monolithic architectures, all six elements of the software stack were tightly coupled. The code base of different modules was tightly coupled, requiring time-consuming dependency checks. Installing new software depended on the schedules of software testers and resource. Even when developers decoupled software functionality, they often coupled in data. That created dependencies. And when they intended to decouple the integration layer from applications, teams still too often hardwired business logic into the ESB, also creating dependencies. When software was ready to put into production, the handover from the development team to the infrastructure team often slowed things down. They were now working on the production team's schedule, competing against a long queue of software releases. Perhaps most importantly, awaiting senior management approval for a new software system or functionality upgrade before it went into production could set things back by weeks. This is the decision-making dependency.

To be sure, the past decade's movement toward services-oriented architectures (SOA) was a big advance: decoupling code from the other five elements. It helped companies design web services around specific business capabilities. Yet in most companies we know, the testing, integration, data, infrastructure and decision-making activities remained tightly coupled. That was why a new web service could take weeks or months before a company's top management approved it, IT production tested it, and rolled it into the field.

In creating web services or what is also called microservices, companies must make sure each service is independent of any others, and independent of any piece in the IT stack. In fact, their ultimate goal should be just that, rather than to create a focused service.

Set boundaries in technology (not on paper)

IT architects have often been stereotyped as "people drawing funny boxes in charts." For their part, software developers have been viewed as the people to write for the code for the modules that those "funny boxes" represent. Unfortunately, this division of labor has all too often led to both groups operating in their own worlds rather than working closely together.

A company that wants to be digitally competitive will need enterprise architects more than ever. However, they no longer can maintain an arm's-length relationship with developers. They must work closely with them to make sure the architectural rules of Perpetual Evolution™—not just the code—are written into software.

That means the architects need to be part of the teams focused on a business capability or group of related capabilities. They will find themselves working alongside product managers, developers, marketers, testers, production people, legal help and others.

Make sure capability teams have freedom (by strict separation from the platform)

The teams working on specific business capabilities must not have to worry about whether their improvements affect their company's underlying technology platform.

Every company has a part of their IT architecture that they manage as a platform, and (increasingly) other parts that are organized by business capabilities (e.g., web or microservices). To shift to a perpetual evolution architecture, they must draw explicit boundaries between these two parts of the asset base. Then they must enforce those boundaries through strict oversight and other governance processes.

Because a company's digital business capabilities are what enable it to make rapid changes in digitally-based products and business processes, we believe IT professionals must shift their focus along these lines as well. To start, that would mean defining the parts of the IT platform in terms of the business capabilities they support (e.g., customer management), rather than as technologies. For example, defining an IT capability as "service integration" will help a company identify the technologies in the organization with comparable functionality. But it will do more— help the company create more meaningful roles such as service integration architect, rather than integration product XYZ architect.

Regard the platform as one that will continuously change

By separating the boundaries between business capabilities and technology platforms, companies will be able to isolate the fast-moving parts of their infrastructure (the business capabilities) from the slower-moving ones (the platforms). Nonetheless, they can't ignore the need to continuously improve their platforms. Companies must make sure they can update pieces of their platforms continuously as well. Crucial advances in platforms can provide key performance improvements. Capitalizing on them requires a platform whose parts are modular, decoupled and organized for reuse.

And only when the pieces of that platform are defined as business capabilities will companies be able to quickly plug in improvements to them, or whole new capabilities.

———————

In nearly every industry, companies have found they need continuous innovation in their digital products and services, and the business processes that support them. Those that can achieve this will stay competitive in a world in which providing a great customer experience has become paramount.

But to do so, companies must abandon their enterprise architecture practices of the past and adopt a new one that enables perpetual evolution in their digital business processes. Those that do this well will take a big step forward in keeping pace with those digital-native companies that have been attacking their businesses.

This article was originally published on McKinsey.com in February 2017.

Oliver Bossert is a senior expert in McKinsey's Frankfurt office. **Jürgen Laartz** is a senior partner in the Berlin office.

IT modernization in insurance: Three paths to transformation

Insurance companies can reap significant benefits from overhauling their core IT systems. Deciding which approach to choose depends on a range of considerations.

by Krish Krishnakanthan, Jens Lansing, Björn Münstermann, Peter Braad Olesen, and Ulrike Vogelgesang

The insurance industry increasingly relies on digital technology to develop products, assess claims, and—most importantly—provide customers with a satisfying experience. In today's world, IT has become an integral production factor, and the booming insurtech wave has given companies a glimpse of what cutting-edge digital technologies can offer.[1] Therefore, IT capabilities will need to fundamentally change as well; for example, costs must be driven down through procurement and vendor management, application development and maintenance optimized, and IT positioned as a strategic partner.[2]

And yet a startling number of application landscapes across the industry continue to rely on decades-old technologies. Furthermore, as industry players have pursued consolidation for years, the IT back end has not followed suit. This inattention has left most large insurers with parallel or redundant systems that drive up the cost of both maintenance and new feature development. In addition, quite a few insurers have decided to focus their IT investments on selective new front-end tools with immediately visible impact.

As digitization accelerates and encompasses an ever-wider share of the insurance value chain, an improvement on the front end alone is not enough. Achieving the full benefits of digitization requires real-time data access as well as agile features development in core systems. To enable this vision, most insurers must substantially overhaul their core systems and, in conjunction, transform their overall business model. Three options can help companies achieve this goal: modernizing a legacy IT platform, building a new proprietary platform, or buying a standard software package. While each has pros and cons, choosing the right path based on a cost-benefit analysis is critical for delivering on IT modernization and subsequently reaping the benefits.

The value at stake

Insurance companies can capture three primary areas of value by transforming their business model and modernizing their core IT systems (Exhibit 1).

— *Increased gross written premiums and reduced churn.* Flexible, digitized product systems enable insurers to revamp their product innovation process, often resulting in a faster time to market for rate changes and new products.[3] Likewise, digitally enabled integration capabilities can facilitate a more satisfying front-end user experience and increased support for agency and broker sales processes—a key driver of sales. All told, improved and faster processes enhance the customer experience and reduce churn, for which insurers have seen premium increases from 0.5 to 1.0 percent in P&C. Similar effects have also been observed in life insurance.

— *Increased operations productivity.* The productivity benefits stretch beyond IT. Indeed, the disruption of introducing a new core system often motivates insurers to overhaul their operations setups and adapt workflow mechanisms, thereby improving work organization. Our Insurance 360° benchmark shows that players with modernized IT are substantially more productive than their peers with legacy IT systems—for example, the total number of policies per full-time equivalent they achieve is more than 40 percent higher.

— *Reduced IT cost.* Once implemented, modern IT systems can substantially reduce the cost of IT core systems by, for instance, running on commodity hardware versus the mainframe systems used today by many insurers. Our Insurance 360° benchmark shows that IT costs per policy for players with modernized IT can

[1] For more on insurtechs, see Peter Braad Olesen, Ari Chester, Scott Ham, and Sylvain Johansson, "Commercial lines insurtech: A pathway to digital," October 2018, McKinsey.com.
[2] Krish Krishnakanthan, Jens Lansing, Markus Löffler, and Björn Münstermann, "Modernizing IT for a strategic role," March 2017, McKinsey.com.
[3] For more on opportunities to streamline product innovation, see Melissa Dalrymple, Mei Dong, Kweilin Ellingrud, Daniel Garza, Gary Herzberg, Brad Mendelson, Jörg Mußhoff, and Jason Ralph, "Life insurance product innovation: What insurers can learn from leading tech and consumer companies," January 2019, McKinsey.com.

Exhibit 1

New core systems can reduce overall costs.

Median of select P&C players[1]
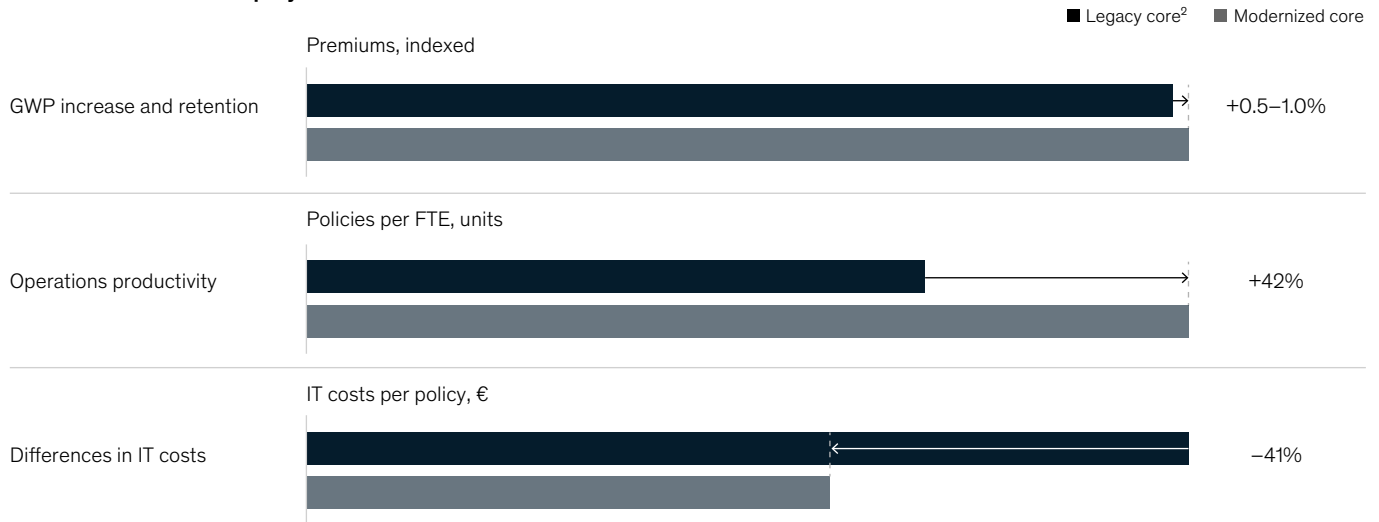
■ Legacy core[2]   ■ Modernized core

Premiums, indexed

GWP increase and retention   +0.5–1.0%

Policies per FTE, units

Operations productivity   +42%

IT costs per policy, €

Differences in IT costs   −41%

[1] McKinsey insurance cost benchmark. Median of select P&C players in Western European peer group, enhanced by insights from client cost benchmarks/expert interviews (2016 year-end analysis).
[2] "Legacy" refers to systems that are old, outdated, and usually running parallel across different areas. Each insurers' system was classified as 1) old but stable and functionally sufficient, 2) legacy IT, 3) currently in modernization/replacement, and 4) recently modernized. Only legacy IT and recently modernized were used for the above analyses.

