BUILDING A STEP-BY-STEP ROADMAP TO DIGITAL TRANSFORMATION

A Software-Defined Foundation Helps You Compete in an App-Driven World
Table of Contents

Modernizing the Data Center Through Automation 3
Stepping Through Your Roadmap to Transformational Success 3
  From Nurture to Enablement 3
  From Enablement to a Roadmap 3
  Before you dive in, prepare 4
Step-by-Step: Evolving the Infrastructure to Support Transformation 4
  STEP 1: Establishing a Virtual Infrastructure 4
  STEP 2: Building Out to Private Cloud 5
  STEP 3: Extending to Hybrid Cloud 6
  STEP 4: Taking a Strategic Approach to Security 7
    Gaining Insight 7
    Protecting the Organization 7
    Enhancing Control 8
Get Your Bearings and Move Forward 9
OVERVIEW
In this paper, we’ll discuss why an outcome-focused roadmap is essential to guiding digital transformation. We will present use cases that illustrate how IT organizations can employ this type of roadmap to move both their initiatives and businesses forward and position themselves for compelling benefits.

Modernizing the Data Center Through Automation
You know where your business needs to go to stay competitive. But how can you take it there? And how can you be sure your technology and business leaders all have the same destination in mind?

Digital transformation is sweeping across every major geography and industry. Companies of all sizes are reimagining and reconfiguring their organizations so they can get new applications to market faster and respond better to shifting customer demands. They are turning to technology to support the innovation they need—and pull ahead of competitors. To deliver on these aspirations, businesses need close alignment with their IT teams, and a more strategic approach.

Change is challenging for any organization, especially on a transformational scale. Conflicting priorities, short-term focus, and cultural inertia can all conspire to block an organization’s evolution. To build momentum, new initiatives must have a meaningful impact on what people and the business care about. That approach requires a focus on outcomes, and a well-defined roadmap that can take a business from its current state to a future-proof engine for innovation.

Stepping Through Your Roadmap to Transformational Success
Propelling digital transformation is about more than simply technology. It takes awareness and enablement to drive understanding and action.

Nurturing a small group of early champions is a first step toward building the awareness required to build support for a technology initiative. To do this, your IT team will want to target a small group of people and partner closely with them to create initial successes. You can then apply suggestions from these early adopters to refine your ideas, processes, or technologies. They’ll also help you to better understand your target audience. Along the way, be sure to capture and communicate meaningful, targeted success stories from early adopters to further drive awareness, generate a buzz, and develop executive support.

From Nurture to Enablement
As an initiative builds momentum, enabling users is the next step. This includes education on how the new initiative can deliver meaningful results to the business. Eliminating confusion and uncertainty about an initiative creates more value for the people involved and gives you an opportunity to drive business strategy.

From Enablement to a Roadmap
After fostering awareness and enablement, your IT organization can move forward to develop a prescriptive roadmap that encompasses culture, competencies, and capabilities. It is important that the roadmap be business-centric, rather than technology-centric, and focus primarily on achieving measurable outcomes. At its core, the purpose of the roadmap is to lay out a set of capabilities for the future. It helps you move beyond a tactical discussion of speeds and feeds to align business drivers, budget requirements, and the technology required to achieve the objective.
Before you dive in, prepare
A well-defined, outcome-focused roadmap creates alignment across disparate teams and unites them with a common language. While it can be tempting to dive right into the tactical elements of a plan, make sure you lay the groundwork first. As with any significant transformation effort, a successful transformation will encompass not just the technology, but also the people and processes related to it.

To understand your current state and the path to target state, first consider your culture, competencies, and capabilities:

- **Culture**: Who is your primary customer and how are you measured
- **Competencies**: The ability for IT to do something successfully or efficiently
- **Capabilities**: The people, processes, and technologies used to ensure a sustained result

Taking a holistic approach to strategy will not only enable you to transform your technology, but transform your people and processes, too.

Step-by-Step: Evolving the Infrastructure to Support Transformation
IT has long played a key role as infrastructure provider, focusing on driving efficiencies and minimizing costs. Its top priorities include reducing CapEx, data center consolidation and migration, increasing standardization, maximizing stability, and reducing outages.

So how can your IT organization employ an outcome-focused roadmap to guide its transformation? Although the role of an infrastructure provider is somewhat tactical, many opportunities are available for IT to transform itself and build a foundation for a more strategic organization.

**STEP 1: Establishing a Virtual Infrastructure**
A fundamental step in driving digital transformation is migrating to a virtual infrastructure. In this early stage of the journey, your goals likely include reducing CapEx and improving agility by responding to requests faster.

**Which Capabilities Are Required?**
To deliver the outcomes they need, your IT team should focus on enabling four key capabilities:

- **Abstracting and pooling compute and storage resources**: This capability enables IT to deliver and control access to key resources through centralized, secure, integrated authentication. You can also standardize virtual machine templates with operating system build profiles.
  - **Why**: Virtualization of compute, storage, and network assets positions IT for several benefits. It helps reduce redundant data center capacity and costs. It can also provide a foundation for private and hybrid cloud, along with the ability to proactively plan capacity and bursting requirements. Perhaps most important, it enables closer alignment with the business through improved communication of service requirements and demands.
• Providing basic templates for server deployments: This capability focuses on standardization of operating system build profiles based on common policies. It enables template configuration for new hosts, and lets IT avoid manual steps to optimize their deployment processes. This initiative also includes development and implementation of service definition templates.

**Why:** Providing basic templates for server deployment enables faster time to market of service blueprints for specified use cases and helps boost overall agility.

• Monitoring and managing infrastructure performance and capacity: This capability provides IT with a unified performance and capacity management solution. It lets organizations enhance existing incident, event, problem, capacity, and demand management processes to introduce process governance. IT can also establish monitoring for capacity and demand, and support “looking back” and “looking forward” capacity management.

**Why:** Infrastructure monitoring with performance and capacity sets up numerous benefits. More accurate demand and capacity forecasting leads to more efficient budgeting and financial planning. It also helps IT improve detection and resolution rates of infrastructure-related incidents.

• Automatically recovering from hardware failures: This capability lets the infrastructure restart virtual machines in response to hardware failures, as well as operating system failures.

**Why:** Enabling automatic recovery from hardware failures reduces planned and unplanned downtime and maximizes network availability for improved IT organization credibility.

STEP 2: Building Out to Private Cloud
As your IT organization progresses on its journey toward digital transformation, a major milestone on the roadmap is private cloud implementation. Organizations moving to this stage of their evolution may be contending with issues like unplanned workload failures, which can halt key business processes and lead to unplanned downtime. They may be seeking ways to overcome long workload delivery times, as well as a perception of slow IT reaction times.

Which Capabilities Are Required?
To move forward in private cloud adoption, your IT organization should focus on enabling capabilities such as:

• Operating a cloud through organizational improvement: The first step in implementing a private cloud is an organizational one. After an analysis of the current state of its organization, IT should then envision and design a target state, including role customization.

**Why:** Organization empowers IT with the ability to implement and adapt to a cloud operating model more quickly.

• Providing resiliency for business services: A private cloud enables IT to provide more efficient fault-tolerance for business services. This capability could include analytics as a service, as well as analytics dashboards.

**Why:** Continuous availability for business services lets IT leverage platform capabilities to prevent business downtime and outages.

• Automating workload provisioning: IT can introduce a culture of automation at this stage, and fully integrate this new approach with its existing network provisioning services. The technology team should also introduce governance with policy-based...
automation. Enabling improved tracing of workload configuration changes is an important part of this capability.

**Why:** When processes are automated, organizations can more efficiently demonstrate regulatory adherence, through log and audit centralization and the ability to provide automated compliance reports.

- **Providing a self-service portal for IT users:** IT can provide a unified web portal to streamline IT requests. This lets organizations establish a more agile consumption model, supported by a standardized service definition template.
  
  **Why:** With a service-oriented operating model in place, IT can provide more nimble access to the technology resources their constituents need to stay competitive.

**STEP 3: Extending to Hybrid Cloud**

The next milestone on the outcome-focused roadmap centers around the ability to seamlessly extend and scale a software-defined data center to the public cloud. This is very important when you’re facing challenges such as unexpected resource demands within a specific timeframe, or the inability to accurately track service levels.

**Which Capabilities Are Required?**

For organizations seeking to progress toward hybrid cloud, IT should focus on enabling capabilities such as:

- **Expanding virtual infrastructure delivery capabilities across public and private clouds:** The ability to leverage resources on a public cloud when required is a cornerstone of hybrid cloud. As part of their virtual infrastructure delivery capabilities, organizations can also implement solutions to avoid resource leakage and react faster to service needs.
  
  **Why:** Hybrid cloud bursting can help organizations expand and run services on public cloud, while managing both under a single operational model. This capability can also provide support for disaster recovery (DR) initiatives to enhance business continuity.

- **Governing cloud consumption:** As part of improved governance, IT can develop and implement a service cost template, as well as a service-level management template. Effective cloud consumption governance can also provide an onboarding process for accessing dashboards and content.
  
  **Why:** Extending and managing resources provided by public clouds helps maintain control by avoiding shadow IT.

- **Tracking assets and configurations across public and private clouds:** This capability lets IT enhance its existing configuration management processes to introduce process governance.
  
  **Why:** With relevant, timely knowledge, IT can better justify budgets, and keep configurations and services under control. It also helps organizations to avoid resource sprawl and optimize infrastructure usage.

- **Providing metrics relevant to individual services:** Another key capability of hybrid cloud centers on determining key performance indicators (KPIs) per service and providing timely metrics through a centralized dashboard. IT can also enhance its existing service-level management processes through improved governance.
  
  **Why:** Relevant data and well-defined processes support monitoring and decision-making, for better strategic outcomes.

---

**A HYBRID CLOUD CAN HELP YOU AVOID THESE PITFALLS**

- Unplanned workload placements that impact performance in unexpected ways.
- Shadow IT initiatives that introduce uncertainty, and cause security and compliance issues.
STEP 4: Taking a Strategic Approach to Security

In a world of multi-cloud environments and changing threat landscapes, organizations are placing renewed focus on security. They need a more strategic architectural approach to cybersecurity that will align the organization’s security strategy with its most important security priorities. For most companies, the most precious asset they have is the trust of their customers.

Gaining Insight

Enhancing insight into an overall security posture is a foundational requirement for cybersecurity. IT may lack visibility across technology domains, applications, and virtual and physical networks. They may also be contending with long problem detection and resolution times.

Which Capabilities Are Required?

To enhance their cybersecurity efforts through better insight across their environments, organizations can focus on:

• **Visualizing application communication across the network**: Organizations can get real-time understanding of network performance and availability with visibility and analytics across virtual and physical networks.
  
  **Why**: Better visualization across the network enables organizations to identify and resolve issues faster and optimizes network performance with visibility and analytics.

• **Centralizing and analyzing all log and audit data**: Enabling the central collection of critical infrastructure information helps drive faster problem resolution. IT may also audit administrator and user activities to comply with industry standards. They can establish enhanced monitoring to better meet demanding, fast-changing regulatory compliance requirements.
  
  **Why**: This capability helps organizations ensure compliance and support more efficient regulatory attestation.

Protecting the Organization

A solution that thoroughly protects network environments is a fundamental pillar of cybersecurity. Today’s organizations are often burdened by high CapEx and OpEx for their security infrastructures and disaster recovery systems. Their existing anti-malware and antivirus processes can consume large amounts of resources and can be easily disabled by malware or even users.

Which Capabilities Are Required?

To enable the level of protection that’s needed for changing cybersecurity priorities, organizations should focus on capabilities such as:

• **Providing workload and network introspection**: Allows next-generation antivirus and anti-malware integration improve performance and minimize risk.
  
  **Why**: Security is increased because antivirus and anti-malware cannot be disabled within a virtual machine when offloaded by the hypervisor.

• **Providing granular application security and isolation**: Enables IT to optimize the infrastructure for regulatory requirements. IT can provide intrinsic application networking and security, as well as implement application modeling for micro-segmentation processes.
  
  **Why**: Deploying security at an application level, together with dynamic security profiles, enables protection that is impossible to achieve with traditional perimeter-based security solutions.

EVERY COMPANY NEEDS SECURITY THAT:

• Is intrinsic, highly granular, and policy-driven.
• Can be applied consistently to all users, devices, applications, data, and infrastructure environments.
• **Enhancing recovery from data center outages**: Allows IT to comply with disaster recovery (DR) plans and provide high availability for services.

  **Why**: It improves business availability and minimizes potential loss of revenue and liability issues.

• **Preventing behavior anomalies and deviations**: Lets IT observe, alert, and remediate changes to a workload’s intended state.

• **Protecting data with encryption**: Helps ensure the integrity of data regardless of its location; this capability enables both data-at-rest and data-in-flight encryption.

• **Verifying transactions with a distributed ledger**: Enables organizations to verify and settle transactions through a distributed ledger, to help minimize fraud and risk.

**Enhancing Control**

Applying control is another fundamental requirement for effective cybersecurity. But traditional network and security thinking may inhibit the adoption of modern solutions that can meet changing needs. As environments become more virtualized, IT roles and responsibilities may not always be clearly defined.

Organizations may be challenged by poorly understood operational procedures, high CapEx and OpEx associated with their network infrastructure, and long delivery times for network functions.

**Which Capabilities Are Required?**

To ensure the control required for today’s cybersecurity imperatives, organizations should move forward to implement capabilities such as:

• **Including networking and security in automation workflows**: Organizations should provide built-in networking and security into application and infrastructure automation.

  **Why**: When network and security are properly integrated into automation, they can be provided on demand as software. Organizations can exercise increased control over network and security for any service and accelerate provisioning time.

• **Abstracting and pooling network resources**: Providing virtual networks and security services on demand enables greater visibility into both activities. Organizations also need to operationalize network virtualization.

  **Why**: Network virtualization accelerates network provisioning time by facilitating deployment from within the virtual infrastructure administrator’s consoles.
Get Your Bearings and Move Forward

We’ve explored how an outcome-focused roadmap can help IT and business more closely align their operations and evolve organizations to address new imperatives.

But before you can take your business where you want to go, you need to gain insight into where you stand today, in terms of your culture, competencies, and capabilities. As you begin to think about a path to the future, collaborate with key business stakeholders to gain a better understanding of your organization’s business priorities for the next few years. Take a full inventory of the state of your IT organization today, identify potential platforms that could support your transformation, and consider what will be needed, such as new cloud capabilities, support for other geographic locations, and other imperatives.

When you’ve drafted a roadmap, be sure to consider whether your team has the capabilities to actually execute on each of the milestones. Determine what you’ll need to operationalize it and develop an understanding of the amount of time and budget required to make it successful. Spikes in budget are always a risk, so develop your roadmap in a way that will spread your initiative out over a year, in measurable phases where you can demonstrate success.

If you’re seeking a technology partner to help you on your journey, contact your VMware account representative for an in-depth evaluation of your current state—and where you would like to take it in the years ahead. We can help you establish a path to achieve the outcomes you desire in a prescriptive, tailored roadmap.

Start the journey to a modernized data center >