Mirazon

WHITEPAPER

Rethinking Your Infrastructure Footprint

A Practical Framework for Evaluating On-Prem, Cloud, and Virtualization

www.mirazon.com
(502) 240-0404
info@mirazon.com

Table of Contents

Why Infrastructure Reduction & Technology Modernization Matter

Modernization isn't about chasing cloud trends or reacting to industry hype. It's about intentionally reducing unnecessary infrastructure, strengthening operational resilience, and aligning technology with how modern businesses actually operate.

At its core, this is a strategic decision, and below is the practical **"why"** behind each driver.

Rising Costs of Maintaining On-Prem Infrastructure

On-prem infrastructure carries a cost curve that rises every year, even when no new systems are introduced. Hardware ages. Support contracts renew, licensing models shift, and operational overhead increases. What once felt predictable has quietly become one of the most expensive components of running IT.

Hardware Life Cycle Costs

Servers, storage, firewalls, and network gear keep the business running—and they all require refreshes every 3–7 years. These refreshes are almost always capital expenditures, and postponing them doesn't eliminate cost—it increases risk.

As hardware moves beyond its intended lifecycle:

- **Warranty extensions become more expensive**
- **Replacement parts get harder to find**
- **Vendor support becomes limited or unavailable**
- **Performance and reliability decline**

Every year a system stays past its intended lifecycle, the cost and risk increase.

Licensing & Support Renewals

Operating systems and applications evolve continuously, but on-prem environments don't evolve automatically alongside them. New versions require:

- Purchasing updated licenses
- Performing disruptive migrations
- Revalidating integrations and dependencies

Meanwhile:

- Support contracts renew annually
- Vendors shift features into higher-tier licenses
- Legacy versions lose support
- Security patches become limited or unavailable

Organizations often end up paying more to maintain platforms that deliver less protection and flexibility.

Environmental & Facility Costs

Even a small on-prem footprint requires ongoing facility investment:

- Power
- Cooling
- Rack space
- Uninterruptible Power Supply (UPS) and battery maintenance
- Physical security and access controls

These costs don't arrive as a single line item, but they impact the operational budget every month and scale with the environment.

Operational Overhead

Every on-prem system demands hands-on care:

Patching

Firmware updates

Monitoring

Troubleshooting

After-Hours Maintenance Windows

Documentation & Configuration Drift Management

What Is "Configuration Drift Management"?

The ongoing practice of spotting and fixing unapproved or undocumented IT changes so systems stay aligned with their secure, intended setup instead of drifting out of shape.

The larger the footprint, the more time IT teams spend sustaining infrastructure instead of enabling business progress.

DID YOU KNOW?

Organizations report **20–30% reductions in IT infrastructure and operations costs** after cloud migration.

Source

Security & Compliance Pressures

Security expectations have changed, and older on-prem systems struggle to keep up. Aging hardware, unsupported operating systems, and inconsistent patching introduce risk that compounds over time. What used to be “good enough” is now a clear liability.

Modernization reduces that exposure by retiring systems that can’t meet current security standards and shifting workloads to platforms that are actively maintained, hardened, and continuously improved.

Aging Operating Systems & Unsupported Hardware

As systems fall out of vendor support:

- **Security patches stop**
- **Vulnerabilities pile up**
- **Firmware and driver updates disappear**
- **Compliance frameworks flag them as high-risk**

Keeping unsupported infrastructure alive forces IT teams into reactive workarounds instead of proactive protection. Over time, the environment becomes harder to secure and increasingly difficult to manage and protect.

Inconsistent Patching & Configuration Drift

Manual or semi-manual patching leads to:

- Servers running different patch levels
- Missed updates
- Configuration drift
- Increased vulnerability exposure

The larger the on-prem footprint, the harder it becomes to maintain consistency.

Security gaps don’t typically appear as one major failure — they emerge gradually through small inconsistencies that accumulate.

