COHORT CONSULTING GROUP

AI-READY CLOUD MODERNIZATION

Accelerating ROI, Strengthening Security, and Enabling AI at Scale

Contents

Executive Summary

Despite widespread cloud adoption, most enterprises still face challenges related to legacy systems. While **83% of executives see modernization as key**, only 27% have implemented significant changes.[1] Although **95% of IT decision-makers find modernization vital,** only 18% engage in continuous efforts.[2] Rising cloud costs, security breaches, and stalled AI projects create challenges, while boards seek clear value from CIOs.

Many cloud migrations intended to save costs have led to higher expenses and inefficiency. Nearly half of cloud initiatives encounter unexpected costs, and a significant portion of IT budgets remain tied to legacy systems, hindering innovation. Legacy environments also increase vulnerabilities, leaving enterprises exposed to threats and regulatory compliance issues.

When addressing cost and security, organizations confront data silos and poor data quality, which prevent AI initiatives from advancing. Data scientists often spend excessive time on data preparation, which stalls projects. Research indicates that **80-90% of CIOs associate AI adoption with the modernization of applications and data platforms**, emphasizing the need for reliable data pipelines to achieve AI readiness.

IT is at a pivotal moment. Even with years of investment in virtualization and cloud, legacy architectures hinder progress. Boards are demanding answers regarding rising IT costs, fragmented data, and security postures. Key priorities include scaling AI safely, building trustworthy data foundations, optimizing cybersecurity, controlling costs, and addressing talent shortages.

Research highlights this issue: **90% of organizations believe that legacy systems must be modernized to unlock their full AI potential,** and 45% cite unforeseen costs as a significant barrier to this goal. Modernization is now a board-level concern, linked to cost efficiency, security, and AI readiness, yet financial unpredictability, legacy complexities, and skill deficits slow progress.

[1] IBM: Modernizing Applications on Hybrid Cloud
[2] RedHat: The State of Application Modernization

The Modernization Imperative

Enterprises face a critical juncture. CIOs have invested in virtualization and cloud services, but legacy architectures hinder agility. Boards demand clarity on rising IT costs and the fragmented state of data security. **Gartner's 2025 CIO Report outlines five pressing priorities:**

1. Safe and effective AI scaling
2. Integrated, trustworthy data foundation
3. Optimized cybersecurity in hybrid IT
4. Controlled cloud and supplier costs
5. Addressing talent and skills shortages

"Application modernization isn't just another IT buzzword. ***It's a business imperative."***

Research indicates that **modernization is now a board-level concern**, linking cost efficiency, security, and AI readiness. Delays stem from financial unpredictability, legacy complexities, and skill gaps. Consequences include:

- 1/3 of IT budgets are tied to legacy maintenance
- Increased cyber risk; 56% cite security as a top modernization driver
- Stalled AI programs: 80-90% of CIOs connect production AI to modernized applications and data

Without modernization, enterprises face higher costs and greater risks. Organizations need to turn modernization into a systematic, repeatable process that integrates financial governance and security, accelerating outcomes with automation and AI agents. By aligning modernization with cost savings, security, and AI readiness, Cohort empowers CIOs to lead with a pragmatic path forward—one that reflects the lessons learned from years of hybrid cloud adoption and translates them into predictable, measurable results.

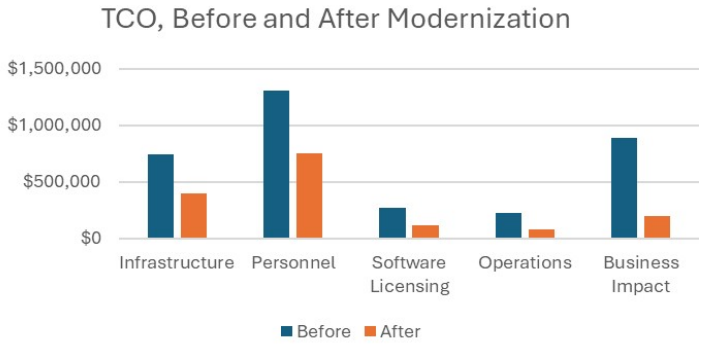
AI-Ready Modernization

FinOps Foundations

The financial promise of cloud was clear: lower costs, elastic scaling, and reduced infrastructure overhead. Yet for many organizations, the opposite has occurred. Lift-and-shift migrations often replicate inefficiencies, leaving CIOs with higher IaaS bills than before.

