DMI

NAVIGATING THE CLOUD MIGRATION MAZE

Many organizations have embraced the cloud only to experience disappointing business and operational outcomes. This guide offers innovative, strategic solutions to the challenges organizations face when embarking on the cloud migration journey.

FOREWORD

Hello,

As a fellow CTO, I understand the complexities and constant evolution of cloud migration, alongside associated platforms and technologies. Cloud migration is more than just a one-off project; it's a journey of digital modernization and strategic endeavor of the highest order, demanding the application of the latest insights and practical approaches.

In navigating today's dynamic tech landscape, we understand the formidable challenges presented by legacy applications and architectures. Once stalwarts of reliability, these systems now act as barriers to agility, scalability, and security. Their shortcomings not only impede technological progress but also pose a significant challenge in delivering seamless experiences to citizens, customers, and users in our fast-evolving digital era. Addressing these challenges has become imperative to ensure a future-ready and user-centric digital ecosystem.

This guide is a product of our collective experiences at DMI and beyond, in supporting digital transformation for some of the largest organizations globally, both within the Public and Private Sectors. It is not a list of promises; instead, it offers real insights, fresh perspectives, and proven strategies honed through hands-on experiences.

We hope you find value in these pages as you navigate the cloud migration maze.

Many thanks to Ajay Shukla, Eric Hutchins, Benjamin Mourad, Liv Crowe, Tushar Phadke, Rakesh Pal, Aniket Taware, Charlie Shifflett, Avery Arbore, and Rohit Shahakar for their contributions to this resource.

Best Regards,

Gary Wang
Chief Technology Officer, DMI

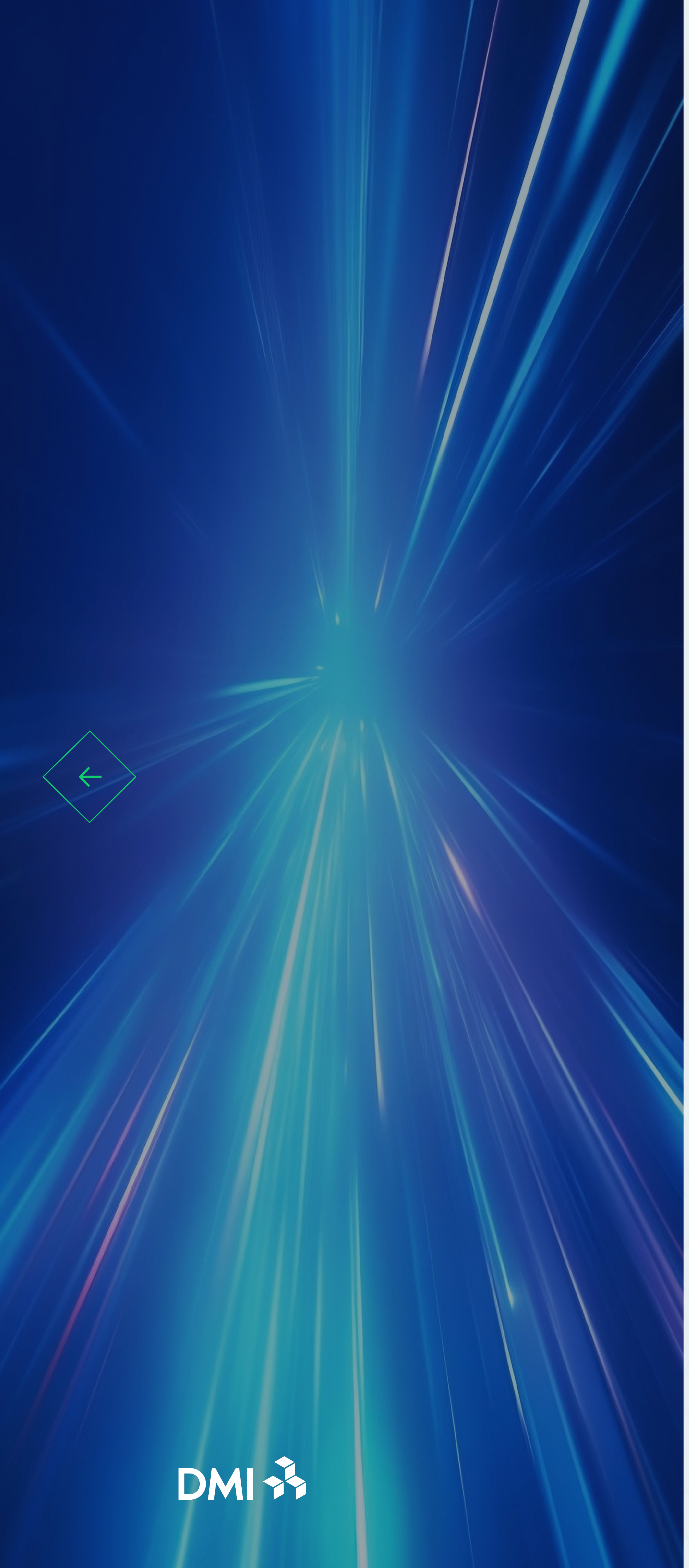


TABLE OF CONTENTS

CLOUD MIGRATION REALITIES: NAVIGATING COSTS, CULTURE, AND COMPLEXITY

Over the last 10 years, many enterprises have embarked on cloud migration projects, only to find themselves mired in a maze of twists and turns leading to disappointing business and organizational outcomes.