Identity, Access, and Zero-Trust Requirements

Modern security expects:

- Strong identity controls
- Multi-Factor Authentication (MFA)
- Conditional access controls
- Network segmentation

Legacy systems rarely support these natively without custom engineering. Modern platforms do.

Incident Response Limitations

Legacy infrastructure slows incident response and recovery:

- Limited logging and visibility
- Manual failover processes
- Slow recovery times

Modern platforms provide built-in telemetry, automation, and rapid recovery capabilities. Faster detection and response directly reduce downtime, business impact, and recovery costs.

Alignment With CIS Controls

Modernization efforts should align with established security frameworks, not just internal preferences. The CIS Controls (v8.1) provide a practical baseline for securing modern environments, and many of the pressures driving infrastructure reduction map directly to these controls.

- **CIS Control 4** – Secure Configuration of Enterprise Assets and Software
- **CIS Control 5** – Account Management
- **CIS Control 6** – Access Control Management
- **CIS Control 13** – Network Monitoring and Defense

By anchoring modernization to CIS v8.1, you're making decisions based on proven best practices — not subjective risk tolerance or outdated preferences. It keeps the whole effort grounded, consistent, and defensible.

DID YOU KNOW?

Technical debt consumes up to 40% of IT budgets in organizations with legacy-heavy environments.

Source

Operational Efficiency & Scalability

As environments grow, operational friction grows with them. Every additional server, appliance, or platform adds maintenance, patching cycles, and another place where something can fail. Over time, complexity slows IT teams and limits the organization's ability to scale.

Modernization reduces that friction by consolidating systems, standardizing platforms, and shifting workloads to environments that are easier to manage and expand.

Reduced Maintenance Overhead

Larger on-prem environments require:

- More patching
- More monitoring
- More firmware updates
- More after-hours maintenance windows

Every system that remains on-prem adds operational load. Reducing infrastructure footprint directly reduces the time required to maintain it.

Standardization & Simplified Management

Legacy environments often grow organically, resulting in:

- Multiple operating system versions
- Mixed hardware generations
- Inconsistent configurations
- Tools that don't integrate cleanly

Modernization allows organizations to standardize on fewer, more capable platforms. That simplification improves:

A smaller, more consistent environment is easier to operate and more predictable.

Scalability Without Complexity

Scaling on-prem infrastructure usually means:

- Purchasing additional hardware
- Expanding storage
- Reconfiguring clusters
- Increasing power and cooling capacity

Modern platforms scale faster and with less disruption. Growth becomes a planning exercise instead of an operational burden.

Improved Collaboration Across IT Teams

Modern platforms make it easier for teams to work together effectively, whereas legacy environments often rely on:

- Tribal knowledge
- Custom scripts
- Manual processes
- One or two people who “know how that system works”

Modernization enables:

- Shared management tools
- Centralized dashboards
- Consistent processes and workflows
- Better visibility across teams
- Reduced reliance on individual expertise

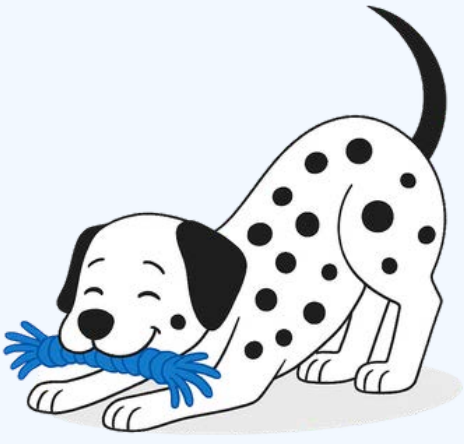
This improves collaboration, reduces bottlenecks, and ensures continuity when staff changes occur.

Faster Response & Reduced Downtime

A modernized environment is easier to support:

- Issues are easier to diagnose
- Failover is more reliable
- Recovery is faster
- Monitoring is more accurate

This leads to fewer outages and shorter disruptions—directly improving productivity across the organization.