Rackspace research shows that **45% of organizations encounter unforeseen cloud costs**, while Gartner notes that enterprises without FinOps maturity overspend by as much as **30% annually**.

Meanwhile, legacy licensing contracts and redundant services compound the issue, while 29% of IT budgets remain tied up in legacy maintenance. Boards increasingly ask CIOs to prove where the savings are—and too often, the numbers don't add up.



Cost reduction can come from five sources:

- **Infrastructure Reduction:** Shifting from VMs to PaaS and serverless cuts infra costs by 30–50%.
- **Personnel Efficiency:** Automation reduces manual ops by 20–30%, freeing staff for higher-value work.
- **License Rationalization:** Retiring legacy OS, DB, and middleware contracts reduces licensing by 15–25%.
- **Operational Efficiency:** FinOps guardrails, policy-as-code, and optimized resource sizing eliminate 20–40% of cloud waste.
- **Business Impact:** Address the impact of performance and availability issues on the business, reducing maintenance and downtime

Evaluation Criteria for FinOps

Cohort's ROI model evaluates each workload across five dimensions:

1. **Current TCO Baseline**
    - Infrastructure: $X/month (compute, storage, network).
    - Personnel: $Y/month (admin, support, DBA hours).
    - Licensing: $Z/month (OS, DB, middleware).
    - Operations: monitoring, DR, managed services.
    - Business impact of downtime or inefficiency.

2. **Target State**
    - Replatform/refactor to PaaS (App Services, SQL Database, Functions).
    - Automate ops with IaC + CI/CD.
    - Embed FinOps controls.
    - Rationalize or retire redundant systems.

3. **Cost Savings Potential**
    - % reduction in infra spend.
    - % reduction in ops effort/FTE hours.
    - % licensing savings.
    - Avoided downtime/incident costs.

4. **Investment Required**
    - One-time modernization cost.
    - Training or reskilling expenses.

5. **Payback & ROI**
    - Payback Period: typically, 12–15 months.
    - ROI %: (Savings – Investment) ÷ Investment.
    - Cumulative Value: savings realized at 24, 36 months.

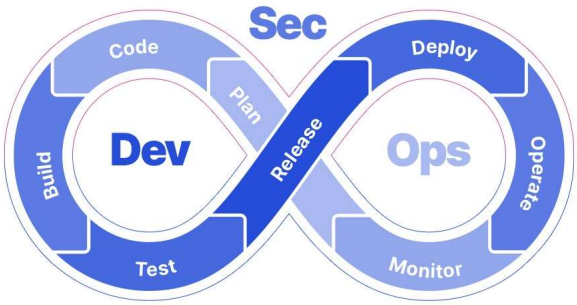
Modernization is not about moving everything at once; it's about **targeting the 40–50% of workloads** where ROI potential is highest. This requires structured discovery, workload classification, and ROI modeling at the application level.

The outcomes from a cost optimization are clear: CIOs who adopt workload-level ROI analysis gain the ability to present modernization as a **self-funding initiative**.

DevSecOps Foundations

Legacy applications are often secured through perimeter-based controls and manual review processes that are poorly suited to modern cloud-native delivery. As delivery velocity increases through modernization and AI-driven change, security controls applied late in the lifecycle introduce friction, rework, and risk. In many enterprises, security remains disconnected from delivery pipelines, resulting in inconsistent "shift-left" adoption, fragmented visibility, and compliance that is episodic rather than continuous.

Industry research and practitioner experience increasingly point to **DevSecOps** as the necessary evolution. DevSecOps extends DevOps by integrating security directly into the software delivery lifecycle—planning, development, testing, release, and operations—so that security becomes a shared responsibility enforced through automation and policy, rather than a late-stage approval step. The objective is not additional tooling, but consistent, repeatable security embedded into the way software is built and delivered.



Compliance requirements such as SOC 2, ISO, PCI, and HIPAA are addressed through **policy-as-code and automation**, enabling continuous compliance rather than manual, point-in-time audits. Security controls generate evidence as part of normal delivery operations, improving audit readiness and reducing operational overhead. DevSecOps practices are implemented as part of an operating model—aligning people, processes, and platforms—rather than as isolated tooling initiatives.

