KPMG

Becoming a CIO of the future

10 actions to help lead your organization through the ever-evolving digital landscape

kpmg.com

Providing a cohesive vision

It's a familiar tune. For years, chief information officers (CIOs) have been told to transition from technical adviser to strategic business partner—someone who can help set the direction of the enterprise, drive innovation, and build competitive advantage. It's still a common refrain. The trouble is, the path to fulfilling that charter, and the challenges to doing so, keep shifting.

What is still true—more than ever—is that the future looks dim for those legacy CIOs who are content to maintain the information technology (IT) estate and make only incremental progress. They may not lose their seat at the table, at least right away, because keeping the IT lights on really does remain critically important. But their ability to influence the business and make a difference in its success will continue to fade. Eventually, their C-suite colleagues will look elsewhere for the technology partners and insights they need to shape the corporate agenda and deliver on its digital transformation goals.

CIOs who successfully lead their organizations through the ever-evolving digital landscape will provide a cohesive vision to move their organization as one. Doing that will involve committing to the following 10 actions. While challenging, they are nonetheless critical to success. We concede that most CIOs are actively moving forward with some of the 10. Still, in our experience, very few are intentionally addressing all 10. And more importantly, in most cases, these 10 are proving to be far more difficult than they may appear on the surface:

01 Create a purposefully designed workforce

Many IT organizations are not built for today, trapping well-meaning and highly capable people in organizational silos and forcing them to compete with increasingly dated skill sets. Ultimately, CIOs find themselves with opportunities to use technology to transform the business but lack the resources to execute their vision. This is about far more than the changing roles and responsibilities of IT. Change is coming from all sides—business demands, individual expectations, and the shifting global talent marketplace.

CIOs can correct course by making a frank assessment of their IT organization's talent and skills. They can then develop an IT talent transformation strategy that includes training for existing staff. Not everyone will be able to make the shift to the modern world. This may call for the CIO to undertake an effort to attract the right mix of engineers and developers needed to deliver on the organization's digital strategy. Winning the competition for talent will be crucial and require a culture focused on providing a great employee experience from recruitment to reskilling to retention.

02 Develop a product-centric IT operating model

Most IT organizations operate in a feature-centric mode in which priorities are based on tradeoffs in time, cost, and scope. Although many IT organizations have embraced agile methods, enabling faster development times, they often remain uninformed of the future expectations of customers and continue to build products that are late to market. Shifting from a feature-centric to a product-centric IT operating model can better align IT with business objectives. It requires not only a commitment to product management but also capabilities in the fields of experience design, design thinking, and dynamic budgeting. Developing applications built on reusable components can boost effectiveness. Typically, the transition to a product-centric IT operating model will begin with a focus on those programs that deliver customer-facing digital products.

03 Build a modern enterprise architecture

Enterprise architecture (EA) is the art and science of designing and continuously evolving the digital enterprise—with a focus on generating positive business outcomes through the power of technology. Today, the business side of the enterprise is increasingly playing a pivotal role in buying and deploying new technology, in effect making de facto EA decisions and impacting the overall technology stack architecture. The CIO, or the enterprise architect, must be more involved from the outset and collaborate with the business on transformational investments that shift from efficiency and throughput to market-responsive outcomes. They must understand the business and technology to bridge the gap between the two worlds, focus the EA function on business outcomes—on enablement, not just governance—and communicate effectively to diverse audiences ranging from the board of directors to development teams. The architect must be able to change course rapidly as business requirements change and deliver an architecture that provides self-service capabilities to end users to enable organizational agility. CIOs will need to invest in broadening the skills of their enterprise architects while also providing them with authority to set multiyear architecture runways to guide the digital transformation. Success for CIOs is measured by their organization's ability to respond quickly to market events and competitors' actions.

CIOs will need to invest in broadening the skills of their enterprise architects

04 Introduce "security by design" and a zero-trust security model

In a world where employees, business partners, and suppliers increasingly need anywhere access to business applications, maintaining the security of the enterprise ecosystem is becoming more challenging—yet essential. Cyber defense has become a massive industry, funded by companies held hostage by encryption attacks, data breaches, and denials of service. A security breach or infrastructure failure can cost millions of dollars per minute. In this environment, too many businesses remain focused on providing a simple user experience by allowing simple connectivity—without understanding the associated risks. At the same time, CIOs relying on traditional risk management controls can find their digital transformation initiatives halted in their tracks by overly cautious security measures.

Navigating competing priorities of user convenience and ironclad safety calls for security to be thoughtfully embedded in the design of every IT investment. This is necessary to create secure cloud environments, secure continuous integration/continuous deployment (CI/CD) pipelines, and safe use of open-source software. Because maintaining cybersecurity can be so tricky in a world evolving at digital speed, CIOs must also continue migrating toward "zero trust" security models, which build on the idea that the enterprise will not trust anything inside or outside its security perimeters without verification. The zero trust journey starts with transforming how IT manages digital identities. Those identities must be simplified and hardened to support the mechanics of the cloud, application programming interfaces (APIs), and diverse groups of tech-savvy users inside and outside the company and also comply with changing compliance requirements. While all this may sound cumbersome, growing numbers of CIOs find it a price worth paying—especially after their enterprise has suffered through a serious security incident.

A security breach or infrastructure failure can cost millions of dollars per minute.