Workforce & Productivity Shifts

Work has changed — a lot. Teams are spread out, people jump between devices, and everyone expects secure, anywhere access to the things they need. The problem? Traditional on-prem environments weren't built for this kind of mobility or collaboration. And it shows: slower productivity, higher support overhead, and a user experience that just can't keep up.

Modernization brings your environment in line with how your workforce actually works today.

Remote and Hybrid Work Expectations

Employees today expect:

- Reliable access from wherever they're working
- Consistent performance on any device
- Minimal downtime or maintenance interruptions
- Tools that behave the same inside and outside the office

But on-prem setups often lean on VPNs, old-school authentication, and network-dependent apps—none of which play nicely with a distributed workforce. Modern platforms strip away those bottlenecks and deliver a smoother, more intuitive experience.

Better Collaboration Across Teams

Modern platforms enable collaboration in ways legacy systems simply can't. On-prem environments often depend on:

On-prem environments depend on:

- Shared drives
- Email attachments
- Manual version control
- Tools that don't integrate cleanly

Modernization supports:

- Real-time collaboration
- Shared workspaces
- Consistent access across devices
- Integrated communication tools

The end result? Teams work better together and friction between departments fades fast.

Reduced Dependency on Physical Infrastructure

As the workforce becomes more mobile, relying on physical infrastructure becomes a limitation:

- Users shouldn't need to be on the corporate network to work
- Applications shouldn't depend on local servers to run
- Collaboration shouldn't rely on shared drives or outdated tools

Modernization removes these constraints and supports a workforce that can operate from anywhere.

Current State Assessment: What's On-Prem and Why

Before you can shrink your infrastructure footprint or modernize anything, you need a clean, honest picture of what you actually have—and why it's there in the first place. Most environments don't follow a master plan; they grow like a messy closet. New systems get tossed in quickly, old ones never fully retire, and "temporary fixes" somehow turn into decade-long residents.

A current state assessment cuts through the clutter. It shows what's running, what it supports, and what it really costs the business to keep it alive.

Typical On-Prem Components

Most on-prem environments include a mix of:

- Virtualization clusters
- File servers & application servers
- Domain controllers and identity infrastructure
- Network appliances (firewalls, switches, VPN concentrators)
- Backup & disaster recovery systems
- Legacy line-of-business applications
- Storage arrays and SAN/NAS platforms

Each piece comes with its own operational, licensing, and lifecycle baggage. Getting a clear view of what exists — and how everything connects — is the foundation for any solid modernization plan.