Delivered through architect-led execution and supported by AI-assisted automation, Cohort's DevSecOps Foundations improves **Security-in-Delivery Maturity**—a measurable indicator of how consistently security is integrated across the delivery lifecycle. The result is reduced risk exposure, increased deployment confidence & velocity, and security that scales with cloud modernization and AI adoption, supporting innovation rather than constraining it.

Evaluation Criteria for DevSecOps Maturity

Cohort's discovery process evaluates each workload and delivery team against a structured **DevSecOps maturity framework**. This assessment ensures security is not treated as a post-deployment control, but as an integrated capability across the software delivery lifecycle. The evaluation focuses on how consistently security is embedded into planning, development, testing, release, and operations.

1. Security Integration in Delivery Pipelines

- Are CI/CD pipelines instrumented with automated security checks (code scanning, dependency analysis, configuration validation)?
- Are security controls enforced consistently across environments (dev, test, staging, production)?
- Are pipeline failures triggered automatically when security policies are violated?

2. Identity, Secrets, and Access Management

- Is identity integrated into delivery pipelines using centralized identity providers?
- Are secrets, keys, and certificates managed through secure vaults rather than hardcoded or manually distributed?
- Are least-privilege and role-based access controls applied consistently across pipelines and runtime environments?

3. Vulnerability and Dependency Management

- Are application dependencies continuously scanned for known vulnerabilities?
- Are vulnerability findings prioritized, tracked, and remediated as part of normal development workflows?
- Is there defined ownership and SLAs for vulnerability remediation?

4. Policy-as-Code and Continuous Compliance

- Are security and compliance requirements codified and version-controlled?
- Are compliance policies automatically enforced during build and release stages?
- Is audit evidence generated automatically through pipeline execution and platform telemetry?

5. Observability, Monitoring, and Feedback Loops

- Is security telemetry collected across pipelines, platforms, and runtime environments?

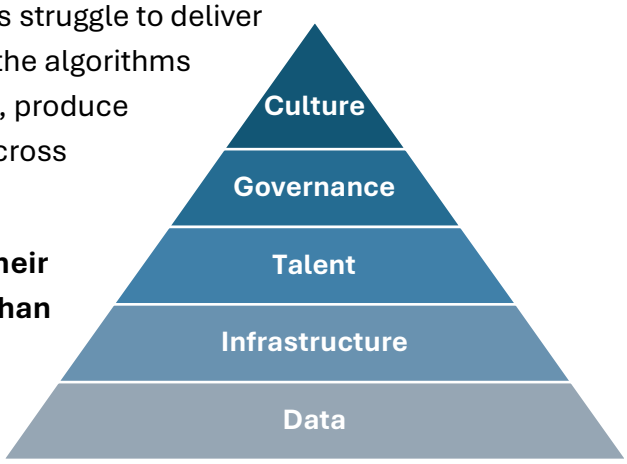
- Are security events and policy violations visible to both engineering and security teams?
- Are feedback loops in place to continuously improve controls based on incidents, near-misses, and audit findings?

When modernization addresses these DevSecOps criteria, organizations move from **reactive security** to **security embedded by design**. Risk is identified earlier, compliance becomes continuous, and delivery teams gain confidence that security supports velocity rather than obstructing it.

The outcome of DevSecOps modernization is clear: **improved security posture, increased deployment confidence, and audit readiness achieved through consistent, automated controls across the delivery lifecycle**.

AI Foundations

AI is a board-level priority, but most enterprises struggle to deliver production AI solutions. The root cause is not the algorithms but the data. Legacy systems trap data in silos, produce inconsistent formats, and duplicate records across environments.



AI Readiness Pyramid

Data scientists report spending 70–80% of their time cleaning and normalizing data, rather than building models. This results in stalled AI initiatives that fail to move beyond pilots. Without modernization, the promise of AI remains unrealized, frustrating directors and eroding confidence in IT leadership.

AI systems rely on high-quality, accessible data, but many businesses lack sufficient training data or have disconnected systems. This phase focuses on building the necessary technical foundation.

- Applications and databases are modernized into Azure-native services such as SQL Database, Synapse, Cosmos DB, and Databricks.
- Data pipelines are established to cleanse, normalize, and enforce governance, ensuring that downstream AI and analytics workloads are fed with reliable and trustworthy data.
- Event-driven architectures and APIs make data accessible in real time, eliminating latency bottlenecks and enabling AI models to operate with fresh inputs.

