IT modernization: Operate and secure hybrid at scale

New approaches for running IT operations in a modern enterprise
Many large organizations have moved applications and workloads to the cloud in hopes of lowering costs, increasing business agility and accelerating resource provisioning. A highly efficient IT operating model is key to achieving these benefits — but despite the growing complexity of operating and securing hundreds of applications on-premises and in the cloud, enterprises are still relying on traditional ways of working.

On-premises environments now include data centers, the edge and an explosion in personal devices for remote working. Cloud has evolved to include hybrid environments with private, public and multicloud, which means hybrid is the new reality for most IT organizations.

Data management and integration across applications and platforms are challenging. Many organizations struggle with balancing employee skills across platforms, optimizing handoffs between teams, providing consistent security controls and managing costs.

To manage this complexity, IT organizations should embrace a modern operating model that emphasizes agile DevSecOps teams, hybrid and multicloud integration, application and data management, intelligent automation, continuous optimization and a secure ecosystem (Figure 1).

Transforming hybrid IT operations fundamentally changes the way IT provides technology services to the business, responds to issues and manages expectations. IT can deliver more value while supporting key business goals such as faster speed to market, lower operating costs, and greater scale and resiliency when business conditions change.
IT must support new ways of doing business including mobile-first services, virtual working and innovative partnerships.

**Key approaches for managing hybrid operations**

<table>
<thead>
<tr>
<th>Approach</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicloud integration and management</td>
<td>Eliminate operational silos and accelerate delivery of IT services</td>
</tr>
<tr>
<td>App management, DevSecOps &amp; site reliability engineering</td>
<td>Enable and orchestrate new operating models with agile development, automated processes and self-healing systems</td>
</tr>
<tr>
<td>Continuity &amp; risk management</td>
<td>Enable cloud-native business continuity</td>
</tr>
<tr>
<td>Continuous optimization</td>
<td>Automatically scale up and down to align to business demand and optimize capital costs</td>
</tr>
<tr>
<td>Intelligent automation</td>
<td>Eliminate manual processes for application management, IT service delivery, development and testing, and security monitoring and incident response</td>
</tr>
<tr>
<td>Platform management</td>
<td>Manage infrastructure operations across the full stack</td>
</tr>
<tr>
<td>Security controls</td>
<td>Secure data and systems, verify digital identities and integrate with IT service management</td>
</tr>
</tbody>
</table>

*Figure 1. Managing hybrid operations spans clouds, platforms, applications, development practices and security controls*

**Managing hybrid and multicloud environments**

To fully align with the business, IT organizations must support new ways of doing business, including mobile-first services, virtual work environments and innovative partnerships. Effectively managing hybrid and multicloud environments requires a common framework for operating and securing complex IT estates and creates greater transparency about costs and business performance. This approach integrates people, processes, technologies, controls and metrics into a modern operating model that can be monitored and continuously improved.

Hybrid operations may vary based on an organization’s industry and region, the regulatory environment, the current IT environment and the path it took to build a hybrid estate. However, the common goal is to bring together employee roles, tools, platforms and processes in a highly efficient, cost-effective environment (Figure 2).
Key capabilities include:

- Integrated operations across public and private clouds to deliver IT services more efficiently
- Levels of automation to streamline processes and activities
- Measurements to optimize costs and consumption
- Responsibilities for the work across organizations
- Delivery of IT services and how they map to business services
- Decision making, risk and compliance management
- Security monitoring, identity management, data protection and threat intelligence

Strategies for operating and securing hybrid at scale

While IT environments are becoming more complex, a wide range of tools and practices to optimize systems and processes has reached maturity. Automation, artificial intelligence (AI) and machine learning are eliminating labor-intensive processes. Modern platforms are consolidating IT services across the entire IT stack, while new ways of working across teams are increasing efficiencies and creating more agile operations. Key strategies for transforming IT operations are discussed in the following pages.