Source: sanitized case examples; McKinsey Value Assurance research

be 41 percent lower than that of players with legacy IT systems. Still, some players struggle to realize these potential savings, partly because of a lack of decommissioning of old systems and partly because of overly complex configurations and challenges in project management.[4]

In addition to these benefits, IT modernization can also lower loss-adjustment expenses through automation and increased accuracy of claims handling—for example, by connecting policy and claims systems to better match policy clauses and covers with claim events. Of course, the extent to which an insurer can take advantage of these benefits depends on its starting position and how

well it can realize the full potential of these systems through product rationalization and organizational and process changes. As a result, many insurance companies that have embarked on a journey to modernize IT have experienced growing pains.

Insurers too often treat systems transformations as IT projects rather than acknowledging them for what they are: overall business transformations. This shortsightedness can result in rebuilding old functionalities within the new systems, often leading to budget overruns and—more importantly—wasted opportunities to modernize. Indeed, modernizing core IT systems could have ripple effects throughout the organization, requiring insurers to consider how they must adapt their operating model in response.

[4] For more on transitioning to standard software, see Sanjay Kaniyar, Peter Peters, and Ulrike Vogelgesang, "Transitioning to standard software: Lessons from ERP pioneers," May 2015, McKinsey.com.

Successful programs follow an integrated transformation approach that combines a radical rethinking of the business model, with transformation from the customer and IT perspective. The key to such an approach is simplicity at the core, and results can include measurable efficiency, effectiveness, customer satisfaction, and sustainable improvements. One drawback, however, is that intensive transformation can place high demands on internal resources and skills. Still, success is more likely than merely following business-side improvements, which do not resolve the root causes of legacy complexity—many of which will only increase over time.

Three approaches to core system modernization

Within the overall complexity of internal capabilities and external trends, the question arises of how to best shape integrated business and IT transformation. Answering that question begins with understanding three modernization options for insurers' core systems: modernizing the legacy platform, building a proprietary platform, or buying a standard software package (Exhibit 2).

Deciding which modernization approach to take depends on a range of considerations, including the state and stability of the legacy system, level of an insurer's ambition, availability of a mature standard solution for the market, effectiveness of IT capabilities, and amount of available resources.

In our experience, insurance companies that have low internal IT capabilities yet hope to benefit from market standards for IT, products, and processes usually benefit most from buying a standard software package. Of course, there are exceptions. Some insurers—such as those with idiosyncratic requirements or strong beliefs in the differentiating nature of a core insurance system— might choose to build a new platform using either prebuilt components or parts of a preexisting landscape. Similarly, insurers with relatively stable, well-maintained, and incrementally modernized systems that still rely on outdated technologies might choose to modify their existing platform and upgrade other components of the architecture, such as the integration layer, to capture the sought-after business value.

Exhibit 2

Insurers must carefully evaluate which IT modernization approach works with their operating models.

Potential approaches	Results
(1) **Modernizing the legacy platform**	• Ownership of system (at lowest total cost) • Low-risk, mature technology • Functionality can be gradually enhanced
(2) **Building a proprietary platform**	• Can be designed and built (with sufficient internal skills) • Differentiating capabilities (in-house or with sufficient scale) • Long-term implantation possible
(3) **Buying a standard software package**	• Sufficient functional coverage and capabilities • Adequately low total cost of ownership • Manageable integration • Relatively short implementation time

Modernizing the legacy platform

Insurers with legacy IT platforms that are functionally adequate but technologically near the end of their lives have limited options to modernize. Some consider "refactoring," which involves altering a system's internal structure without modifying its functionality. This process allows the insurer to upgrade to modern technology while retaining features tailored to its specific business needs.

For example, one large Northern European P&C insurer had a stable and well-performing claims system, but it was based on outdated technology and architecture incapable of supporting advanced digital technology. To future-proof the architecture and lower IT costs, the company decided on a refactoring approach that consisted of a 1:1 code migration using a combination of automated migration and manual recoding.

Still, refactoring has two drawbacks. First, a 1:1 code migration can result in a missed opportunity for modern system integration and data architecture that supports digital requirements. Second, some insurers have seen costs for this approach grow substantially higher than anticipated. This is partly because the code transversion often cannot be automated as initially planned and partly because the refactored code structurally lacks the architectural advantages of modern programming languages. Furthermore, any future changes will be complex and time-consuming.

To address these challenges, some insurers use a somewhat different approach of "blackboxing" the modernization. In this approach, insurers expose core insurance functionality as services to the outside while carving out functionality from the legacy systems on the inside by either building it from scratch or implementing current technology. Thus, the core back-end systems are slowly modernized. While this approach can be appealing from a risk and cost perspective, it is only a viable longer-term solution if the existing core systems have been well-maintained, documented, stable, and well-performing and if the insurer has ongoing access to the necessary maintenance skills.

Building a proprietary platform

In the early days of computer technology, building a new proprietary platform was the only approach for insurers. This typically involved building a system architecture that perfectly fit the unique requirements of the insurer and then seamlessly integrating it into the remaining landscape.

Some incumbent insurers continue to take this route. For example, a European life insurer developed a new, proprietary web-based platform to serve as the foundation for its digital strategy. This approach allowed the insurer to tailor the platform to its local offerings and gradually implement them, starting with individual life—the result was a 30 percent reduction in administrative costs. As another example, a large North American complex commercial and specialty insurer opted for a custom-built approach to enable new end-to-end underwriting and policy administration capabilities. The decision was based on a lack of relevant external offerings and a lack of access to the latest technologies and architectures. Executives therefore chose to build a data-centric architecture with strong analytical capabilities, which was necessary to handle complex commercial lines underwriting flows.

Numerous insurtechs have also taken this approach because they believed in the differentiating nature of a strong core system and a reliance on technical frameworks as foundations upon which to build their own platforms. However, in contrast to incumbent insurers, insurtechs do not have a legacy system to address or modernize.

The drawbacks of building a proprietary platform tend to include higher costs, longer timelines, and additional risks compared with modernizing a legacy platform or buying a software package. This approach can lead to an extended functionality freeze

during the programming phase, which poses a core challenge. Furthermore, new solutions pose the risk of being insufficiently innovative. This can be because of lacking creative and appropriately skilled internal talent or large-scale IT project delivery capabilities; projects can also get bogged down in delivering must-have but nondifferentiating features.

Buying a standard software package

Standard software packages have become increasingly appealing to many insurers looking to overhaul their core systems. Standard systems are typically much more streamlined and include ready-made functionality for pricing, underwriting, customer self-service and automation, and claims processing. As a result, they can improve efficiency across the enterprise. Broadly speaking, a standard software package promises the following key benefits:

— Faster and less risky implementations compared with modernizing or building a new proprietary platform
— Best-practice functionalities and regular upgrades that include product and process innovations as well as regulatory requirements
— Cost benefits from shared development between multiple insurers
— Access to a pool of skilled resources outside the insurance company

While all these benefits combined can't always be realized, the appeal of standard core insurance software remains strong. In the United States, for example, nine of the top 12 P&C insurers use standard software for claims and policy administration. Standard software is similarly popular in Central and Eastern Europe, the Nordics, and the United Kingdom. Regions where the use of standard software is less consistent include some parts of Western Europe. In Germany, for example, standard software has been gaining ground in life insurance, with a couple of relatively mature systems emerging, while adoption on the P&C side has been slower. Though the market momentum in this region remains moderate, a clear trend of more insurers using standard software each year has emerged.[5]

One European insurance company gained the ability to change ratings and pricing on a weekly basis by implementing a standard software package for several P&C products. This standard software package could also reduce the time to market for new products from months to days and substantially reduce training times for sales agents. These functional improvements went along with an overall lower total cost of ownership.

While standard packages are gaining momentum, challenges remain for insurers that choose to take this approach. The software package must fit the insurer, and its implementation must focus on adopting rather than adapting to the standard software. For many insurance carriers, this implies a significant cultural transformation on the business side, evolving from an "anything goes" attitude to a "simplicity first" mindset on the IT side—from coding a new solution to configuring an existing solution. Otherwise, the implementation of standard software could prove costly and result in a long timeline and lower-than-expected benefits. Furthermore, the insurer can develop a dependency on an external vendor and its software product road map, which could curtail flexibility and increase costs.

Choosing the right path

Each path to IT modernization has different pros and cons. In addition to choosing between the three fundamental options described above, the timing and extent of existing policies migration need to be considered. While the majority of insurers

---

[5] For more details on managing the transition to standard software, see Kaniyar, Peters, and Vogelgesang, "Transitioning to standard software."

develop a platform for both their existing and new business, some carriers opt to start with a greenfield implementation specifically for the new business that would provide an option to migrate the existing business later.[6]

Choosing the right path depends on several important factors, including starting point, transformation preferences, capabilities, and business-model objectives. Leaders should ask themselves tough questions when considering the health of current core systems, investment ability and appetite, business and IT capabilities, and the true extent of the organization's digital ambitions.