Why These Systems Exist

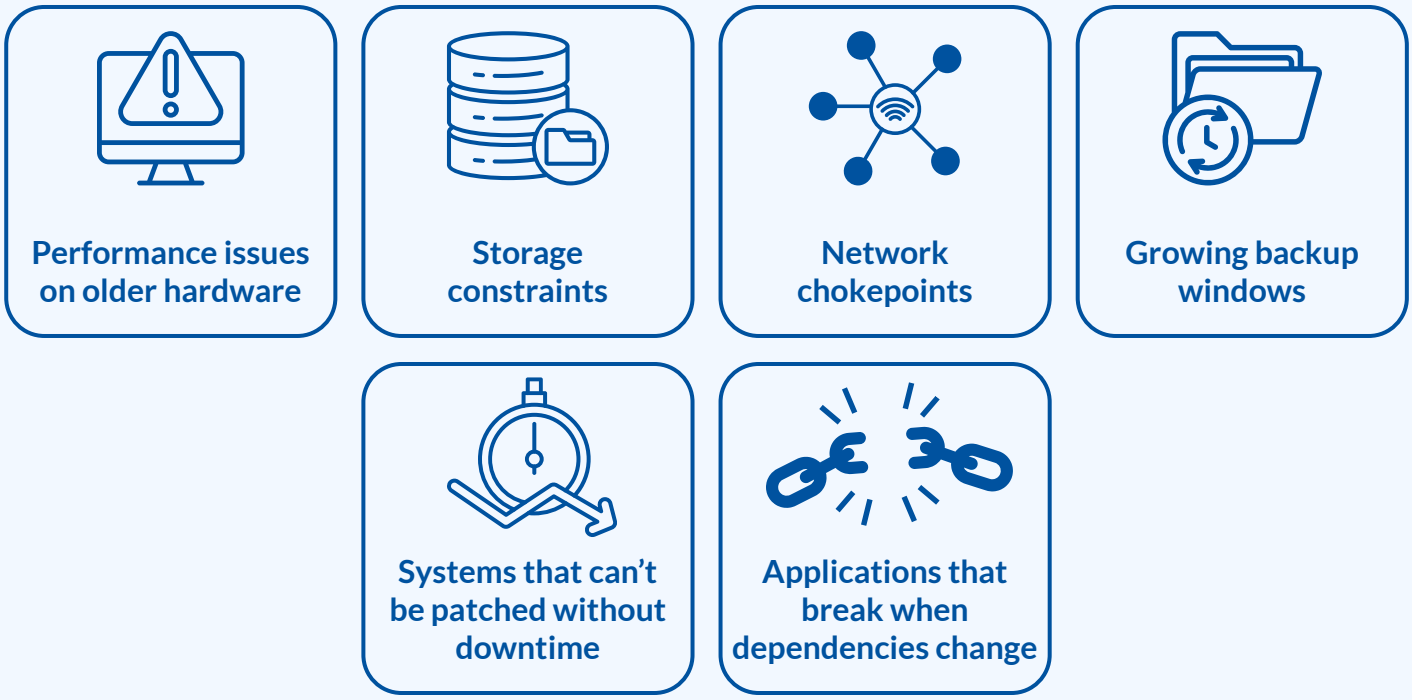
Very few systems exist because someone intentionally designed the environment that way. They're usually there because:

- A business unit needed something quickly
- A vendor required an on-prem install
- A legacy application couldn't be moved
- A previous project left behind infrastructure that still "works"
- The organization grew faster than the environment evolved
- No one had time to revisit older decisions

Documenting *why* each system exists helps determine whether it still serves a real purpose… or if it's just running on inertia.

Current Environment Bottlenecks

As environments age, bottlenecks start to appear:



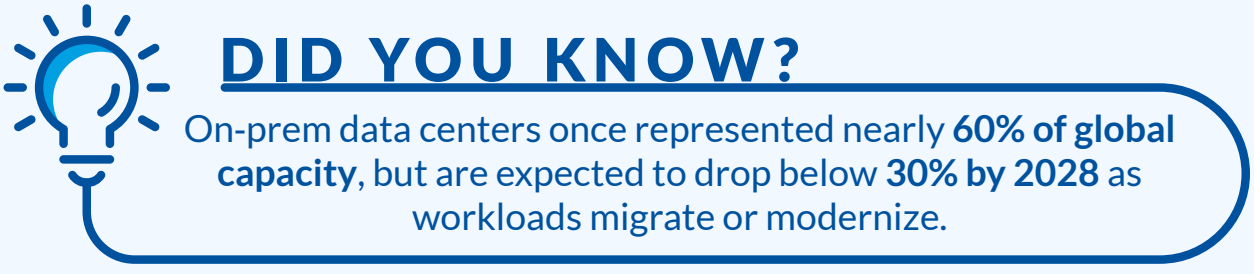
These bottlenecks slow operations, spike support tickets, and add risk. Identifying them early helps you prioritize what needs to move, modernize, retain, or retire (we'll talk more about this later).

Identify Systems That Must Remain On-Prem

Not everything can (or should) move off-prem. Some workloads legitimately need to stay local due to:

- Latency-sensitive operations
- Manufacturing or industrial control systems
- Regulatory requirements
- Hardware-dependent applications
- Specialized appliances that have no cloud equivalent

The goal isn't to eliminate on-prem entirely—it's to *right-size* it. A clear inventory of what must remain helps define the minimum viable on-prem footprint.



Source

Cloud & Virtualization Evaluation

Once you understand your current environment, the next step is figuring out which workloads belong in the cloud, which fit better on modern virtualization platforms, and which should stay on-prem. This isn't about cramming everything into one model—it's about choosing the right landing zone for each system based on business needs, technical requirements, and long-term sustainability.