Multicloud integration and management. While it might be simpler to consolidate on a single private or public cloud, the reality is that most organizations are already managing multiple clouds, but are not achieving efficiencies across the environment. Multicloud integration enables:

- Self-service provisioning
- Advanced automation of processes
- Centralized IT service management (ITSM)
- A common control plane for managing operations
- Financial management to gain visibility and financial control over all cloud services

Leading university integrates hybrid landscape

A large university needed to enable researchers and students to provision private and public cloud services quickly in a controlled way. DXC deployed a hybrid integration solution with a self-service portal with financial, governance and security controls. A ServiceNow catalog unifies request management, life-cycle actions and all controls. The school simplified its ordering process, automated landing zone choices and controlled spending.
In this environment, IT departments can transform from being managers of discrete IT software products and infrastructure into serving as cloud service brokers with an aggregated self-service catalog for IT services.

Application owners can choose cloud providers and quickly build new higher-level offerings to address business requests such as provisioning a corporate website or development environment for a new product.

**Application management, DevSecOps and site reliability engineering (SRE).**

*Application management* is a resource-intensive, high-touch IT function that requires constant focus on managing skill sets across the enterprise. Traditional approaches to application management are evolving with cloud adoption.

*DevSecOps*, the deployment of agile teams that continuously deliver code and integrate applications, has emerged as a fast, highly efficient approach to deliver applications, update loosely coupled services and shorten time to market for new features. DevSecOps eliminates delays and handoffs through automation of software testing, release and deployment processes.

In most enterprises, approximately 70 percent of the IT budget is spent simply keeping the lights on rather than moving the organization forward. In DXC Technology’s experience, an estimated 30 percent of data center capacity sits idle at any given point in time.

Historically, security testing was performed at the end of the pipeline, often resulting in major disruptions or delays to the development process. Security is now embedded into DevSecOps teams (Figure 3).

---

**Airline boosts software releases 300% with DevSecOps**

A leading commercial airline’s development team faced a growing backlog of work and struggled with inefficient processes for monitoring, deployment and incident handling. The company worked with DXC to establish agile practices and a DevSecOps program with automation, streamlined processes, continuous integration and testing, and one-click deployment. As a result achieved a 300 percent increase in average releases per month, an 83 percent reduction in deployment time and an 89 percent reduction in time to resolve incidents.

---

*Figure 3. Embedded security in DevSecOps processes*
By shifting left, DevSecOps ensures continuous testing throughout the development life cycle and incorporates security controls into the overall product development. Checks for vulnerabilities continue even after deployment to test applications in the real world and ensure that the code is secure against the most up-to-date attack techniques.

New computing platforms require a new operating model that takes a software engineering approach to operations. Site reliability engineering (SRE) implements the automation and the power of DevSecOps and applies it to the full stack. Software engineers continuously focus on increasing automation, availability and reliability through continuous feedback loops. This requires a merging and reskilling of traditional application management and operations teams into combined teams that apply cloud-native methodologies and share multiple skills.

By eliminating the silos between operations and development, SRE lowers operating costs while simultaneously increasing application reliability and availability. SRE teams focus on different metrics than those of traditional operations such as service level objectives (SLOs), service level indicators (SLIs), service level agreements (SLAs) and error budgets.

With a constant focus on elimination of manual tasks, known as “toil,” organizations are able to automate the resolution of common incidents at scale. This focused approach leads to the development of automation and self-healing techniques that use machine learning to automatically implement corrective actions, making operations more proactive than reactive in solving problems.

Continuity and risk management. Countless organizations worldwide have discovered shortcomings in business continuity programs in 2020 during the COVID-19 crisis and subsequent lockdown orders that created remote workforces nearly overnight. The crisis raised key questions for continuity planners to address, such as where to focus resources, how to fill key functional roles quickly, and how to backup and secure data spread across a host of remote workers’ devices.