Insurers must overhaul their core IT systems to achieve the full benefits of a digital transformation. Given the digital advances in insurance—especially in personal lines—transforming the core is the next frontier. Combining core and business transformation, through an appropriate and considered approach, can yield significant IT modernization benefits.

---

[6] For more on next-generation banking systems, see *Banking & Securities matters,* "Next-generation core banking platforms: A golden ticket?," blog entry by Brian Ledbetter, Xavier Lhuer, Sandhosh Kumar, and Philip Tuddenham, August 12, 2019, McKinsey.com.

This article was originally published on McKinsey.com in November 2019.

Krish Krishnakanthan is a senior partner in McKinsey's Stamford office, **Jens Lansing** is an associate partner in the Dusseldorf office, **Björn Münstermann** is a partner in the Munich office, **Peter Braad Olesen** is an associate partner in the Copenhagen office, and **Ulrike Vogelgesang** is a senior expert in the Hamburg office.
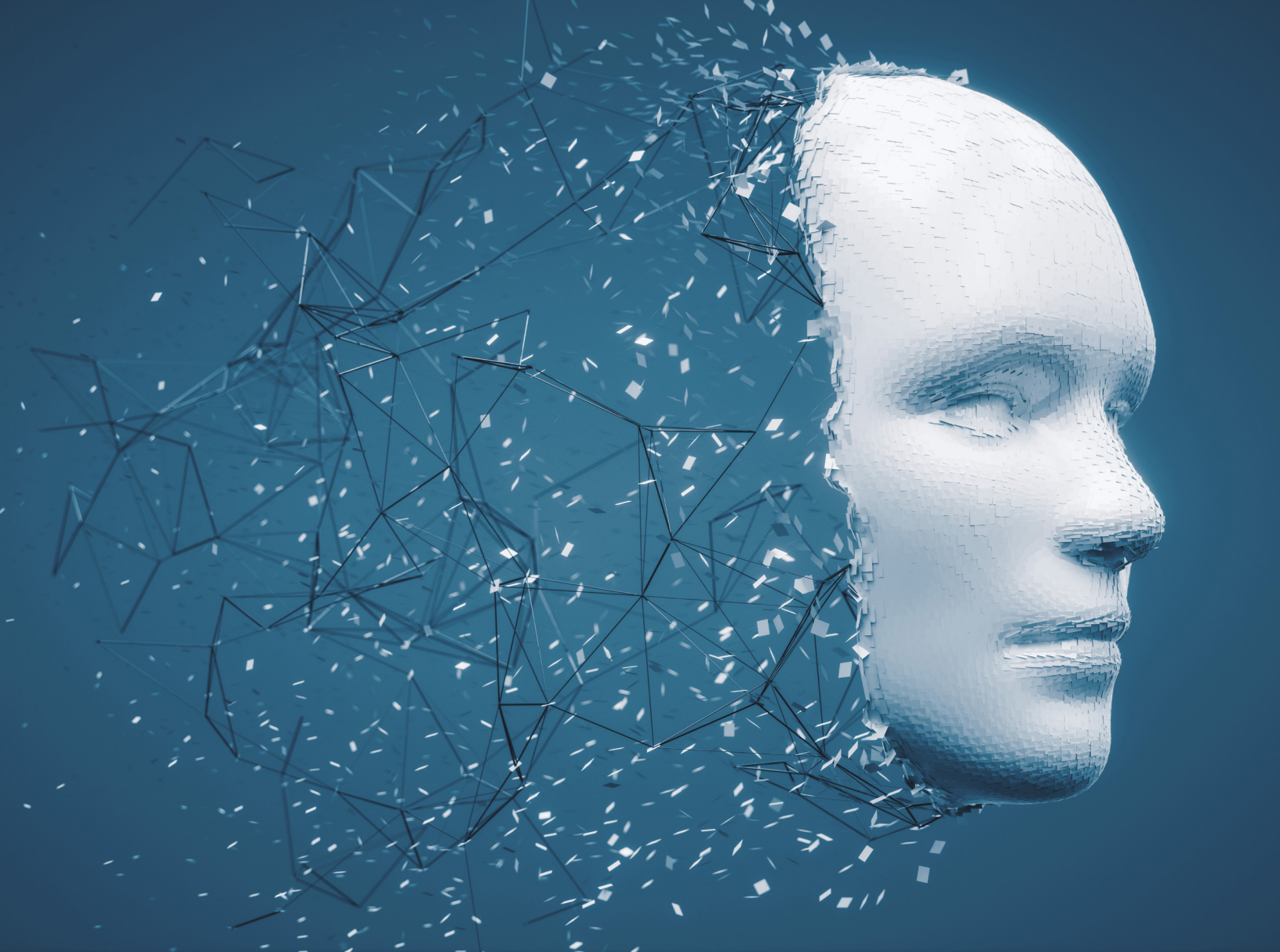
© Chad Baker/Getty Images

Insurance 2030—
The impact of AI on the future of insurance

The industry is on the verge of a seismic, tech-driven shift. A focus on four areas can position carriers to embrace this change.

by Ramnath Balasubramanian, Ari Libarikian, and Doug McElhaney

Welcome to the future of insurance, as seen through the eyes of Scott, a customer in the year 2030. His digital personal assistant orders him a vehicle with self-driving capabilities for a meeting across town. Upon hopping into the arriving car, Scott decides he wants to drive today and moves the car into "active" mode. Scott's personal assistant maps out a potential route and shares it with his mobility insurer, which immediately responds with an alternate route that has a much lower likelihood of accidents and auto damage as well as the calculated adjustment to his monthly premium. Scott's assistant notifies him that his mobility insurance premium will increase by 4 to 8 percent based on the route he selects and the volume and distribution of other cars on the road. It also alerts him that his life insurance policy, which is now priced on a "pay-as-you-live" basis, will increase by 2 percent for this quarter. The additional amounts are automatically debited from his bank account.

When Scott pulls into his destination's parking lot, his car bumps into one of several parking signs. As soon as the car stops moving, its internal diagnostics determine the extent of the damage. His personal assistant instructs him to take three pictures of the front right bumper area and two of the surroundings. By the time Scott gets back to the driver's seat, the screen on the dash informs him of the damage, confirms the claim has been approved, and reports that a mobile response drone has been dispatched to the lot for inspection. If the vehicle is drivable, it may be directed to the nearest in-network garage for repair after a replacement vehicle arrives.

While this scenario may seem beyond the horizon, such integrated user stories will emerge across all lines of insurance with increasing frequency over the next decade. In fact, all the technologies required above already exist, and many are available to consumers. With the new wave of deep learning techniques, such as convolutional neural networks,[1] artificial intelligence (AI) has the potential to live up to its promise of mimicking the perception, reasoning, learning, and problem solving of the human mind (Exhibit 1). In this evolution, insurance

will shift from its current state of "detect and repair" to "predict and prevent," transforming every aspect of the industry in the process. The pace of change will also accelerate as brokers, consumers, financial intermediaries, insurers, and suppliers become more adept at using advanced technologies to enhance decision making and productivity, lower costs, and optimize the customer experience.

As AI becomes more deeply integrated in the industry, carriers must position themselves to respond to the changing business landscape. Insurance executives must understand the factors that will contribute to this change and how AI will reshape claims, distribution, and underwriting and pricing. With this understanding, they can start to build the skills and talent, embrace the emerging technologies, and create the culture and perspective needed to be successful players in the insurance industry of the future.

Four AI-related trends shaping insurance

AI's underlying technologies are already being deployed in our businesses, homes, and vehicles, as well as on our person. The disruption from COVID-19 changed the timelines for the adoption of AI by significantly accelerating digitization for insurers. Virtually overnight, organizations had to adjust to accommodate remote workforces, expand their digital capabilities to support distribution, and upgrade their online channels. While most organizations likely didn't invest heavily in AI during the pandemic, the increased emphasis on digital technologies and a greater willingness to embrace change will put them in a better position to incorporate AI into their operations.

Four core technology trends, tightly coupled with (and sometimes enabled by) AI, will reshape the insurance industry over the next decade.

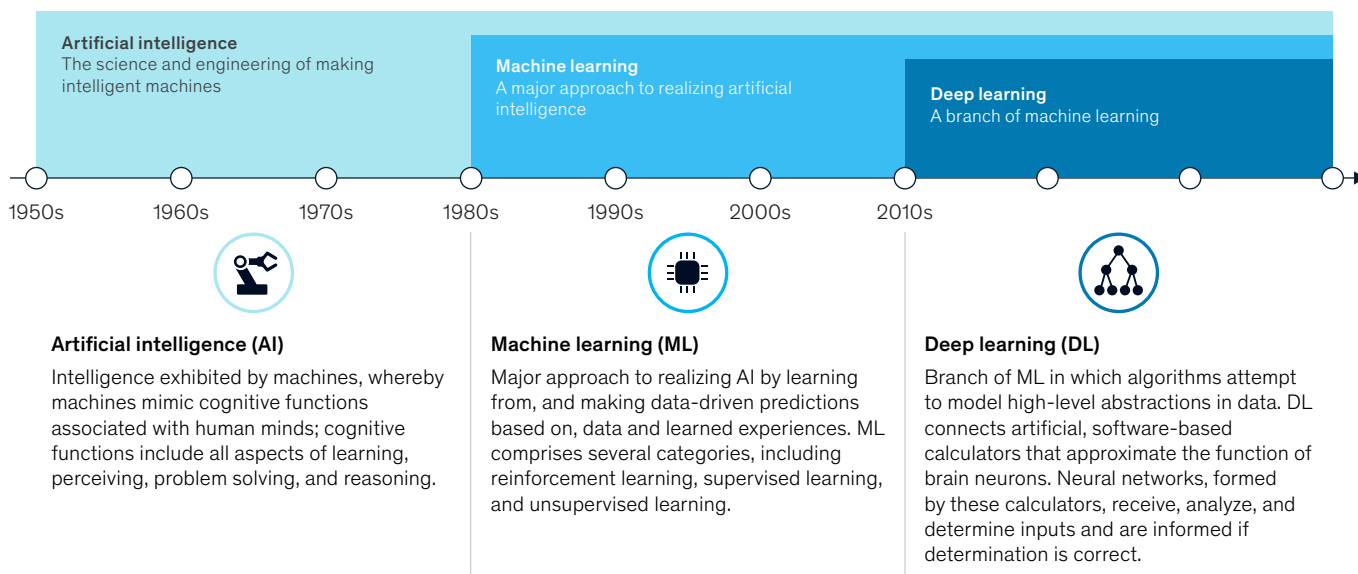### Explosion of data from connected devices
In industrial settings, equipment with sensors have been omnipresent for some time, but the coming years will see a huge increase in the number of connected consumer devices. The penetration

---

[1] Convolutional neural networks contain millions of simulated "neurons" structured in layers.