CIOs gain confidence in advancing AI strategies, directors see progress toward digital transformation, and engineers inherit modern data architectures built for innovation.

Evaluation Criteria for AI Foundations

Through its discovery process**, Cohort evaluates workloads against a structured framework for AI readiness.** This ensures modernization decisions are tied not only to cost and security outcomes but also to the ability to enable AI at scale. Key evaluation dimensions include:

2. **Data Availability**
    - Is the application generating data in a way that can be consistently accessed?
    - Are logs, transactions, and interactions captured in structured or semi-structured formats that can be ingested?

3. **Data Quality and Structure**
    - Are datasets normalized, de-duplicated, and free from systemic errors?
    - Do schemas follow consistent models that allow integration across applications?

4. **Integration Capability**
    - Can the workload expose or consume APIs?
    - Does it support event-driven patterns (e.g., messaging, streaming) that enable near-real-time AI processing?

5. **Scalability and Performance**
    - Can the workload scale elastically to handle the data volumes and compute demands of AI workloads?
    - Does the architecture support modern platforms such as Azure Synapse, Databricks, or Cosmos DB for distributed analytics?

6. **Governance and Security**
    - Are access controls, lineage, and audit trails in place for sensitive data?
    - Does the workload comply with regulatory frameworks (HIPAA, SOC2, ISO) that govern AI use in regulated industries?

When modernization addresses these AI readiness criteria, enterprises create the conditions for the adoption of AI at scale. Data platforms are no longer fragmented and brittle; instead, they are unified, governed, and consumable**.**

The outcome from AI-Ready Data Modernization is clear: a future-proof data foundation that accelerates AI adoption across the enterprise.

The Broader Benefits of Modernization

The promise of modernization extends beyond lower costs, stronger security, and enabling AI. Those are fundamental pillars, **but the larger story is about business agility**, the ability to adapt quickly, seize opportunities, and deliver new value faster than competitors.

Legacy applications are notoriously slow to change; even minor updates can take weeks of regression testing. Modernization breaks down monoliths into modular, cloud-native services that can be deployed and scaled independently. Gartner research shows that enterprises adopting modern architectures can reduce release cycles from months to weeks, dramatically increasing responsiveness to customer and regulatory demands. For business leaders, this translates into faster time-to-market for products, services, and digital experiences.

Modernized platforms are inherently more resilient. By leveraging distributed cloud services, automated recovery, and observability tooling, enterprises can withstand failures without disrupting customer-facing operations. The benefit here is not just uptime—it's business continuity. Modernization allows CIOs to present the board with clear evidence that critical systems can survive outages, cyber incidents, or unexpected demand spikes.

Modern systems also improve usability for both internal and external stakeholders. For customers, this means more reliable, personalized, and secure digital services. For employees, modernization reduces toil: developers spend less time patching and more time building, while end-users benefit from smoother, faster applications. Forrester highlights that organizations that modernize can see **20–30% gains in employee productivity** due to reduced manual work and streamlined processes.

Ultimately, modernization serves as the foundation for innovation. With flexible architectures, governed data, and scalable platforms, enterprises can adopt new technologies faster—whether that's AI, edge computing, or industry-specific platforms. Modernization doesn't just support today's strategy; it makes organizations future-proof, able to integrate the next wave of digital capabilities without starting from scratch.

AI-Ready Modernization Framework

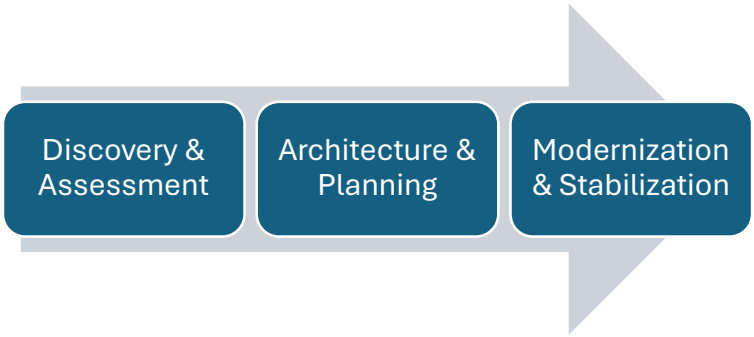
Modernization is **often perceived as a series of one-off projects**, each executed differently and with unpredictable results. Cohort's Modernization Framework redefines it as a repeatable, predictable engineering discipline.