Many organizations are now reevaluating in-house programs and exploring ways to move to a recovery-as-a-service model, taking advantage of third-party services and cloud resources. This approach ensures protection of traditional IT, cloud, physical and virtual servers, and it includes SLAs that help ensure high levels of continuity. DXC has found that this usage-based approach typically costs 40 percent less than in-house programs and can restore normal business processes within 4 hours and limit data loss to 15 minutes.

Modern apps help agency save €97M, rapidly respond to crisis

To help the Government of Flanders streamline services, DXC built and managed an applications platform that enables Flemish citizens to enter their data only once to access all public services. The platform consolidated millions of transactions for 200 government entities, saving citizens €97 million in administrative costs and improving security. During the COVID-19 crisis, DXC used the platform to roll out a new web application in less than 2 weeks to issue badly needed emergency aid payments to Flemish entrepreneurs — processing 50,000 applications in the first 4 days.
Continuous optimization. Operations teams face many challenges in keeping hybrid and multicloud estates running at peak efficiency. In complex environments, they must constantly configure and optimize systems for a wide range of factors including compute, memory, storage, latency, security, placement and databases. As requirements change and cloud services evolve, traditional manual approaches to optimization are no longer practical. Many organizations are turning to continuous optimization tools that employ advanced AI automation to optimize all parameters to match workloads to clouds, ensure peak application performance and lower costs.

Continuous optimization typically is seen as a natural extension of DevOps processes for continuous delivery and continuous integration, enabling organizations to rapidly provision, size and shift workloads to the appropriate resources, while ensuring adherence to corporate policies and regulatory requirements. Under DXC’s Technical Doctrine, serverless computing is the preferred method of deployment, with the cloud provider running the servers and dynamically managing the allocation of machine resources — eliminating the need for IT staff intervention. Where serverless is not an option, platform as a service (PaaS) offers a way to offload capacity management issues to a third party. In addition, optimization techniques can also be applied to containers as organizations gradually transform applications and databases and move to modern IT estates.

Intelligent automation. Intelligent automation uses real-time data and machine learning to continuously measure and elevate performance throughout the IT operations environment. Key areas of focus include:

- **Application services automation.** These AI-based technologies proactively detect application issues affecting users and automatically trigger steps for remediation. They also analyze application source code to identify inefficiency, redundancy, unreachable code or flawed logic, thereby reducing defects and improving code maintainability and quality. DXC has seen up to a 30 percent improvement in applications that support productivity and a 50 percent reduction in average time to resolve incidents.

- **IT delivery automation.** Analytics, AI and Lean processes give IT operations a high-definition view of the IT services delivery operations, which yields deeper insights and more useful information. The result: fewer business disruptions, reduced human error and operational risks, and lower costs.

- **DevSecOps automation.** A host of tools automate DevSecOps processes, including continuous integration, continuous deployment and intelligent test automation, which enables more sophisticated testing that more readily adapts to code changes. Using these tools, DXC has helped DevSecOps teams filter out the noise and reduce the time for setting up test automation scripts by up to 40 percent.

- **Security management automation.** Automation of well-established processes for security incident investigation and remediation speeds up the recovery process and gets the business back to normal quickly after an attack.

To the greatest extent possible, organizations should automate known good code for repeatable tasks in development, testing, deployment and operations. The utopia of software delivery is NoOps, where systems are self-healing and respond to events with no human touch.
Platform management. When it comes to platform choice, there is no one-size-fits-all model in the hybrid and multicloud world. Decisions about platforms come down to business needs such as speed or scalability and how the platform fits into the existing portfolio and long-term strategic technology plans. Ideally, the best approach minimizes the amount of change while maximizing business value. That's why platform as a service (PaaS) has become an attractive option for organizations looking to modernize. Examples include:

- **PaaS for SAP.** Deploying mission-critical solutions such as SAP can simplify operations and management. PaaS encompasses the full stack and supports platform automation, simplified processes and enterprise-grade scale. This enables the business to rapidly create and ramp-up or ramp-down the SAP landscapes.