Exhibit 1

Artificial intelligence can deliver on industry expectations through machine learning and deep learning.

Artificial intelligence
The science and engineering of making intelligent machines

Machine learning
A major approach to realizing artificial intelligence

Deep learning
A branch of machine learning

1950s   1960s   1970s   1980s   1990s   2000s   2010s

Artificial intelligence (AI)
Intelligence exhibited by machines, whereby machines mimic cognitive functions associated with human minds; cognitive functions include all aspects of learning, perceiving, problem solving, and reasoning.

Machine learning (ML)
Major approach to realizing AI by learning from, and making data-driven predictions based on, data and learned experiences. ML comprises several categories, including reinforcement learning, supervised learning, and unsupervised learning.

Deep learning (DL)
Branch of ML in which algorithms attempt to model high-level abstractions in data. DL connects artificial, software-based calculators that approximate the function of brain neurons. Neural networks, formed by these calculators, receive, analyze, and determine inputs and are informed if determination is correct.

Source: Nvidia; Rockwell Anyoha, "The history of artificial intelligence," *Science in the News,* August 28, 2017, sitn.hms.harvard.edu

of existing devices (such as cars, fitness trackers, home assistants, smartphones, and smart watches) will continue to increase rapidly, joined by new, growing categories such as clothing, eyewear, home appliances, medical devices, and shoes. Experts estimate there will be up to one trillion connected devices by 2025.[2] The resulting avalanche of new data created by these devices will allow carriers to understand their clients more deeply, resulting in new product categories, more personalized pricing, and increasingly real-time service delivery. For example, a wearable that is connected to an actuarial database could calculate a consumer's personal risk score based on daily activities as well as the probability and severity of potential events.

Increased prevalence of physical robotics
The field of robotics has seen many exciting achievements recently, and this innovation will continue to change how humans interact with the world around them. Additive manufacturing, also known as 3-D printing, will radically reshape manufacturing and the commercial insurance products of the future. By 2025, 3-D-printed

buildings will be common, and carriers will need to assess how this development changes risk assessments. In addition, programmable, autonomous drones; autonomous farming equipment; and enhanced surgical robots will all be commercially viable in the next decade. By 2030, a much larger proportion of standard vehicles will have autonomous features, such as self-driving capabilities. Carriers will need to understand how the increasing presence of robotics in everyday life and across industries will shift risk pools, change customer expectations, and enable new products and channels.

Open-source and data ecosystems
As data becomes ubiquitous, open-source protocols will emerge to ensure data can be shared and used across industries. Various public and private entities will come together to create ecosystems in order to share data for multiple use cases under a common regulatory and cybersecurity framework. For example, wearable data could be ported directly to insurance carriers, and connected-home and auto data could be made available through Amazon,

[2]World Economic Forum, 2015.

Experts estimate there will be up to one trillion connected devices by 2025.

Apple, Google, and a variety of consumer device manufacturers.

Advances in cognitive technologies

Convolutional neural networks and other deep learning technologies currently used primarily for image, voice, and unstructured text processing will evolve to be applied in a wide variety of applications. These cognitive technologies, which are loosely based on the human brain's ability to learn through decomposition and inference, will become the standard approach for processing the incredibly large and complex data streams that will be generated by "active" insurance products tied to an individual's behavior and activities. With the increased commercialization of these types of technologies, carriers will have access to models that are constantly learning and adapting to the world around them—enabling new product categories and engagement techniques while responding to shifts in underlying risks or behaviors in real time.

The state of insurance in 2030

AI and its related technologies will have a seismic impact on all aspects of the insurance industry, from distribution to underwriting and pricing to claims. Advanced technologies and data are already affecting distribution and underwriting, with policies being priced, purchased, and bound in near real time. An in-depth examination at what insurance may look like in 2030 highlights dramatic changes across the insurance value chain.

Distribution

The experience of purchasing insurance is faster, with less active involvement on the part of the insurer and the customer.[3] Enough information is known about individual behavior, with AI algorithms creating risk profiles, so that cycle times for

completing the purchase of an auto, commercial, or life policy will be reduced to minutes or even seconds. Auto and home carriers have enabled instant quotes for some time but will continue to refine their ability to issue policies immediately to a wider range of customers as telematics and in-home Internet of Things (IoT) devices proliferate and pricing algorithms mature. Many life carriers are experimenting with simplified issue products, but most are restricted to only the healthiest applicants and are priced higher than a comparable fully underwritten product. As AI permeates life underwriting and carriers are able to identify risk in a much more granular and sophisticated way, we will see a new wave of mass-market instant issue products.

Smart contracts enabled by blockchain instantaneously authorize payments from a customer's financial account. Meanwhile, contract processing and payment verification are eliminated or streamlined, reducing customer acquisition costs for insurers. The purchase of commercial insurance is similarly expedited as the combination of drones, the IoT, and other available data provides sufficient information for AI-based cognitive models to proactively generate a bindable quote.

Highly dynamic, usage-based insurance (UBI) products proliferate and are tailored to the behavior of individual consumers. Insurance transitions from a "purchase and annual renewal" model to a continuous cycle, as product offerings constantly adapt to an individual's behavioral patterns. Furthermore, products are disaggregated substantially into microcoverage elements (for example, phone battery insurance, flight delay insurance, different coverage for a washer and dryer within the home) that consumers can customize to their particular needs, with the ability to instantaneously compare prices from

---

[3] Simon Kaesler, Matt Leo, Shannon Varney, and Kaitlyn Young, "How insurance can prepare for the next distribution model," June 12, 2020, McKinsey.com.

various carriers for their individualized baskets of insurance products. New products emerge to cover the shifting nature of living arrangements and travel. UBI becomes the norm as physical assets are shared across multiple parties, with a pay-by-mile or pay-by-ride model for car sharing and pay-by-stay insurance for home-sharing services, such as Airbnb.[4]

The role of insurance agents has changed dramatically by 2030. The number of agents is reduced substantially as active agents retire and remaining agents rely heavily on technology to increase productivity. The role of agents transitions to process facilitators and product educators. The agent of the future can sell nearly all types of coverage and adds value by helping clients manage their portfolios of coverage across experiences, health, life, mobility, personal property, and residential. Agents use smart personal assistants to optimize their tasks as well as AI-enabled bots to find potential deals for clients. These tools help agents to support a substantially larger client base while making customer interactions (a mix of in-person, virtual, and digital) shorter and more meaningful, given that each interaction will be tailored to the exact current and future needs of each individual client.

Underwriting and pricing

In 2030, underwriting as we know it today ceases to exist for most personal and small-business products across life and property and casualty insurance.[5] The process of underwriting is reduced to a few seconds as the majority of underwriting is automated and supported by a combination of machine and deep learning models built within the technology stack. These models are powered by internal data as well as a broad set of external data accessed through application programming interfaces and outside data and analytics providers. Information collected from devices provided by mainline carriers, reinsurers, product manufacturers, and product distributors is aggregated in a variety of data repositories and data streams. These

information sources enable insurers to make ex ante decisions regarding underwriting and pricing, enabling proactive outreach with a bindable quote for a product bundle tailored to the buyer's risk profile and coverage needs.

Regulators review AI-enabled, machine learning–based models, a task that requires a transparent method for determining traceability of a score (similar to the rating factor derivations used today with regression-based coefficients). To verify that data usage is appropriate for marketing and underwriting, regulators assess a combination of model inputs. They also develop test policies for providers when determining rates in online plans to ensure the algorithm results are within approved bounds. Public policy considerations limit access to certain sensitive and predictive data (such as health and genetic information) that would decrease underwriting and pricing flexibility and increase antiselection risk in some segments.

Price remains central in consumer decision making, but carriers innovate to diminish competition purely on price. Sophisticated proprietary platforms connect customers and insurers and offer customers differentiated experiences, features, and value. In some segments, price competition intensifies, and razor-thin margins are the norm, while in other segments, unique insurance offerings enable margin expansion and differentiation. In jurisdictions where change is embraced, the pace of pricing innovation is rapid. Pricing is available in real time based on usage and a dynamic, data-rich assessment of risk, empowering consumers to make decisions about how their actions influence coverage, insurability, and pricing.

Claims

Claims processing in 2030 remains a primary function of carriers, but more than half of claims activities have been replaced by automation.[6] Advanced algorithms handle initial claims routing, increasing efficiency and accuracy.