05 Take advantage of value-based managed services

Traditional IT outsourcing providers, or managed services providers (MSPs), may seek to take over their customers' select, noncompetitive business responsibilities—providing their "mess for less" and ensuring they run smoothly. They are not, by contrast, focused on making their customers more agile or efficient or, heaven forbid, helping them migrate to the cloud. In fact, they often have contractual incentives to do just the opposite to avoid disrupting their revenue stream. For example, cloud technologies may eliminate a substantial portion of what an MSP does. In the managed services model CIOs should be seeking today, the MSP will have the skills and capabilities required to address

IT's modern mission; they will look beyond its contract for opportunities to improve the efficiency of the customer's internal business processes. To support their organization's relationship with this new type of provider, CIOs will want to look beyond traditional service level agreements and pricing mechanisms and focus instead on partnering with their service providers for win-win transformational change. CIOs can make this work better by also taking steps to integrate service-providing partners into their business strategy and product-centric teams.

06 Embrace modern software innovation and delivery practices

"Hurry up to wait" has become the reality of the agile enterprise as the development and integration of new software applications and IT infrastructure continues to take weeks or months. In part, that's because legacy enterprises are burdened with legacy IT operating models and governance, risk, and control processes that were never optimized for speed. The challenge is compounded by the shortage of IT talent relative to demand.

CIOs can help their companies innovate more quickly and with less risk by building and deploying IT systems using modern development, security, and operations (DevSecOps) practices. DevSecOps seeks to develop high-quality software at the lowest possible cost in the shortest

possible time through iterative planning, execution, and delivery. It incorporates stakeholder input to define new system capabilities and eliminates typical development hurdles while embedding security and governance directly into the systems development life cycle. Agile coaching alone won't be enough; CIOs must create a DevSecOps transformation program that aligns interdependencies and integrated milestones with other initiatives. A working DevSecOps model also requires supporting multiple CI/CD platforms to allow teams to program on varying codebases and refactoring or rearchitecting legacy technology and antiquated platforms to support automation.

07 Adopt a cloud-first IT strategy

Is your cloud journey stuck? Most organizations have been moving at least some IT workloads to the cloud, but many struggle to realize the targeted benefits. It's only going to get tougher from here. If cloud migration were a baseball game, then most organizations would still be in the third inning, with the following three almost sure to be even more challenging. But they'll also be more impactful.

The goal in all cases, whether migrating to a public or private cloud, is to improve the speed and agility of the business. That won't come with simply lifting and shifting existing applications to the cloud—what many organizations have been doing in the first three innings of the game—or expanding the use of virtual servers. It will come from making cloud the enabler of DevSecOps and security by design. Cloud is the core of

the architecture runway and the foundation of a product-centric organization. Done right, it requires tackling technical debt—legacy IT systems and applications—with surgical precision. A cloud-first IT strategy also requires taking bets on software as a service, platform as a service, infrastructure as a service, and serverless IT providers. It requires making decisions on applications that provide competitive advantage. It requires options for application teams to go cloud-native, replace existing IT platforms with PaaS, and rearchitect on low-code platforms. It requires rethinking data platforms and integrations. Finally, a cloud-first strategy requires the whole organization to move aggressively as one—or risk being stuck in place for years with little return on investment.

08 Develop next-generation IT operations

Most IT organizations are operating with a bimodal strategy in which they support cloud and legacy technologies on two separate tracks. Experience has shown that bimodal models are not sustainable and that failing to transition to a hybrid approach risks surfacing new problems across the IT landscape. To facilitate the shift to a hybrid IT model,

CIOs can take advantage of technologies that extend from the cloud to manage on-premises platforms, embed automation in all layers of IT support, and treat data as an asset—all of which will be important to earning the trust of both internal and external customers.

09

Create a data-driven enterprise

Businesses are awash in data but struggling to extract full value from it, often because they don't share a common data language across the enterprise and with suppliers, distributors, end customers, and other stakeholders. With different entities and applications all using different terminologies to identify parts, products, and transactions— or not tracking them at all—it becomes impossible to share and analyze data at scale efficiently. A genuinely data-driven enterprise, by contrast, is built on a common data language. It sounds simple, but developing and implementing that common language is tedious, nitpicky work that never goes quickly. Still, this integration of data across sources and departments is as critical to becoming a truly data-driven enterprise as maintaining the right

levels of data security. Once a common language has been established and implemented, data from multiple sources can then be integrated and swiftly fed into systems of insight and action for use by data analysts and business leaders. Data ownership may continue to lie with the business in a data-driven enterprise, i.e., the business controls content and accuracy. However, the CIO is responsible for developing and managing the organization's data technology backbone in partnership with business leaders or the chief data officer, if one has been designated. Throughout, the CIO's focus is on enabling high-speed, automated data intake, distribution, and analysis.

10

Build a resilient technology stack and operating model

Many factors have pushed digital resilience to the top of the corporate agenda over the past two years: the pandemic and its attendant supply chain disruptions, the proliferation of ransomware, hazards stemming from climate change, and geopolitical conflict. Nonetheless, many organizations have yet to build a resilient technology stack and operating model. Among other things, they've treated the challenge solely as a technology problem rather than one that aligns stack and strategy to business needs. And they have failed

to test their recovery processes sufficiently to prove that full-service value chains can be continued and ideally recovered after a disruption. CIOs can build more resilience into their IT systems by defining the risks to the business and the gaps in current capabilities, then developing a resilience strategy that reduces risk to acceptable levels— with resilience requirements for critical vendors built into the package.

CIOs of the future will be business technology leaders, not back-office managers. They will help drive innovation and business outcomes. This will be good for the company they serve and its customers. And it will help with attracting and retaining ambitious, creative engineers, developers, and data scientists.

KPMG applies its extensive experience and deep domain knowledge to help CIOs build modern IT organizations fit for tomorrow. To learn more about how KPMG could help your business, please contact:

Marcus Murph
Principal, U.S. CIO Advisory
Practice Leader
214-840-2671
marcusmurph@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia