KPMG

The future of IT: Next generation IT operating models

Part three: orchestrate

January 2018

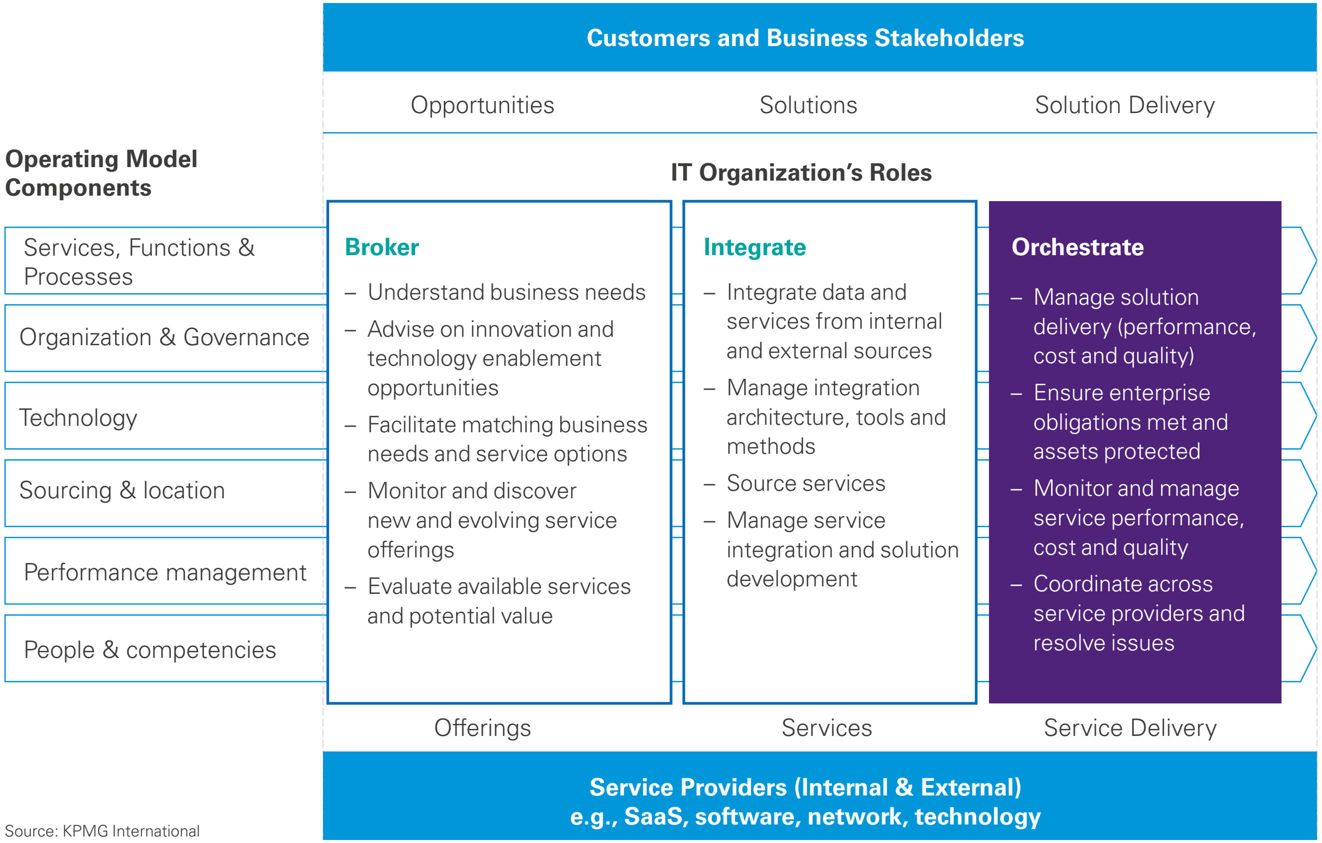
Introduction

Today, most organizations are somewhere along a digital transformation journey employing disruptive technologies to innovate across products, services, and business models. CIOs have been struggling to keep up with the insatiable demand for new digital capabilities from their business stakeholders. In fact, many have been watching their business counterparts increasingly turn to external providers for the technology enablement they need. In response, some CIOs have adopted multi-speed IT, increased their use of agile methodologies, or even created standalone digital units separate from the traditional IT organization. But these are only stop gap measures. What's really needed is adoption of an entirely new IT operating model to manage the greater complexity of today's emerging technology.

KPMG first introduced the next generation IT operating model in late 2014 encompassing three new roles for IT: broker, integrate, and orchestrate (see Figure 1). This is not just a new name for the traditional plan, build, run legacy IT operating model. Where plan, build, run also described a functional organization structure comprised of technical silos, the broker, integrate, orchestrate (BIO) model describes roles that are independent of any organizational structure. In fact, we believe that the IT BIO model can support a variety of functional / organizational structures based, for example, on a line of business, product/platform, or channel alignment. One thing is clear – whatever new organization structure is implemented, it will break down the traditional technology silos while requiring new skills.

In this, the third in a series of three reports, we will take a closer look at the role of 'Orchestrate' in the new operating model and the implications for CIOs.

Figure 1: The broker, integrate, orchestrate (BIO) IT operating model



Customers and Business Stakeholders

Opportunities | Solutions | Solution Delivery

Operating Model Components

- Services, Functions & Processes
- Organization & Governance
- Technology
- Sourcing & location
- Performance management
- People & competencies

IT Organization's Roles

Broker

- Understand business needs
- Advise on innovation and technology enablement opportunities
- Facilitate matching business needs and service options
- Monitor and discover new and evolving service offerings
- Evaluate available services and potential value

Integrate

- Integrate data and services from internal and external sources
- Manage integration architecture, tools and methods
- Source services
- Manage service integration and solution development

Orchestrate

- Manage solution delivery (performance, cost and quality)
- Ensure enterprise obligations met and assets protected
- Monitor and manage service performance, cost and quality
- Coordinate across service providers and resolve issues

Offerings | Services | Service Delivery

Service Providers (Internal & External)
e.g., SaaS, software, network, technology

Source: KPMG International

The orchestrate role ensures delivery

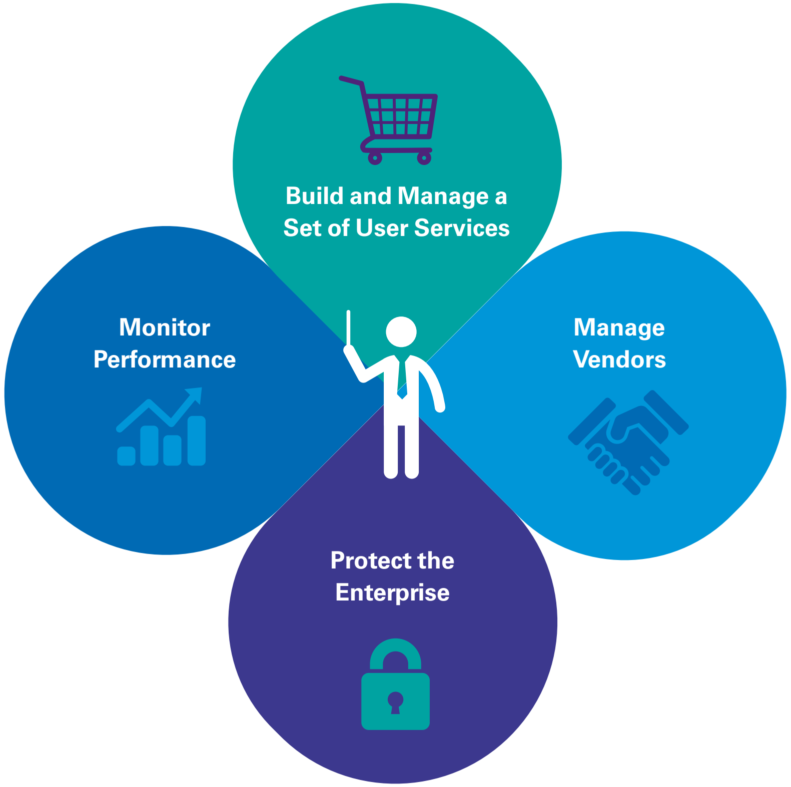
Today's digital businesses are underpinned by a complex portfolio of technology-enabled capabilities sourced from an ever-expanding ecosystem. The complexity of this ecosystem is only going to increase. For large enterprises it often includes on-premises data centers with virtualized servers and private clouds, off-premises public clouds, a variety of open source and proprietary software platforms, custom built legacy applications, and SaaS solutions, all supported by a collection of internal IT staff, vendors, system integrators, and consultants. With many digital businesses running 24x7, all of this technology must be always available, secure, and compliant with constantly evolving regulations that can vary from country to country.

Orchestrate's Four Major Responsibilities

As discussed in the first two reports in this series, the broker role works closely with IT's customers to shape demand, and identify and evaluate new solutions and services to provide the business with the technology-enabled capabilities it needs to remain competitive. The integrate role ensures that all new solutions and services work seamlessly with existing applications and data. In the next generation IT operating model, the orchestrate role embraces the transformation to IT as a Service (ITaaS), delivering services and ensuring that performance, cost, and quality are meeting or exceeding expectations, that applications and data are secure and compliant, and the business is getting optimal value. The goal is to hide the complexity and provide the same ease of use and responsiveness of the consumer online experience to procuring business services. This is essential if the business's increasing expectations are to be met and a genuine return on investment is to be realized.

The orchestrate role carries out four major responsibilities: (1) build and manage a set of user services: (2) manage vendor relationships; (3) protect the enterprise; and (4) monitor service delivery performance – see Figure 2.

Figure 2: Orchestrate's four major responsibilities



The orchestrate role ensures delivery cont...

01 Build and manage a set of user services

The broker role matches business needs with appropriate services and solutions, and whenever possible to ones that already exist in the service catalog. The orchestrate role manages the service portfolio and ideally provides a user-friendly portal into all existing services and solutions including services primarily for the business units, individuals, and IT itself.

This portal incorporates standard service catalog functionality including self-service capabilities and integrated workflow. With the migration to hybrid cloud environments well underway, a consumption platform underpins a growing segment of the portfolio.

Such portals are also being increasingly complemented by a wider range of more bespoke support options, such as localized or specialized help desks, drop-in desks and the development of online 'chat' agents. Everything needs to be geared around increasing the flexibility of the support available to the user.

The consumption platform is a composite of tools and processes that provides access to underlying services and manages their operation. It includes four major functions: management and control; orchestration; identity; and security and governance. Using a combination of intelligent automation, open source tools, pre-built templates, and in-line governance, the consumption platform can support self-service provisioning of cloud-based services with compliance embedded within the provisioning process.

Taking a centralized approach ensures standardized implementations across the enterprise and investment protection. Key elements of a consumption platform are depicted in Figure 3.

— **Management & Control** provides overall administration including access, financial management, performance management, and support for analytic-based reporting.

— **Orchestration** provides for automated provisioning including workflow management, standardized templates, and policy enforcement. It also enables integration in support of agile pipelines including continuous integration and continuous deployment.

— **Identity** provides a centralized approach to identity management including authentication, authorization, and auditability for compliance.

— **Security & Governance** capabilities include support for cryptography, vulnerability management, and data management and governance.

As new solutions and services are developed or procured they will be added to the portal and the wider support services available.

The orchestrate role ensures delivery cont...

02 Manage vendor relationships

With the near-universal use of cloud technology and SaaS greatly reducing the need for infrastructure technical support, the orchestrate role becomes focused on configuring and managing the complexity of the IT operating model requirements.

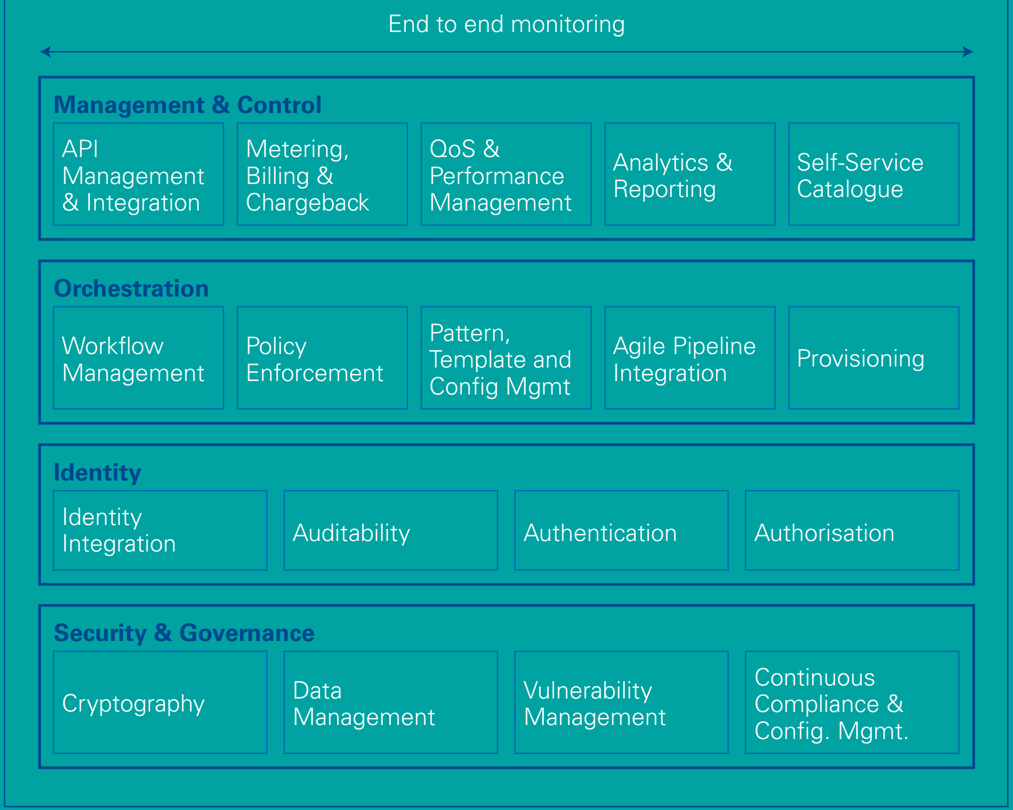
Technology-enabled capabilities continue to grow in complexity and involve many different suppliers, each providing one component. It is not uncommon to build a solution using public cloud infrastructure from one vendor, a suite of middleware comprised of proprietary and open source components from other vendors, and an application built by a systems integrator. The orchestrate role coordinates across all service providers, manages escalation processes and resolves issues.

The emphasis for the internal IT team shifts to managing the complexity of cloud technology. For example, managing thousands of technical cloud configuration options with the potential to drive cost, spin up and spin down, more complex interface management, increased number of releases and forced releases from SaaS platform providers. New skillsets will be needed internally to deal with this. Managing it will be critical to ensuring that organizations achieve the expected return on investment. Conversely, failure to do so could mean that cloud technologies cost an organization more than their old legacy systems did – defeating the whole object of agile IT.

As buy versus build and participating in digital ecosystems becomes the preferred method for obtaining new capabilities, the orchestrate role provides centralized sourcing and vendor management (SVM). The broker role will retain responsibility for developing the overall sourcing strategy, while the orchestrate role will focus on execution including contract management, risk management and performance management.

Looking further ahead to the next wave, the orchestrate role will also need to manage increasing amounts of AI, robotics and automation. This will only increase complexity further – so planning needs to start now. With organizations likely to be using a greater number of SaaS and cloud providers, as well as more niche tool providers, end-user solutions and network providers, the number of supplier companies that an organization works with is set to grow. Managing this effectively will become a key determinant of success in the orchestrate role.

Figure 3: A consumption platform example



End to end monitoring

Management & Control

API Management & Integration | Metering, Billing & Chargeback | QoS & Performance Management | Analytics & Reporting | Self-Service Catalogue

Orchestration

Workflow Management | Policy Enforcement | Pattern, Template and Config Mgmt | Agile Pipeline Integration | Provisioning

Identity

Identity Integration | Auditability | Authentication | Authorisation

Security & Governance

Cryptography | Data Management | Vulnerability Management | Continuous Compliance & Config. Mgmt.

The orchestrate role ensures delivery cont...

03 Protect the Enterprise

Digital business transformation has significantly increased the importance of technology to overall business performance. Cyber security related incidents are almost a daily occurrence whether coming in the form of ransomware, data and identity theft, or some other disruption. While security is ultimately everyone s responsibility, the orchestrate role has overall responsibility for protecting the enterprise and ensuring compliance with relevant policies and standards.

Protecting the enterprise consists of raising awareness of everyone s role in securing the enterprise through education, safeguarding it by taking proactive measures to prevent incidents, and detection by monitoring critical events and occurrences. Monitoring and data mining together form an excellent instrument to detect strange patterns in data traffic, to find the location on which the attacks focus and to observe system performance.

When incidents do happen, the orchestrate role responds by activating a well-rehearsed plan as soon as evidence of a possible attack occurs. During an attack, the organization should be able to directly deactivate all technology affected.

Security controls are an integral part of IT service offerings facilitated by making security practices as easy as possible for service owners to adhere to, and ensure protection without impeding productivity.

The center assesses risk, develops controls and implements componentized security services that are utilized in cloud, application and consumer service offerings. In addition, the center measures security compliance and remediates issues when needed. It also empowers IT to provide secure services by embedding security expertise in service teams.

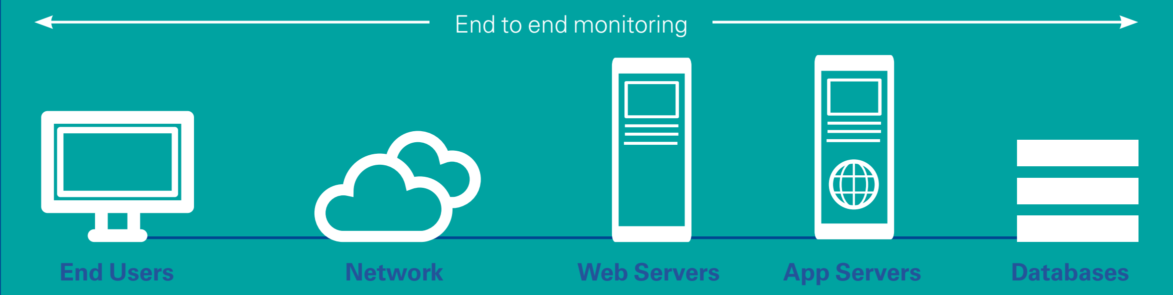
04 Monitor service delivery performance

With a large and growing investment in technology enablement, it is important to make sure that outcomes are meeting or exceeding expectations and value is optimized. Consequently, the orchestrate role is responsible for monitoring, measuring, and communicating end-to-end service delivery performance which is increasingly important, especially given the multi-tiered combination of hardware, software and services that comprise many solutions.

Today's web applications enable increasingly complex tasks while users' expectations are for 24x7 availability. A problem can occur at any point along the application delivery chain so it is important to implement monitoring tools that provide visibility into all tiers from the user interface to application execution to database processing – see Figure 4. Through constant monitoring it is possible to shift from being reactive to proactive by detecting performance degradation and faults early, before they can cause a major incident.

Each service has a service manager that has overall accountability for the performance of the service. Service managers work closely with the operations team to manage the overall health of their service and ensure that it is delivering its expected outcomes.

Figure 4: End-to-end service performance management



Key orchestrate players

Perhaps the biggest challenge confronting CIOs as they transform the IT operating model is their people and managing the changing roles and skills required. The sheer scale and pace of technology disruption has profound implications for the types of positions and skills the IT organization will need - see Figure 5. The orchestrate role will require that new positions are created along with new skills. Some of the current IT positions need to evolve, while increasing levels of automation and ongoing cloud migration cause others to be scaled back or even eliminated. Several representative key players in the integrate role include:

Cloud Architects

As more organizations adopt a cloud-first strategy, the role of cloud architect becomes key. Cloud architects are responsible for an organization's cloud computing strategy. This includes the approach to cloud adoption, cloud application design, and cloud management and monitoring. Cloud architects oversee application architecture and deployment in cloud environments including public, private and hybrid cloud. Additionally, cloud architects act as consultants on cloud-related issues. Security in the cloud is important, and cloud architects require a high level understanding of key security concepts. An initial knowledge of some basic security concepts such as firewalls is necessary. In addition to a variety of technical and non-technical skills, the cloud architect must be a great collaborator in order to empower and connect with a variety of other architecture roles in the organization including enterprise architects and senior IT architects.