A structured evaluation keeps you out of the "we've always done it this way," "move everything," or emotionally driven decision traps. Instead, you get a consistent, defensible framework for placing workloads where they make the most sense.

Cloud Readiness

Not every workload is cloud-ready—and even cloud-ready workloads don't always need to move right away. Cloud readiness is all about understanding whether a system can run effectively in the cloud without adding unnecessary risk or complexity. Here's what you should consider:

Application Architecture
Can it run in a virtual machine (VM) or container, or is it tightly tied to on-prem hardware?

Network Dependencies
Does it rely on low-latency connections to local systems?

Authentication & Identity
Can it integrate with modern identity providers?

Data Gravity
How much data does it store, and how often does it move?

Vendor Support
Does the vendor support cloud deployment?

Cloud readiness isn't a simple yes/no checklist — it's an evaluation of effort, risk, and what it will take to move that workload successfully.

Virtualization Strategy

For workloads that aren't cloud-ready—or simply aren't suited for the cloud—modern virtualization is still a powerful, practical option. A well-designed virtualization strategy delivers:

This is where organizations can right-size their on-prem environment:

- Consolidating older hardware
- Reducing the number of hosts
- Standardizing on a single hypervisor
- Improving backup and recovery
- Simplifying patching and lifecycle management

Virtualization isn't "the old way." It's still a core part of a balanced, efficient infrastructure strategy.

Cost Modeling: Capital vs. Operational Expense

Modernization decisions often come down to how you want to spend your dollars:

On-prem = capital expense (hardware, licensing, facilities)
Cloud = operational expense (consumption-based billing)

A reliable cost model should include:

- Hardware refresh cycles
- Licensing and support renewals
- Power and cooling
- Staff time
- Cloud consumption estimates
- Data transfer costs
- Backup and disaster recovery (DR) requirements

The goal isn't to make one option look "cheaper" than the other—it's to understand the real cost of each path so leadership can make smart, aligned decisions.

Security & Compliance Considerations

Security and compliance requirements influence where workloads should live. Key questions you should ask include:

- Are there requirements for where data is stored?
- Does the workload require specific regulatory controls?
- Does the cloud provider meet the necessary compliance frameworks?
- Does the workload rely on legacy authentication or network models?
- Can the system be secured more effectively in the cloud or on-prem?

Security shouldn't be an afterthought — it should be part of the evaluation criteria from the start.

Securing Cloud Environments: MFA, Conditional Access, and Zero Trust

Shifting workloads to the cloud doesn't just change where your systems live—it changes how you secure them. In the cloud, identity becomes the perimeter, and protecting that perimeter takes more than passwords and old-school network boundaries.

A strong cloud security posture includes:

- **MFA for everyone—no exceptions**: Enforce MFA for all users and administrators, and lean toward phishing-resistant methods whenever you can.
- **Conditional Access policies**: Use policies that account for location, device compliance, risk scoring, and session controls so access always matches context.
- **Zero Trust principles**: Make sure you're verifying explicitly, using least-privilege access, and operating with an assume-breach mindset.
- **Privileged access controls**: Protect admin roles, enforce just-in-time access, and maintain well-secured break-glass accounts.
- **Continuous monitoring and logging**: Cloud-native telemetry makes it easier—and faster—to detect issues and respond before they escalate.

These controls ensure your workloads aren't just moved to the cloud — they're secured in a way that meets modern expectations and real-world threats.