'The challenges faced by these organizations can range from institutional resistance from within the organization leading to poor user adoption, to technical issues relating to legacy applications, to lagging project timelines and budget appropriation.

In our experience, here are the most common challenges faced by organizations embarking on a cloud migration:

- Post migration cloud costs exceeding expectation
- Lack of cloud expertise
- Cultural resistance
- Hurdles for implementing security in cloud environments
- Navigating ATO (Authority to Operate) challenges in Federal cloud migrations and overcoming continuous ATO obstacles unique to Federal environments
- The time and effort required to re-factor legacy applications and to transform data services

Cloud Migration is more than just a technology change. It brings in new business models, accelerates service modernization and new service delivery, and demands new operating processes and an agile organizational culture.

For example, managing the public cloud spend has been a formidable challenge for organizations. Many organizations that migrated to the cloud have experienced cost overrun. Cloud is a form of utility computing. All running resources in the cloud are billable services. Therefore, it is very important for an organization to implement a rigorous FinOps practice to maintain a real-time total visibility on cloud expense, establish policies and automate governance, detect waste and right-size resources continuously, and constantly review and optimize purchase plans. Forrester projects that the FinOps Open Cost and Usage Specification (FOCUS) standard, an initiative driven by the FinOps Foundation (a part of The Linux Foundation's non-profit technology consortium), will help to normalize cloud billing in 2024.[1] Microsoft and Google were early supporters, and AWS has recently joined FinOps, with its acceptance of FOCUS. The result: a vendor-neutral, multicloud view of resources. This will enable non-IT stakeholders, such as the CFO's office and vendor management, to better engage with cloud operations teams.

After all, FinOps should be a shared responsibility between the FinOps team and other departments and project managers who own the workloads. For organizations that cannot afford a dedicated FinOps team, such organizations should keep FinOps efforts decentralized among various departments and project teams. The responsibility of keeping cloud costs under control should be fully delegated to the respective teams in the absence of a dedicated FinOps team.

Another challenge is the lack of organizational readiness in adapting to the technology, process, and business changes demanded by cloud computing. Those organizations that migrated to cloud without adequately developing cloud skill sets, adjusting service management processes, optimizing business and service delivery strategies, managing stakeholders communication, and building an agile and DevOps culture, often failed in achieving the anticipated benefit. This failure often led to service performance degradation, the loss of confidence from management team, and unhappy customers and users. Preparing organizational readiness with an effective Organizational Change Management (OCM) practice throughout the cloud migration process is very important.

The third challenge is the application modernization challenge. Modernizing legacy applications with cloud native architecture is a common goal of cloud migrations. However, refactoring legacy applications traditionally has been a lengthy and costly effort. In recent years, AI-power code analysis, business logic analysis, code refactoring, and code generation solutions have proven to be effective accelerators. Leveraging Low-Code/No-Code solutions to re-architect / re-platform applications can be another effective approach to address this challenge.

CLOUD ECONOMICS AND FINANCIAL MANAGEMENT: ADDRESSING THE CLOUD COST CHALLENGES

Every cloud migration project needs to be built upon an understanding of cloud economics -- specifically, cloud computing's costs, benefits, and the underlying economic principles that drive them.

In some cases, the advantage of cloud economics is Total Cost Reduction (TCO), but there are many other qualitative benefits of cloud migration. Cloud computing can enable businesses to better manage their IT expenses such as avoiding upfront hardware and software costs and ensuring flexibility to provision resources according to requirements. Since cloud resources can be removed at any time, migrating to the cloud can provide the elasticity and scalability needed for development projects, as well as for applications in production with fluctuating service demands. Cloud computing also offers qualitative benefits, such as increased agility, allowing businesses to quickly deploy new applications globally, scale resources to meet surges in demand, and adapt to changes in the environment. Cloud also enables innovation acceleration by providing access to a broad spectrum of cloud-based services and tools, expediting the development and launch of new products and services.