---

[4] Some insurtech companies are already designing these types of products; Slice, for example, provides variable commercial insurance specifically tailored for home sharing.

[5] Ramnath Balasubramanian, Ari Chester, and Nick Milinkovich, "Rewriting the rules: Digital and AI-powered underwriting in life insurance," July 31, 2020, McKinsey.com.

[6] Andy Fong, Kristen Ganjani, Elixabete Larrea, and José Miguel Novo Sánchez, "Claims 2030: A talent strategy for the future of insurance claims," December 10, 2020, McKinsey.com.

IoT sensors and an array of data-capture technologies, such as drones, largely replace traditional, manual methods of first notice of loss. Claims triage and repair services are often triggered automatically upon loss. In the case of an auto accident, for example, a policyholder takes streaming video of the damage, which is translated into loss descriptions and estimate amounts. Vehicles with autonomous features that sustain minor damage direct themselves to repair shops for service while another car with autonomous features is dispatched in the interim. In the home, IoT devices will be increasingly used to proactively monitor water levels, temperature, and other key risk factors and will proactively alert both tenants and insurers of issues before they arise.

Automated customer service apps handle most policyholder interactions through voice and text, directly following self-learning scripts that interface with the claims, fraud, medical service, policy, and repair systems. The turnaround time for resolution of many claims is measured in minutes rather than days or weeks. Human claims management focuses on a few areas: complex and unusual claims, contested claims where human interaction and negotiation are empowered by analytics and data-driven insights, claims linked to systemic issues and risks created by new technology (for example, hackers infiltrate critical IoT systems), and random manual reviews of claims to ensure sufficient oversight of algorithmic decision making.

Claims organizations increase their focus on risk monitoring, prevention, and mitigation. The IoT and new data sources are used to monitor risk and trigger interventions when factors exceed AI-defined thresholds. Customer interaction with insurance claims organizations focuses on avoiding potential loss. Individuals receive real-time alerts that may be linked with automatic interventions for inspection, maintenance, and repair. For large-scale catastrophe claims, insurers monitor homes and vehicles in real time using the integrated IoT, telematics, and mobile phone data, assuming mobile phone service and power haven't been disrupted in the area. When power goes out, insurers can profile claims by using data aggregators, which consolidate

data from satellites, networked drones, weather services, and policyholder data in real time. This system is pretested by the largest carriers across multiple catastrophe types, so highly accurate loss estimations are reliably filed in a real emergency. Detailed reports are automatically provided to reinsurers for faster reinsurance capital flow.

How insurers can prepare for accelerating changes

The rapid evolution of the industry will be fueled by the extensive adoption and integration of automation, deep learning, and external data ecosystems. While no one can predict exactly what insurance might look like in 2030, carriers can take several steps now to prepare for change.

1. Get smart on AI-related technologies and trends

Although the tectonic shifts in the industry will be tech-focused, addressing them is not the domain of the IT team. Instead, board members and customer-experience teams should invest the time and resources to build a deep understanding of these AI-related technologies. Part of this effort will require exploring hypothesis-driven scenarios in order to understand and highlight where and when disruption might occur—and what it means for certain business lines. For example, insurers are unlikely to gain much insights from limited-scale IoT pilot projects in discrete parts of the business. Instead, they must proceed with purpose and an understanding of how their organization might participate in the IoT ecosystem at scale. Pilots and proof-of-concept (POC) projects should be designed to test not just how a technology works but also how successful the carrier might be operating in a particular role within a data- or IoT-based ecosystem.

2. Develop and begin implementation of a coherent strategic plan

Building on the insights from AI explorations, carriers must decide how to use technology to support their business strategy. The senior leadership team's long-term strategic plan will require a multiyear transformation that touches

operations, talent, and technology. Some carriers are already beginning to take innovative approaches such as starting their own venture-capital arms, acquiring promising insurtech companies, and forging partnerships with leading academic institutions. Insurers should develop a perspective on areas they want to invest in to meet or beat the market and what strategic approach—for example, forming a new entity or building in-house strategic capabilities—is best suited for their organization.

This plan should address all four dimensions involved in any large-scale, analytics-based initiative—everything from data to people to culture (Exhibit 2). The plan should outline a road map of AI-based pilots and POCs and detail which parts of the organization will require investments in skill building or focused change management. Most important, a detailed schedule of milestones and checkpoints is essential to allow the organization to determine, on a regular basis, how the plan should be modified to address any shifts in the evolution of AI technologies and significant changes or disruptions within the industry.

In addition to being able to understand and implement AI technologies, carriers also need to develop strategic responses to coming macrolevel changes. As many lines shift toward a "predict and prevent" methodology, carriers will need to rethink their customer engagement and branding, product design, and core earnings. Auto accidents will be reduced through use of vehicles with self-driving capabilities, in-home flooding will be prevented by IoT devices, buildings will be reprinted after a natural disaster, and lives will be saved and extended by improved healthcare. Likewise, vehicles will still break down, natural disasters will continue to devastate coastal regions, and individuals will require effective medical care and support when a loved one passes. As these changes take root, profit pools will shift, new types and lines of products will emerge, and how consumers interact with their insurers will change substantially.

Winning carriers of the future will create and enact strategic plans that position their brand, products, customer interactions, and technology successfully to take advantage of the new economic structure on the horizon.

Exhibit 2

There are four core elements in defining a successful AI strategy.
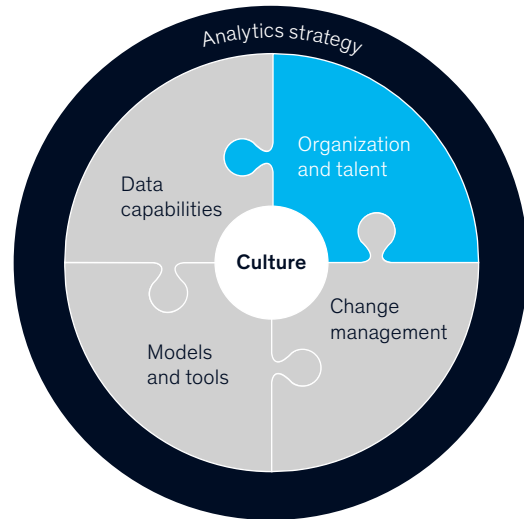
All of these efforts can produce a coherent analytics and technology strategy that addresses all aspects of the business, with a keen eye on both value creation and differentiation.

3. Create and execute a comprehensive data strategy

Data is fast becoming one of the most—if not the most—valuable asset for any organization. The insurance industry is no different: how carriers identify, quantify, place, and manage risk is all predicated on the volume and quality of data they acquire during a policy's life cycle. Most AI technologies will perform best when they have a high volume of data from a variety of sources. As such, carriers must develop a well-structured and actionable strategy with regard to both internal and external data.

Internal data will need to be organized in ways that enable and support the agile development of new analytics insights and capabilities. With external data, carriers must focus on securing access to data that enriches and complements their internal data sets. The real challenge will be gaining access in a cost-efficient way. As the external data ecosystem

continues to expand, it will likely remain highly fragmented, making it quite difficult to identify high-quality data at a reasonable cost. Overall, data strategy will need to include a variety of ways to obtain and secure access to external data, as well as ways to combine this data with internal sources. Carriers should be prepared to have a multifaceted procurement strategy that could include the direct acquisition of data assets and providers, licensing of data sources, use of data APIs, and partnerships with data brokers.

4. Create the right talent and technology infrastructure

In augmented chess, average players enabled by AI tend to do better than expert chess players enabled by the same AI. The underlying reason for this counterintuitive outcome depends on whether the individual interacting with AI embraces, trusts, and understands the supporting technology. To ensure that every part of the organization views advanced analytics as a must-have capability, carriers must make measured but sustained investments in people. The insurance organization of the future will require talent with the right mindsets and skills.[7] The next generation of successful frontline insurance workers will be in increasingly high demand and must possess a unique mix of being technologically adept, creative, and willing to work at something that will not be a static process but rather a mix of semiautomated and machine- supported tasks that continually evolve. Generating value from the AI use cases of the future will require carriers to integrate skills, technology, and insights from around the organization to deliver unique, comprehensive customer experiences. Doing so will require a conscious culture shift for most carriers that will

rely on buy-in and leadership from the executive suite. Developing an aggressive strategy to attract, cultivate, and retain a variety of workers with critical skill sets will be essential to keep pace. These roles will include data engineers, data scientists, technologists, cloud computing specialists, and experience designers. To retain knowledge while also ensuring the business has the new skills and capabilities necessary to compete, many organizations will design and implement reskilling programs. As a last component of developing the new workforce, organizations will identify external resources and partners to augment in-house capabilities that will help carriers secure the needed support for business evolution and execution. The IT architecture of the future will also be radically different from today's. Carriers should start making targeted investments to enable the migration to a more future-forward technology stack that can support a two-speed IT architecture.[8]

———————

Rapid advances in technologies in the next decade will lead to disruptive changes in the insurance industry. The winners in AI-based insurance will be carriers that use new technologies to create innovative products, harness cognitive learning insights from new data sources, streamline processes and lower costs, and exceed customer expectations for individualization and dynamic adaptation. Most important, carriers that adopt a mindset focused on creating opportunities from disruptive technologies—instead of viewing them as a threat to their current business—will thrive in the insurance industry in 2030.

---

[7] Julie Goran, Krish Krishnakanthan, Eleonora Sharef, and Kurt Strovink, "How US insurers can build a winning digital workforce for the future," September 9, 2020, McKinsey.com.
[8] Driek Desmet, Markus Löffler, and Allen Weinberg, "Modernizing IT for a digital era," September 1, 2016, McKinsey.com.

This article was originally published on McKinsey.com in April 2018.