The cloud architect will be a key contributor to the development of the consumption platform discussed earlier. They will work closely with IT operations specialists and automation specialists to design the consumption platform architecture, select the appropriate tools, and develop the templates, scripts, and programming to automate many of the processes.

Supplier Relationship Managers

As organizations source more services, components, and capabilities from the ecosystem, supplier relationship management becomes even more important and supplier relationship managers become key players in the orchestrate role. A supplier relationship manager (SRM) is responsible for building and managing relationships with the vendors that are part of the firm's ecosystem. The focus is to develop two-way, mutually beneficial relationships with strategic partners to deliver greater levels of innovation than could be achieved by operating through a traditional, transactional procurement model. The increasing use of cloud and SaaS providers in the ecosystem will also increase the emphasis on flexible commercial management, in turn increasing the complexity of managing supplier relationships.

SRMs have several major responsibilities including:

- Evaluating potential suppliers using criteria such as industry experience, capacity, quality standards and financial stability. They ensure that vendors understand their organization's expectations and requirements and negotiate contract terms that are commercially minded and work in the interests of the organization, in the context of the additional flexibility offered by cloud and SaaS technology.

- Managing supplier performance by monitoring factors such as delivery reliability, quality and accuracy of estimates and invoices. They track and analyze vendor performance and generate reports for use in purchasing, manufacturing and logistics. Performance management enables the identification and management of risk. If suppliers fail to reach their contractual requirements, they can pose a risk of disruption to the business.

- Communicating between suppliers and their own organization to keep vendors informed on developments in the organization or changes in market conditions that might affect demand. They may involve vendors in planning sessions so that vendors can integrate their own production schedules with the organization's requirements, improving efficiency and reducing the risk of excess capacity or supply shortages.

Key orchestrate players cont...

Cybersecurity Engineers

Cybersecurity threats are increasing at alarming rates and imposing significant financial risks to businesses. Costs to the business from a security breach include remediation and reputational costs, along with fines and other remedies. With its responsibility to protect the enterprise, cyber security engineers are key players in the orchestrate role. Security is as much about cultural behaviors as it is about technology so much of what cybersecurity engineers must do is to change behaviors and make sure that every individual recognizes that a secure enterprise begins with them. Beyond this the cybersecurity engineer has three primary responsibilities including:

- Designing the computer security architecture in order to ensure that the business strategy and security are aligned. Some industries are more sensitive than others and operate under different legal and regulatory requirements. The cybersecurity engineer defines the organization's security processes and information security systems.
- Identifying and defining system security requirements for each application and service in order to describe concretely what must be done to assure the security of the system and its data.
- Engineering, implementing and monitoring security measures to protect systems. Security measures range from requiring complex passwords to segmenting networks to deploying intrusion detection and prevention systems.

Figure 5: Orchestrate role representative players and outcomes

Objectives	Representative players	Desired outcomes
Build and manage a service demand portal	Cloud Architects	– Comprehensive service catalog – High degree of self-service – Embedded governance – Automated provisioning
Manage vendor relationships and delivery	Supplier Relationship Managers	– Strategic partners vs. suppliers – Outcome-based incentives
Protect the enterprise and ensure compliance	Cybersecurity Engineers	– Secure infrastructure – Protected data – Compliance with all regulations
Monitor end-to-end service delivery performance	Service Managers	– Actionable outcome-based metrics – Role and function specific dashboards – End-to-end and lifecycle perspectives

Source: KPMG International

Key orchestrate players cont...

Business Service Managers

As IT transforms into an “as a service” business, the role of business service manager becomes key within the orchestrate role. Breaking down the legacy siloed approach, business service managers work on behalf of, and in conjunction with, the business to ensure that services and products are delivering what the organization needs. More frequent and rapid connections to the business will be needed: traditional monthly service reviews will not be sufficient. Retaining end-to-end responsibility for a specific service from initial definition and development through its entire lifecycle including retirement, the business service manager has a number of responsibilities including:

- Overseeing the initial release of the service. The business service manager works with the initial customer/consumer of the service to obtain the requirements, get the interface defined, and get it built, tested and deployed.
- Managing the service performance. Once the service has been deployed, the business service manager monitors the service utilization, availability, and overall performance to ensure that it is meeting the needs of the customer and returning value for cost.
- Planning future releases. The business service manager also works on defining the next release of the service based on observing the performance of the current release and soliciting input from customers.
- Marketing the service to others. Often services developed for one set of customers has appeal and value to other customers. The business service manager is responsible for marketing the service across the enterprise to other potential customers in an effort to amortize the cost over a broader base and to eliminate potential redundancies.