At its core, the framework distinguishes between strategy and *execution*. Upfront discovery identifies workloads, inventories, technical and financial baselines, and scores them against criteria such as cost optimization, security posture, and AI readiness.

This creates a structured pipeline of modernization projects, sequenced by business impact and ROI. By decoupling the decision-making process from execution, organizations avoid paralysis and gain a clear roadmap that allows investments to be justified at the board level.

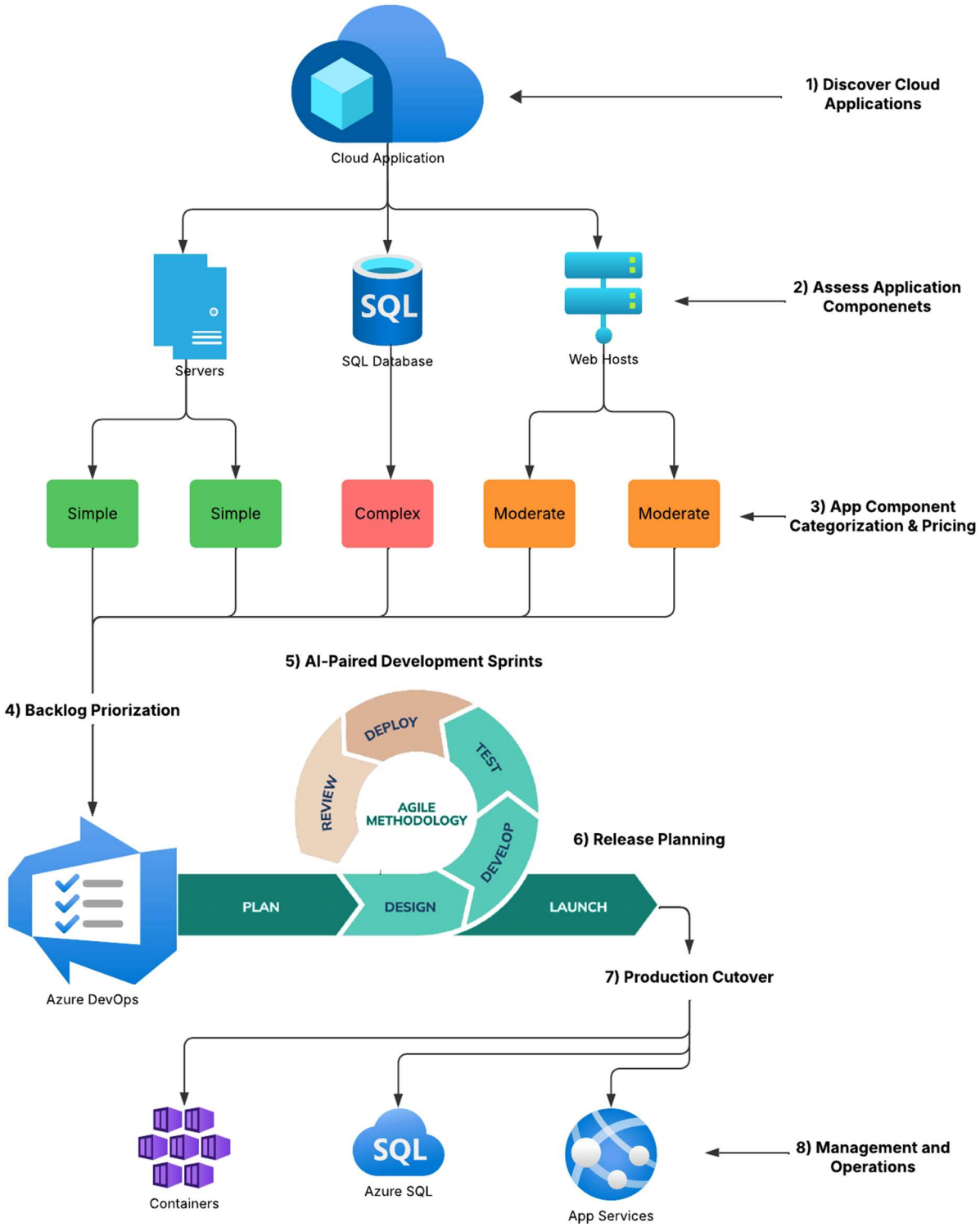
Project execution is then delivered through an offshore POD-based delivery model. Each POD is a cross-functional unit that combines the skills needed for application, data, and security modernization. The onshore strategy team provides architecture oversight, business alignment, and ROI governance, while offshore delivery PODs handle the day-to-day engineering work across multiple workloads concurrently.