Ramnath Balasubramanian and **Ari Libarikian** are senior partners in McKinsey's New York office, and **Doug McElhaney** is a partner in the Washington, DC, office.

The authors wish to thank Gijs Biermans, Bayard Gennert, Nick Milinkovich, and Erik Summers for their contributions to this article.

Cybersecurity: Linchpin of the digital enterprise

As companies digitize businesses and automate operations, cyberrisks proliferate; here is how the cybersecurity organization can support a secure digital agenda.

by James Kaplan, Wolf Richter, and David Ware

Two consistent and related themes in enterprise technology have emerged in recent years, both involving rapid and dramatic change. One is the rise of the digital enterprise across sectors and internationally. The second is the need for IT to react quickly and develop innovations aggressively to meet the enterprise's digital aspirations. Exhibit 1 presents a "digitization index"—the results of research on the progress of enterprise digitization within companies, encompassing sectors, assets, and operations.

As IT organizations seek to digitize, however, many face significant cybersecurity challenges. At company after company, fundamental tensions arise between the business's need to digitize and the cybersecurity team's responsibility to protect the organization, its employees, and its customers within existing cyber operating models and practices.

If cybersecurity teams are to avoid becoming barriers to digitization and instead become its enablers, they must transform their capabilities along three dimensions. They must improve risk management, applying quantitative risk analytics. They must build cybersecurity directly into businesses' value chains. And they must support the next generation of enterprise-technology platforms, which include innovations like agile development, robotics, and cloud-based operating models.

Cybersecurity's role in digitization

Every aspect of the digital enterprise has important cybersecurity implications. Here are just a few examples. As companies seek to create more digital customer experiences, they need to determine how to align their teams that manage fraud prevention, security, and product development so they can design controls, such as authentication, and create experiences that are both convenient and secure. As companies adopt massive data analytics, they must determine how to identify risks created by data sets that integrate many types of incredibly sensitive customer information. They must also incorporate security controls into analytics solutions

that may not use a formal software-development methodology. As companies apply robotic process automation (RPA), they must manage bot credentials effectively and make sure that "boundary cases"— cases with unexpected or unusual factors, or inputs that are outside normal limits—do not introduce security risks.

Likewise, as companies build application programming interfaces (APIs) for external customers, they must determine how to identify vulnerabilities created by interactions between many APIs and services, and they must build and enforce standards for appropriate developer access.[1] They must continue to maintain rigor in application security as they transition from waterfall to agile application development.

Challenges with existing cybersecurity models

At most companies, chief information officers (CIOs), chief information-security officers (CISOs), and their teams have sought to establish cybersecurity as an enterprise-grade service. What does that mean? They have consolidated cybersecurity-related activities into one or a few organizations. They have tried to identify risks and compare them to enterprise-wide risk appetites to understand gaps and make better decisions about closing them. They have created enterprise-wide policies and supported them with standards. They have established governance as a counterweight to the tendency of development teams to prioritize time to market and cost over risk and security. They have built security service offerings that require development teams to create a ticket requesting service from a central group before they can get a vulnerability scan or a penetration test.

All these actions have proven absolutely necessary to the security of an organization. Without them, cybersecurity breaches occur more frequently—and often, with more severe consequences. The needed actions, however, exist in tension with the emerging digital-enterprise model—the outcome of an end-
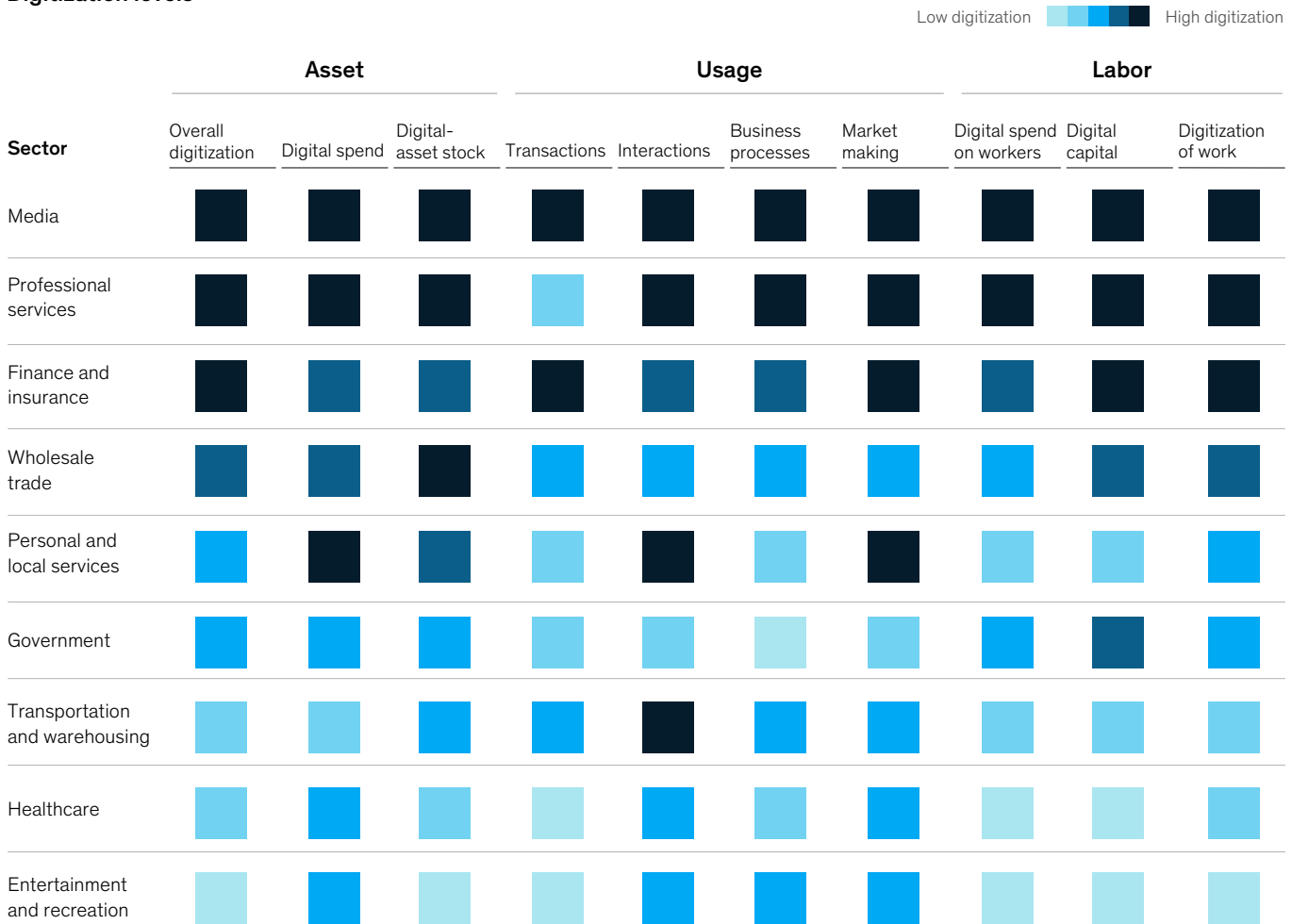
---

[1] An API is software that allows applications to communicate with each other, sharing information for a purpose.

Exhibit 1

Across sectors, companies are digitizing, with profound implications for cybersecurity functions.

Digitization levels

Low digitization ▢▢▢▢ High digitization

Sector	Asset			Usage				Labor		
	Overall digitization	Digital spend	Digital-asset stock	Transactions	Interactions	Business processes	Market making	Digital spend on workers	Digital capital	Digitization of work
Media										
Professional services										
Finance and insurance										
Wholesale trade										
Personal and local services										
Government										
Transportation and warehousing										
Healthcare										
Entertainment and recreation										

Source: Appbrain; Blue Wolf; ContactBabel; eMarketer; Gartner; IDC; LiveChat; US Bureau of Economic Analysis; US Bureau of Labor Statistics; US Census Bureau; Global Payments Map by McKinsey; McKinsey Social Technology Survey; McKinsey analysis; McKinsey Global Institute analysis

to-end digital transformation—from the customer interface through the back-office processes. As companies seek to use public cloud services, they often find that security is the "long pole in the tent"—the most intractable part of the problem of standing applications on public cloud infrastructure.

At one financial institution, development teams were frustrated with the long period needed by the security team to validate and approve

incremental items in their cloud service provider's catalog for production usage. Developers at other companies have puzzled over the fact that they can spin up a server in minutes but must wait weeks for the vulnerability scan required to promote their application to production. IT organizations everywhere are finding that existing security models do not run at "cloud speed" and do not provide enough specialized support to developers on issues like analytics, RPA, and APIs (Exhibit 2).

The misalignment between development and cybersecurity teams leads to missed business opportunities, as new capabilities are delayed in reaching the market. In some cases, the pressure to close the gap has caused increased vulnerability, as development teams bend rules to work around security policies and standards.

Cybersecurity for the digital enterprise

In response to aggressive digitization, some of the world's most sophisticated cybersecurity functions are starting to transform their capabilities along the three dimensions we described: using quantitative risk analytics for decision making,

building cybersecurity into the business value chain, and enabling the new technology operating platforms that combine many innovations. These innovations include agile approaches, robotics, cloud, and DevOps (the combination of software development and IT operations to shorten development times and deliver new features, fixes, and updates aligned with the business).

Using quantitative risk analytics for decision making

At the core of cybersecurity are decisions about which information risks to accept and how to mitigate them. Traditionally, CISOs and

Exhibit 2

Current cybersecurity operating models do not operate at 'cloud speed.'
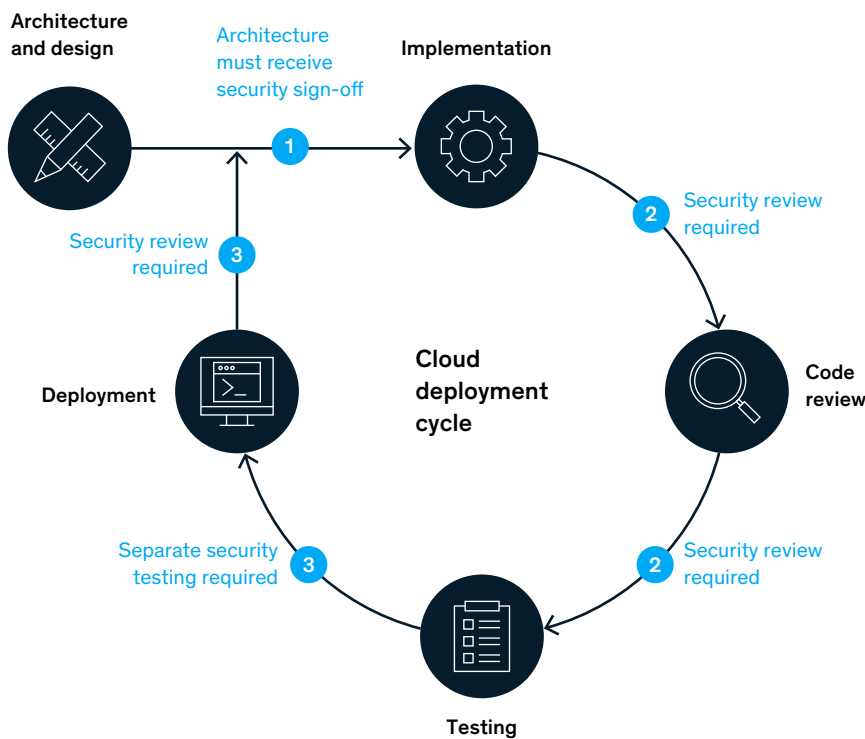
Stage gates

1 Designing secure architecture requires special knowledge

2 Secure code review, test design, and implementation require specially trained developers not available to many teams

3 Cloud environments must be configured to security standards and instrumented with monitoring before deployment into production

Activities

Architecture and design	Implementation	Code review	Testing	Deployment
– Analyze resource availability from cloud service provider – Analyze capacity requirements – Develop initial solution design – Design interfaces	– Instantiate development and testing environments – Begin solution implementation	– Review code – Conduct automated code scanning – Accept code into code base	– Develop test cases – Do continuous testing – Fix bugs and errors; make changes – Do regression testing	– Instantiate cloud infrastructure – Establish cloud services – Deploy production application – Do final testing

their business partners have made cyberrisk-management decisions using a combination of experience, intuition, judgment, and qualitative analysis. In today's digital enterprises, however, the number of assets and processes to protect, and the decreasing practicality and efficacy of one-size-fits-all protections, have dramatically reduced the applicability of traditional decision-making processes and heuristics.

In response, companies are starting to strengthen their business and technology environments with quantitative risk analytics so they can make better, fact-based decisions. This has many aspects. It includes sophisticated employee and contractor segmentation as well as behavioral analysis to identify signs of possible insider threats, such as suspicious patterns of email activity. It also includes risk-based authentication that considers

metadata—such as user location and recent access activity—to determine whether to grant access to critical systems. Ultimately, companies will start to use management dashboards that tie together business assets, threat intelligence, vulnerabilities, and potential mitigation to help senior executives make the best cybersecurity investments. They will be able to focus those investments on areas of the business that will yield the most protection with the least disruption and cost.
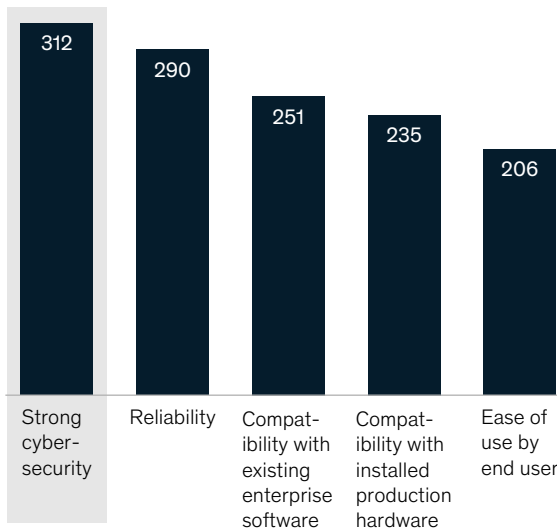
Building cybersecurity into the business value chain

No institution is an island when it comes to cybersecurity. Every company of any complexity exchanges sensitive data and interconnects networks with customers, suppliers, and other business partners. As a result, cybersecurity-related questions of trust and the burden of mitigating protections have become central to value chains in many sectors. For example, CISOs for pharmacy benefit managers and health insurers are having to spend significant time figuring out how to protect their customers' data and then explaining it to those customers. Likewise, cybersecurity is absolutely critical to how companies make decisions about procuring group health or business insurance, prime brokerage, and many other services. It is the single most important factor companies consider when purchasing Internet of Things (IoT) products (Exhibit 3).

Leading companies are starting to build cybersecurity into their customer relationships, production processes, and supplier interactions. Some of their tactics include the following:

— Use design thinking to build secure and convenient online customer experiences. For example, one bank allowed customers to customize their security controls, choosing simpler passwords if they agreed to two-factor authentication.

— Educate customers about how to interact in a safe and secure way. One bank has a senior executive whose job it is to travel the world and teach high-net-worth customers and family

Exhibit 3

Priority requirements have changed for acquiring Internet of Things products: Cybersecurity has moved to the top.

Top 5 priorities when buying IoT products,[1]
number of survey responses

Strong cyber-security	312
Reliability	290
Compatibility with existing enterprise software	251
Compatibility with installed production hardware	235
Ease of use by end user	206

[1] IoT = Internet of Things. Besides basic functionality.

Source: McKinsey 2019 IoT Pulse Survey of more than 1,400 IoT practitioners (from middle managers to C-suite) who are executing IoT at scale (beyond pilots). Composition was 61% from US, 20% from China, and 19% from Germany, with organizations of $50 million to more than $10 billion in revenue. This question on IoT-product purchases received 1,161 responses.

offices how to prevent their accounts from being compromised.

— Analyze security surveys to understand what enterprise customers expect and create knowledge bases so that sales teams can respond to customer security inquiries during negotiations with minimum friction. For instance, one software-as-a-service (SaaS) provider found that its customers insisted on having particularly strong data-loss-prevention (DLP) provisions.

— Treat cybersecurity as a core feature of product design. For instance, a hospital network would have to integrate a new operating-room device into its broader security environment (Exhibit 4).

— Take a seamless view across traditional information security and operational technology security to eliminate vulnerabilities. One auto-parts supplier found that the system holding

the master version of some of its firmware could serve as an attack vector to the fuel-injection systems it manufactured. With that knowledge, it was able to put additional protections in place. Pharma companies have found that an end-to-end view of information protection across their supply chains was needed to address certain key vulnerabilities (Exhibit 5).

— Use threat intelligence to interrogate supplier technology networks externally and assess risk of compromise.

Done in concert, these actions yield benefits. They enhance customer trust, accelerating their adoption of digital channels. They reduce the risk of customers or employees trying to circumvent security controls. They reduce friction and delays as suppliers and customers negotiate liability and responsibility for information risks. They build security intrinsically into customer-facing and

Exhibit 4

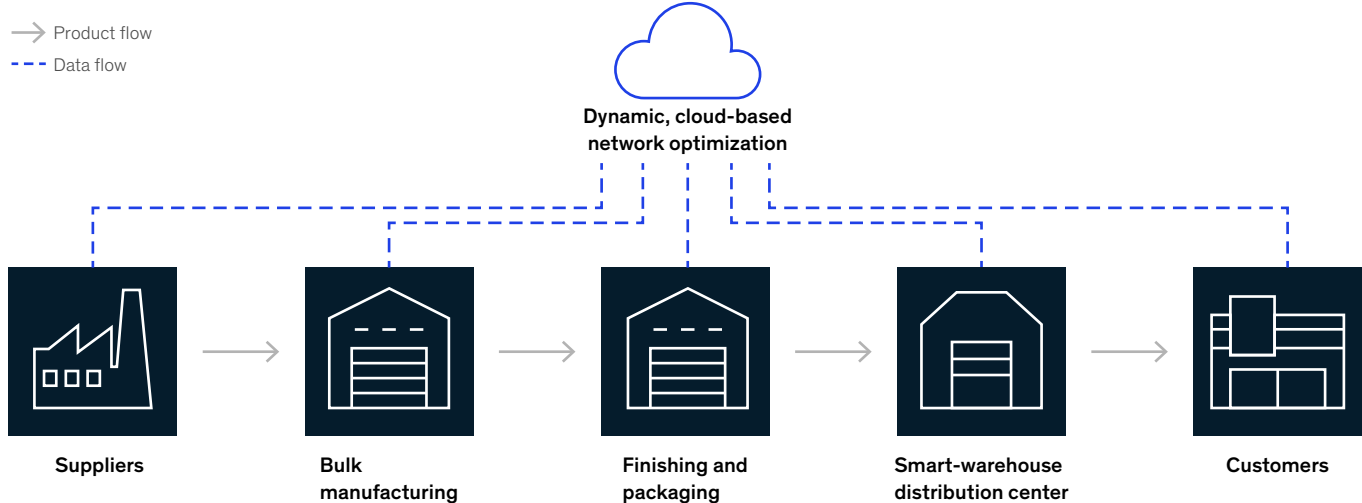## Embedding security into a product-development process can yield significant results.