Integration With Existing Systems

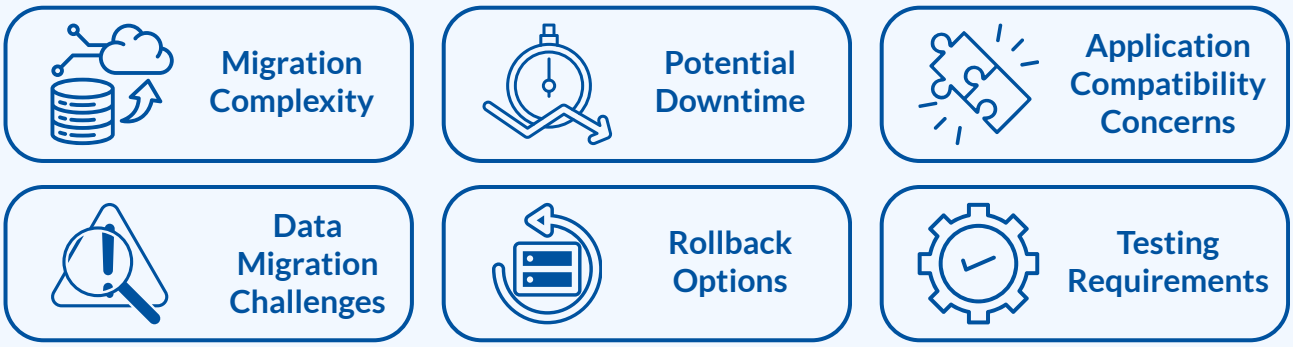
Workloads rarely live in isolation. Integration considerations include:

- Dependencies on on-prem databases or file shares
- Legacy applications that can't move
- Authentication flows
- Network routing and latency
- Application Programming Interface (API) or service-to-service communication

A workload might be cloud-ready on paper but still be a poor candidate if its dependencies can't come with it.

Risk Mitigation

Every modernization effort carries some risk. The evaluation process should uncover:



A strong modernization plan doesn't pretend risk doesn't exist—it manages it through smart planning, thoughtful sequencing, and clear decision criteria.

Move, Modernize, Retain, or Retire

Once you've evaluated your workloads, each one needs a clear next step. This framework keeps everything consistent and grounded in reality—not guesswork or bias. The goal isn't to shove everything into the cloud or keep everything anchored on-prem. It's about putting each system where it actually makes sense based on business value, technical needs, cost, and long-term sustainability.

Every workload falls into one of four paths: **move, modernize, retain, or retire.**

Move

Workloads that are cloud-ready *and* benefit from cloud capabilities should be moved. These are typically systems that:

- Don't require low-latency access to on-prem resources
- Have modern architectures or vendor support for cloud deployment
- Benefit from elastic scaling, global access, or consumption-based billing
- Are easier to secure and maintain in a cloud environment
- Reduce on-prem footprint without introducing operational risk

Moving these workloads cuts down infrastructure overhead and puts them on platforms that evolve automatically.

Modernize

Some workloads can't move as is—but they can be modernized to become more efficient, secure, or cloud-ready. Modernization may include:

- Upgrading operating systems
- Refactoring applications
- Replacing legacy components
- Moving to containerized or service-based architectures
- Consolidating multiple systems into a single platform

Modernization extends the life of critical workloads, reduces technical debt, and lays the groundwork for future migration.

Retain

Some workloads truly do need to stay on-prem. These often include:

- Latency-sensitive systems
- Manufacturing or industrial control systems
- Hardware-dependent applications
- Systems with strict regulatory or data residency requirements
- Specialized appliances with no cloud equivalent

Keeping these workloads on-prem isn't a compromise—it's a strategic choice. The goal is to **right-size** the on-prem footprint so only the systems that genuinely belong there stay there.

Retire

Some workloads no longer deliver meaningful value—or they've already been replaced by better tools. These should be retired to reduce cost, risk, and operational overhead.

Common candidates include:

- Legacy applications with no active users
- Systems replaced by Software-as-a-Service (SaaS) platforms
- Redundant servers or services
- Old file shares or archives that can be consolidated
- Tools deployed for one-off projects

Retiring unused or low-value systems is one of the fastest ways to shrink your footprint and simplify the environment.