- **Multicloud on VMware.** While it's still a staple of the data center, the VMware platform has rapidly evolved to support complex multicloud environments. Through a managed services environment, organizations can now rapidly provision the application as well as the infrastructure for compute, storage and network. It’s providing a way for enterprises to extend their VMware investments to private and public cloud environments.

- **Managed container PaaS.** Container-based PaaS solutions can be implemented rapidly across multiple clouds. The advantage of this method is a single platform to build, deploy and manage applications with continuous integration and end-to-end security. Environments are continually kept up to date by re-spinning the container with new versions of software, reducing the window needed for patching.

While IT platforms can vary based on use cases and functions, they all need to support strong security controls, identity management and network integration to meet hybrid operating demands.

**Secure the ecosystem.** Security in the hybrid environment is a shared responsibility across cloud services providers, internal IT security teams and security services vendors. Security teams typically manage multiple toolsets that provide monitoring and threat detection for on-premises and multiple clouds, making it challenging to prioritize incidents. Integration with IT service management systems and having autogenerated alerts are important for securing complex environments and managing handoffs between security and IT teams.

Foundationally, a sound data protection strategy is key to securing new IT operating models. Protecting sensitive data and customer privacy are top priorities in the current threat landscape, where ransomware attacks and data breaches are rampant. An understanding of how data is created, accessed, processed, stored and destroyed should guide organizations on implementing security and IT processes and controls that protect data throughout the data life cycle. With more data stored in the cloud and work-from-home becoming the new norm, the traditional enterprise perimeter is expanding.

Organizations must scrutinize how data is accessed and grant access only with well-defined business workflows. In the coming years, the adoption of Zero Trust principles and a security architecture will play key roles in guiding these business process and permitting access to resources based on user privileges.
Zero Trust, a “deny all, allow some” strategy that’s proven to protect IT assets, ensures proactive enforcement of policies to mitigate adversarial attacks and, when successful, ensure access is kept to a bare minimum. Such proactive enforcement is becoming necessary to mitigate adversarial attacks and, even when they succeed, ensure that access is restricted. Ultimately, these protections give IT and the business greater confidence to innovate faster and embrace new business models.

**Conclusion: Next steps toward modern operations**

Highly efficient operations are crucial to the success of the modern enterprise. Getting there starts with a complete assessment of people, processes, technologies, controls and metrics. Key questions include:

- What’s the best approach to integrating our existing hybrid infrastructure?
- How can we automate and continuously optimize to achieve NoOps?
- Are our security measures keeping pace with changing IT environments?
- How can we get a real-time, consolidated view of IT operations?
- How can we ensure that data is easily accessible?
- How can we align IT skills with business needs?

Going forward, organizations will make the move from traditional IT to integrated hybrid operations. Remember that tools are only part of the solution for managing modern environments. Changing the culture and aligning the organization to business demands are also important success factors. These hybrid IT investments will pay off through fast, flexible and secure operations.

**How DXC can help**

DXC Technology is a recognized global leader in helping customer companies achieve complex, enterprise-scale transformation. We build and deploy modernization using agile methodologies including sprints at scale and continuously optimize processes so companies can reduce cost and risk while increasing business agility at every stage. DXC has helped our customers:

- Use automation to improve incident triaging by 90%
- Release applications 46× faster
- Achieve a 100% success rate in recovering 1,000+ disaster declarations

Talk to DXC’s experts about how we use ideation, pilots and proofs of concept to quickly identify your modernization priorities.

Learn more at [www.dxc.technology/ITModernization](http://www.dxc.technology/ITModernization)
About the author

James Miller is chief technology officer and vice president for Cloud and Platform Services at DXC Technology. As part of his role, he builds strong partnering relationships with customers, advises senior leadership on technology trends and initiatives, and provides oversight and thought leadership to grow both DXC and our customers’ businesses. Previously, Jim was a Fellow and industry chief technologist for manufacturing, automotive, aerospace and defense, and strategic accounts at Hewlett Packard Enterprise.