In IT services, Total Cost of Ownership (TCO) gauges the overall costs of owning and operating an IT system, including hardware, software, financing, maintenance, support, power and cooling, and security to access facility. It is important to apply the concept of TCO to compare the cost of running applications in cloud with the cost of running them on premises. The selection of appropriate pricing models and CSP savings plans, like pay-as-you-go, reserved instances, and spot instances, is crucial, ensuring proper cost structure that is aligned with application availability, performance, and business requirements. Additionally, cost optimization strategies, such as resource right-sizing, utilization of reserved instances, resource elimination, scheduling resource shutdown during non-business hours, and storage tiering play a pivotal role in enhancing cloud economics.

One important factor to any cloud economics model is a quantitative TCO comparison between cloud and data center environments. The model should also include an analysis of the qualitative benefits that would come with migrating workloads to the cloud. While in some cases, TCO in the cloud may appear higher than on-premises data center environments, the qualitative benefits of the cloud -- scalability, security, and availability -- are far superior to on-premises legacy environments.

The following are the key quantitative and qualitative benefits that organizations can cite in favor of a cloud migration project:

COST REDUCTION

A cloud migration can lead to cost reduction by taking advantage of elasticity, scalability, and automation features available in the cloud. This flexible scaling results in significant cost savings for workloads with fluctuating service demands. This also includes the reduction of overheads related to maintaining and managing data center(s) by consolidating or shutting down data center(s).

IMPROVED SECURITY AND AGILITY

A cloud migration can lead to better security and compliance with the latest tools and services provided by the CSPs. Additionally, organizations that migrate to the cloud have more agility in provisioning global application and infrastructure environments and thus shorter time to the market and increased productivity. They also achieve better performance with the horizontal and vertical elasticity (scale up/down and scale in/out) capability of the cloud environment.

LEVERAGE THE LATEST TECH

The latest technology platforms are available as services in the cloud. This can translate to administrative labor reduction by use of CSP PaaS offerings and automation, minimal capital investment needed for the refreshment of EOL (End of Life) hardware and software, and disaster recovery and backup archive solutions that boost operational efficiency and resiliency.

SUSTAINABILITY

A cloud infrastructure can help organizations achieve sustainability goals by reducing data center footprints.

MASTERING COST EFFICIENCY WITH CLOUD FINOPS

With enterprise cloud spend on the rise and frequently managed ineffectively, controlling, and reducing these expenses has become more urgent than ever for today's businesses. According to Gartner, by 2024, around 60% of I&O leaders will face public cloud cost overruns that will negatively impact their budgets.[2]

We believe organizations need a FinOps initiative that can drive the change necessary for financial accountability, financial efficiency, and overall cost control in the cloud. This initiative can be driven by either centralized or decentralized teams. The FINOPS framework defined by the FinOps Foundation is based upon three pillars: Inform, Optimize and Operate. These three pillars help in forecasting, reporting, controlling, and optimizing the cost in an ongoing operational model. At the activity level, these three pillars can be implemented by the four functions below:

COST OBSERVABILITY

Visibility into current and past costs in cloud environments will help in proactively managing current costs. Cost observability can be achieved by creating dashboards, weekly and monthly reporting, and setting up daily and weekly alerts if costs exceed the budgeted and targeted amounts. Costs incurred by various departments and projects must be reported to respective leaders and alerts should be utilized for anomalies that may occur.

COST OPTIMIZATION

A CSP's Well-Architected Framework defines best practices for cost optimization. These best practices include using auto-scalable and size adjustable architectures to avoid the over-provisioning of resources and thus keeping the cost optimized. Enterprise Agreements with CSPs for centralized purchasing help in achieving volume discounts. In addition to this, long-term commitments for resources often result in significant cost reduction. Many companies opt for a centralized procurement approach with enterprise agreements to benefit from lower pricing for all business units and projects. Cloud platform vendors also offer various usage-based pricing models, such as on-demand, reserved instances, spot instances, and more. The potential savings from commitment-based strategies, such as Reserved Instances and Hourly Savings Plan are substantial, when compared to on-demand instances.

Compute infrastructure is typically one of the largest parts of an organization's cloud bill. As a result, it is often the source of the most significant opportunities to reduce costs. Provisioning cloud resources can lead to inefficiencies, especially in teams lacking governance controls. Cloud management tools can help identify inactive resources using metrics like network traffic and CPU load. Advanced analytics and automation tools can continuously monitor and automatically shut down unused resources. Also, non-production and non-critical environments need not to be running 24x7 and can be shut down in off-business hours. This will result in cost reduction. Additionally, tools that provide cost insights by instances, tags, pods, clusters, and other factors can help uncover excess costs.

Cloud storage is easy to provision and can lead to unnecessary storage capacity. Identifying and removing unneeded volumes and snapshots is crucial. Usage data helps right-size overprovisioned volumes, and snapshot retention policies should be reviewed and adjusted. Cloud storage offers various options with different characteristics. Storing data in the appropriate storage tier and automating data migration between tiers can reduce storage costs.