Relevant CIS Controls for Modernization Decisions

When you're deciding whether a workload should move, modernize, retain, or retire, the CIS Controls (v8.1) offer a solid, objective lens to evaluate your options. The most helpful ones include:

- **CIS Control 3** - Data Protection
- **CIS Control 4** - Secure Configuration of Enterprise Assets and Software
- **CIS Control 6** - Access Control Management
- **CIS Control 12** - Network Infrastructure Management
- **CIS Control 13** - Network Monitoring and Defense

Using these controls keeps the decision-making grounded in real best practices—not instinct, habit, or opinion—and helps you determine the right landing zone for every workload.

Migration Roadmap

Once every workload has been evaluated and assigned a path (move, modernize, retain, or retire), it's time to build a clear, predictable roadmap. A solid migration plan lowers risk, avoids unnecessary disruption, and makes sure the business knows *what* is happening, *when* it's happening, and *why* it matters.

This is where strategy turns into action.

Planning & Prioritization

Not everything should move at once—and that's a good thing. Prioritization is based on:

High-value, low-risk workloads usually go first. High-risk or highly integrated systems move later, once the foundation is ready.

A clear sequence keeps surprises at bay and keeps expectations properly aligned.

Cost Analysis & Budget Alignment

Modernization works best when the budgeting is predictable. This includes:

- Cloud consumption estimates
- Hardware refresh avoidance
- Licensing changes
- Migration tooling or services
- Staff time and training
- Decommissioning costs for retired systems

The goal is to sync the roadmap with budget cycles so leadership understands both the short-term investment and the long-term savings.

Pre-Migration Preparation

Successful migrations aren’t about speed—they're about preparation. This phase includes:

- Validating application dependencies
- Confirming authentication and access requirements
- Ensuring data integrity and backup readiness
- Establishing rollback plans
- Testing connectivity and performance
- Preparing users for upcoming changes

Good prep work reduces downtime and helps avoid last-minute chaos during cutover.

Migration Execution

Execution should be calm, controlled, and repeatable—not a fire drill. Key elements include:

- Moving workloads in controlled waves
- Performing cutovers during low-impact windows
- Monitoring performance and stability in real time
- Coordinating with application owners and business units
- Documenting each step for consistency and auditability

A disciplined execution process makes migrations predictable instead of stressful.

Validation & Optimization

After each migration wave, workloads need to be validated to ensure everything’s running as expected.

This should include:

This step ensures stability and helps catch issues early so each subsequent wave runs smoother.

Documentation & Maintenance

Modernization isn't a one-time event—it's an ongoing practice. After migration:

- Update architecture diagrams
- Document new processes and standards
- Retire or decommission old systems
- Review monitoring and alerting
- Establish lifecycle management for the new environment

Clear, current documentation keeps the environment healthy, manageable, and aligned with business needs long-term.

Alignment With Information Technology Infrastructure Library (ITIL) Practices

Modernization fits hand in glove with ITIL's emphasis on structured, repeatable, and measurable service management. ITIL helps make sure the environment doesn't just get modernized—it stays stable and well-governed. The key practices that support long-term success include:

Service Design

Ensures new architectures are intentional, documented, and aligned with real business needs instead of wishful thinking.

Change Enablement

Provides controlled, auditable processes for updates, migrations, and lifecycle changes—no surprises, no cowboy changes.

Service Operation

Standardizes monitoring, incident response, and day-to-day workflows so operations run smoothly and consistently.

Continual Service Improvement (CSI)

Encourages ongoing review of performance, cost, and risk to make sure the environment stays aligned over time—not just on day one.

Referencing ITIL highlights an important truth: modernization isn't a one-time effort. It's an ongoing discipline that becomes part of how the business operates every day.

Where You Go From Here

You've got the clarity, the framework, and the path—now it's about building momentum. Modernization works best when it's steady, transparent, and aligned with what the business actually needs next. Start small, build confidence with early wins, and let those wins create momentum. Each improvement compounds, making the environment easier to manage, easier to secure, and easier to scale.

And if you want a partner who can help you plan it, validate it, and get it done without the headaches, **reach out to us**! Our team is ready to walk with you through the process and help you turn your roadmap into real-world progress.

Contact Us

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com