From treating security and privacy as afterthoughts . . .			. . . to incorporating them by designing and building an agile security-and-privacy model	
Developers are unclear when security and privacy requirements are mandatory	Product owners don't consider security and privacy tasks during sprint planning	**Requirements**	Prioritize security and privacy tasks according to product risk level	Make product owners aware of need to prioritize security and privacy tasks and be accountable for their inclusion in releases
		Design		
Unclear how to handle distribution of tasks within development team	Chief information-security and privacy officers (CISPOs) have limited capacity to support development teams	**Development**	Security and privacy champions (tech leads) assist teams in distributing tasks	Add capacity through CISPOs, who clarify security and privacy requirements with champions and product owners
No unified real-time standardized monitoring of state of security and privacy tasks		**Testing**	Product-assessment dashboards give developers real-time views of security and privacy within products	
Security and privacy needs are often dealt with before deployment, causing launch delays	Teams unclear how often to engage CISPOs	**Deployment**	Launch delays eliminated as security and privacy tasks are executed across life cycles	Simplified predeployment activities with CISPOs only for releases meeting risk criteria
Unclear accountability for security and privacy in product teams	Lack of integration in security and privacy tool sets introduces complexity	**Throughout process**	Define and communicate roles and responsibilities during agile ceremonies	Integrate and automate security- and privacy-related testing and tracking tools

Exhibit 5

An end-to-end view of information across the pharma supply chain is needed to address vulnerabilities.

Supply chain

→ Product flow
- - - Data flow

Dynamic, cloud-based
network optimization

Suppliers → Bulk manufacturing → Finishing and packaging → Smart-warehouse distribution center → Customers

● Advanced business capability   ● Resulting cyberrisks

Suppliers
- Predictive supplier risk protection
- Risk of exposed vendor details and trade secrets

Bulk manufacturing
- Yield optimization through advanced analytics and digitized operations
- Hacking of legacy equipment
- Unauthorized changes in safety or compliance regulations
- Loss of intellectual property and competitive advantage

Finishing and packaging
- Fully integrated and automated production
- Attack on process, leading to shutdowns or errors
- Transition from closed to open systems prompts new security risks

Customers
- No-touch order management
- Leak of customer data, leading to loss of customer trust and competitive data

Overarching technologies
- Machine-learning forecasting and integrated production planning
- Inaccurate business decisions and bad-actor access
- Real-time monitoring
- Unauthorized monitoring of processes and leakage of business decisions

operational processes, reducing the "deadweight loss" associated with security protections.

Enabling an agile, cloud-based operating platform enhanced by DevOps

Many companies seem to be trying to change everything about IT operations. They are replacing traditional software-development processes with agile methodologies. They are repatriating engineering talent from vendors and giving developers self-service access to infrastructure. Some are getting rid of their data centers altogether as they leverage cloud services. All of this is being

done to make technology fast and scalable enough to support an enterprise's digital aspirations. In turn, putting a modern technology model in place requires a far more flexible, responsive, and agile cybersecurity operating model. Key tenets of this model include the following:

— Move from ticket-based interfaces to APIs for security services. This requires automating every possible interaction and integrating cybersecurity into the software-development tool chain. That will allow development teams to perform vulnerability scans, adjust DLP rules, set up application security, and connect

to identify and gain access to management services via APIs (Exhibit 6).

— Organize security teams into agile scrum or scrumban teams that manage developer-recognizable services, such as identity and access management (IAM) or DLP. Also, recruiting development-team leaders to serve as product owners for security services can help, just as business managers are product owners for customer journeys and customer-oriented services.

— Tightly integrate security into enterprise end-user services, so that employees and contractors can easily obtain productivity and collaboration tools via an intuitive, Amazon-like portal.
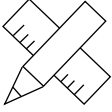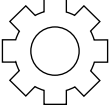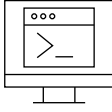
— Build a cloud-native security model that ensures developers can access cloud services instantly and seamlessly within certain guardrails.

— Collaborate with infrastructure and architecture teams to build required security services into standardized solutions for massive analytics and RPA.

— Shift the talent model to incorporate those with "e-shaped" skills—cybersecurity professionals with several areas of deep knowledge, such as in integrative problem solving, automation, and development—as well as security technologies.

Taken together, these actions will eliminate roadblocks to building digital-technology

Exhibit 6

Automation, orchestration technology, and application programming interfaces (APIs) can eliminate manual security processes and interactions.

Automation opportunities in a notionally secure DevOps model

	Architecture and design	Implementation	Code review	Testing	Deployment
App APIs	API-configurable application-level controls designed into new applications	APIs for configuration and debugging (eg, test instrumentation) added during implementation phase	Automated code-review systems modified to search for application-specific threat scenarios	Automated and configurable security test cases added to nightly testing regime	Fully configured, production-ready application possible via API calls alone
Process APIs	New application-level API options added to deployment-configuration process	Configurable security tests added to nightly testing regime	Configurable automated code reviews added to precommit/ preacceptance process for newly written code	Nightly testing results collected and curated for individual developers/ teams via configurable test-management system	Predeployment security-review process replaced by automated tests and configuration checks
Infrastructure APIs	API for deployment and instantiation processes rearchitected to accommodate new applications	Configuration options for instantiation of automated, project-specific development environment made available	Automated code scanning implemented for deployed web applications to maintain quality and code integrity	Cloud environments regularly tested for security via automated vulnerability assessment and identification tools	Security tools and configuration options applied via API to new environments at deployment time

Security-trained developers and engineers enable automation and orchestration throughout cloud-development, -deployment, and -operations phases

How a large biopharma company built cybersecurity capabilities to enable a digital enterprise

A large biopharma company had recently concluded a major investment program to enhance its foundational cybersecurity capabilities, dramatically reducing its risk profile. However, the business strategy began to evolve in new ways, with expanding online consumer relationships, digitally enabled products, enhanced supply-chain automation, and massive use of analytics. The company now needed new cybersecurity capabilities that would both address new business risks and facilitate business and technology innovation.

To get started, the cybersecurity team engaged a broad set of business partners, capturing current and planned strategic initiatives. It then mapped out the new risks that these initiatives would create and the

ways in which cybersecurity protections might slow or block the capture of business opportunities. At the same time, the cybersecurity team looked at a broad set of emerging practices and techniques from the pharma industry and other sectors, including online services, banking, and advanced manufacturing. Based on all this, it developed an overarching vision for how cybersecurity could protect and enable the company's digital agenda, and it prioritized 25 initiatives. Some of the most important were the following:

— collaborating with the commercial team to build patient trust by designing security into online patient journeys

— collaborating with the manufacturing team to enhance transparency into configuration of plant assets

— collaborating with the broader technology team to create the application programming interfaces (APIs) and the template to ensure secure configuration of systems running in the public cloud

— dramatically expanding automation of the security environment to reduce time lags and frustrations developers and users experienced when interacting with the cybersecurity team

The cybersecurity team then used its vision and initiatives to articulate to senior management how it could enable the company's digital business strategy and the support and assistance it would require from other organizations to do so.

---

operating models and platforms. Perhaps more importantly, they can ensure that new digital platforms are inherently secure, allowing their adoption to reduce risk for the enterprise as a whole (see sidebar, "How a large biopharma company built cybersecurity capabilities to enable a digital enterprise").

———————

With digitization, analytics, RPA, agile, DevOps, and cloud, it is clear that enterprise IT is evolving rapidly and in exciting and value-creating ways. This

evolution naturally creates tension with existing cybersecurity operating models. For organizations to overcome the tension, they will need to apply quantitative risk analytics for decision making, create secure business value chains, and enable operating platforms that encompass the latest innovations. These actions will require significant adaptation from cybersecurity organizations. Many of these organizations are still in the early stages of this journey. As they continue, they will become more and more capable of protecting the companies while supporting the innovative goals of the business and IT teams.

This article was originally published on McKinsey.com in July 2019.

James Kaplan is a partner in McKinsey's New York office, **Wolf Richter** is a partner in the Berlin office, and **David Ware** is an associate partner in the Washington, DC, office.

Contact

For more information on core technology transformations in insurance, please contact:

Americas
Zanoni Arenas
Senior expert, São Paolo
Zanoni_Arenas@McKinsey.com

Sanjay Kaniyar
Partner, Boston
Sanjay_Kaniyar@McKinsey.com

Krish Krishnakanthan
Senior partner, Stamford
Krish_Krishnakanthan@McKinsey.com

Ani Majumder
Partner, New York
Ani_Majumder@McKinsey.com

Stefano Martinotti
Partner, Santiago
Stefano_Martinotti@McKinsey.com

Jesus Moreno
Partner, Buenos Aires
Jesus_Moreno@McKinsey.com

Alessandro Rosa
Senior partner, São Paolo
Alessandro_Rosa@McKinsey.com

Africa
Umar Bagus
Partner, Johannesburg
Umar_Bagus@McKinsey.com

David Entwisle
Partner, Johannesburg
David_Entwisle@McKinsey.com

Asia
Brent Carson
Partner, Sydney
Brent_Carson@McKinsey.com

Lari Hämäläinen
Senior partner, Tokyo
Lari_Hamalainen@McKinsey.com

Dino Ho
Senior expert, Hong Kong
Dino_Ho@McKinsey.com

Gregor Theisen
Senior partner, Hong Kong
Gregor_Theisen@McKinsey.com

Europe
Jens Lansing
Partner, Düsseldorf
Jens_Lansing@McKinsey.com

Nadine Methner
Partner, Frankfurt
Nadine_Methner@McKinsey.com

Björn Münstermann
Senior partner, Munich
Bjoern_Muenstermann@McKinsey.com

Peter Braad Olesen
Associate partner, Copenhagen
Peter_Braad_Olesen@McKinsey.com