Specialty PODs—such as Data Architecture, Security, and Automation—act as accelerators, embedding best practices like policy-as-code compliance, FinOps guardrails, and AI-ready data pipelines. This modular model ensures that modernization is both scalable and standardized.



Finally, the framework emphasizes automation and continuous improvement. Infrastructure-as-Code, CI/CD pipelines, and AI agents are built into the delivery lifecycle, reducing manual effort and eliminating variance. In this way, the Cohort Modernization Framework not only delivers immediate cost, security, and AI benefits but also establishes modernization as a continuous capability rather than a stop-start initiative.

Diagram: The Cohort Modernization Process



Business Outcomes

The true measure of modernization lies in the **outcomes achieved** rather than the **technologies used**. CIOs must demonstrate financial value, mitigate risks, and foster business agility and innovation to drive growth.

Executed with discipline, modernization can yield significant savings, typically **30-50% in infrastructure and operations costs**, with payback periods of 12-15 months. IBM's research states re-architected applications can **reduce maintenance costs by 30-50% and infrastructure costs by 15-35%.**

As the cost of security breaches continues to rise, modernization integrates Zero Trust principles. It automates compliance and DevSecOps pipelines that address vulnerabilities preemptively, leading to measurable resilience with reduced breach likelihood and improved regulatory assurance.

AI adoption is increasingly critical, with **80–90% of CIOs acknowledging** the need for app and data modernization. Modernization on cloud-native platforms enforces governance and allows for real-time access, transforming data into a revenue-generating asset.

For customers, modern platforms ensure reliable and personalized digital experiences, enhancing loyalty. Internally, modernization streamlines manual tasks for developers and enhances IT operations, resulting in **productivity gains of 20–30%** by reducing friction.

Crucially, modernization fosters innovation by diminishing technical debt and embedding agility, allowing organizations to adopt new technologies quickly. It should be viewed as an operating model for sustained competitiveness rather than a one-time project.

Ultimately, modernization impacts not just IT but the entire enterprise, strengthening financial models, resilience, and workforce capabilities while unlocking new revenue opportunities. CIOs who link modernization to ROI, Security, AI Readiness, Agility, Experience, and Innovation will exceed board expectations and drive the business forward with confidence.

Next Steps

Successful modernization begins with clarity. Organizations that struggle most often lack alignment on which workloads to modernize first, which business outcomes matter most, and how to sequence investments to deliver measurable value.

Cohort helps enterprises establish this clarity through a **Modernization Strategy Workshop**—a focused executive session designed to align business, technology, and security leaders around modernization priorities. The workshop identifies the primary drivers for modernization—cost optimization, security, and AI readiness—and produces an initial shortlist of candidate applications for deeper evaluation.

Following the workshop, Cohort conducts a structured **Discovery** to inventory applications, platforms, and delivery pipelines, establishing technical and financial baselines. Workloads are evaluated across cost optimization potential, security posture (including DevSecOps maturity), and AI readiness, enabling objective comparison and early identification of high-impact opportunities.

Insights from discovery are synthesized during the **Assessment** phase into a prioritized modernization roadmap. This roadmap sequences workloads by ROI and complexity, defines target modernization approaches, and outlines the delivery plan required to achieve measurable outcomes.

Execution then moves into the **Modernization** phase, delivered through Cohort's specialized Modernization AI-powered delivery PODs. Engagements are **fixed-price** and outcome-driven, providing predictable delivery while maintaining velocity. All work is owned and operated by experienced architects and engineers with deep backgrounds in Microsoft, AWS, and large-scale enterprise modernization.

By progressing through **envisioning, discovery, assessment, and modernization**, enterprises move from strategy to execution with confidence and achieve predictable, repeatable, and scalable **business outcomes**.

Schedule your free modernization strategy briefing today.

contact@cohortcg.com

www.cohortcg.com

COHORT
CONSULTING
GROUP