Next steps

Changing the IT operating model is an enormous challenge with very high stakes. It is further complicated because IT must continue to support existing portfolios including retained infrastructure and legacy applications during the transformation. For some time, IT will be operating with a hybrid model as infrastructure and operations migrate to the cloud, legacy applications and services are retired, modernized or replaced, existing skillsets are upgraded or acquired, and stakeholders adjust to the new approach.

For many, the biggest challenges are around organizational change management and the human capital element. IT organizations will get smaller even as demand increases due to the convergence of several secular trends. These include the virtualization and/or migration of infrastructure to the cloud which will shrink and over time quite potentially eliminate data center footprints and associated operations staff, the increasing automation of many manual processes and functions through intelligent automation; the evolution of applications development away from large waterfall project-based work to smaller, cross-functional agile teams; and the ongoing absorption of former IT functions by the business. In addition to shrinking IT headcount, many of the remaining roles will evolve and require new skills.

As a first step, begin by assessing your current staffing and skills against the requirements of the orchestrate role and conduct a gap analysis. Key questions to ask are:

— How can your existing IT staff be developed to take on new roles and what skills/training will they need?

— How can IT create opportunities to recruit internal candidates from the business?

— How will your talent management capabilities have to change to ensure that you have access to the needed skills both internally and externally?

— How can you satisfy the most immediate needs while you build your capabilities?

— What manual processes can be automated now, in six months, in one year?

This will identify some roles that can be eliminated or reduced, some roles that can migrate into the business and functional areas, and candidates ready for re-skilling. It will also reveal what new skills need to be sourced externally.

The second step is to begin an assessment of your cyber security, vendor management and performance monitoring capabilities. Do you have in place the expertise, resources and committed funding to develop these capabilities? Key questions to ask are:

— How will cyber security practices have to evolve?

— How will you acquire the expertise in security, vendor management, and performance management?

— How can you develop strategic relationships with your vendors and partners?

Contributors

With thanks to the following subject matter experts for providing their input and guidance in this paper.

Marc Snyder
Managing Director, Technology Global Center of Excellence
T: +1 978 807 0522
E: msnyder@kpmg.com

Peter Ironside
Director, CIO Advisory
KPMG in the UK
T: +44 (0)759 520 0997
E: peter.ironside@kpmg.co.uk

How KPMG can help

KPMG recognizes that today's CIOs face increasingly complex demands and challenges in becoming the strategic technology partner their businesses require.

KPMG's CIO Advisory professionals can help CIOs, technology leaders, and business executives harness technology disruption, more effectively manage technology resources to drive agile, improved business performance, enhance strategic position, and improve the strategic value of their technology investments.

If your IT organization is seeking ways to leverage technology as a source of innovation and competitive growth, KPMG member firms can help. For more information on CIO Advisory's service and capabilities, please visit www.kpmg.com/cioagenda

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. CRT083993

Contacts

Lisa Heneghan
Global Head of Technology, Management Consulting
KPMG International
T: +44 7718 582 368
E: lisa.heneghan@kpmg.co.uk

Denis Berry
KPMG in the USA
T: +1 312 919 4302
E: dberry@kpmg.com

Phil Crozier
KPMG in the UK
T: +44 20 7311 1353
E: phil.crozier@kpmg.co.uk

Guy Holland
KPMG in Australia
T: +61 410 530 410
E: guyholland@kpmg.com.au

Marc E. Snyder
KPMG in the USA
T: +1 978 807 0522
E: msnyder@kpmg.com

Claudio Soutto
Head of CIO Advisory, Latin America region
KPMG International
T: +55 11 3940 3285
E: claudiosoutto@kpmg.com.br