Network traffic among Availability Zones, to the Internet or to another cloud can significantly contribute to cloud costs. Balancing services across zones and minimizing unnecessary data transfers can reduce these costs. Network tracing and logging tools can help identify misconfigurations causing unnecessary traffic.

COST GOVERNANCE

The most important step in performing cost governance is to develop policies for cost control and change management and to implement an approval process for any resource changes and additions that would increase cloud costs. Such policies should define enterprise standards for cloud services procurement and consumption, architecture guidelines, budgetary controls, and reporting.

Budgeting and the creation of chargeback policies are two other important parts of cost governance. The chargeback policies should cover allaspects of resources and workloads that relate to cost or usage, including creation, modification, and decommissioning. Periodic verification should ensure that policies and procedures are followed and implemented for any changes in the cloud environment. During your IT change management meetings, raise questions to find out the cost impact of planned changes, the business justification, and the expected outcome.

The essential part of cost governance is that all cost additions be reviewed for approval and all cost changes must be tracked and recorded. In fact, organizations should rightly expect cloud cost to grow with the growth in the business. The concept of unit cost helps to ensure that an increase in the cloud spend is proportionate to the business growth

COST COMMUNICATIONS

Finally, the communication of cloud spending details of various applications, projects, departments and project teams is an essential part of any FinOps initiative. One efficient way to accomplish this is to provide dashboards to various teams, so that they can track their cloud spend. This helps various groups to monitor their spending and to limit spending within their departmental budget. Alerts should be triggered if the cloud spending of the respective group exceeds the targeted budget.

OCM SHIELDS RISKS AND ELEVATES EMPLOYEE EXPERIENCE: ADDRESSING THE CULTURAL RESISTANCE

> *The dynamic disruption that is an essential catalyst to innovations such as cloud adoption and migrations can have an opposite effect on employees within the organization, slowing or thwarting the anticipated benefits and efficiencies associated with the transformation. Robust, holistic, and sustained organizational change management (OCM) is a vital part of any transformational effort, as it can help prevent the inevitable ROI erosion and unmet project expectations borne from employee disengagement, confusion, and frustration.*

Much of this confusion, especially in an age when so much change is driven by technology, is experiential and based on context. Consider this: According to Workspace.com, the median organizational ratio of IT roles to non-IT roles is 1:27[3], meaning that less than 4% of an organization makes a substantial number of decisions with profound impact on the other 96%. And with the frequency of these initiatives increasing five-fold in less than a decade, impacted stakeholders report growing frustration and lack of patience with solutions intended to make jobs easier.

The most common sources of frustration, and related resistance to change, are ineffective communications, lack of stakeholder engagement, disruption to daily routines, insufficient efforts to sustain change, and knowledge gaps related to roles, goals, and how the relevant technology works for them.

Because most of the factors that influence any successful change initiative are not related to technology, it is more critical than ever to focus on the employees' and organization's readiness for adopting cloud.

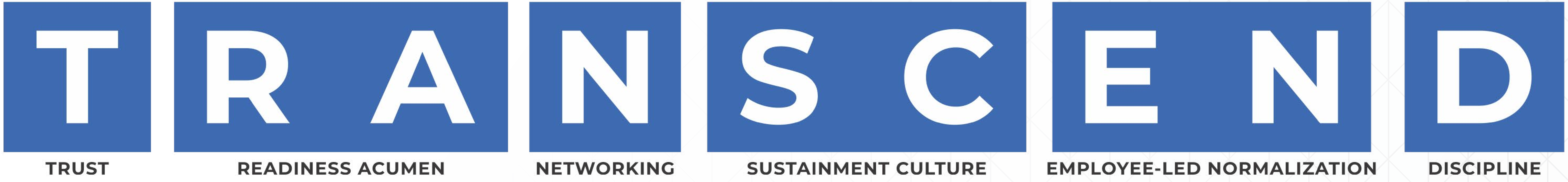
Employees need to be re-skilled/up-skilled, educated and trained for managing and operating cloud services. The organization involved needs to update strategies and operating plans, foster the culture of Agile, build knowledge on new technologies, and implement proper organization structure and processes for supporting new business and service models.

Organizations that want to be smart, efficient, and effective in adopting cloud with sustainable success make OCM an essential part of their transformational journey.

THE TRANSCEND METHODOLOGY

A HUMAN-CENTERED APPROACH TO ENABLING SUCCESSFUL ADOPTION OF TRANSFORMATIVE TECHNOLOGY

Aligning strategy, predictive behaviors & human-centric organizational change management (OCM) **user-owned adoption**



DEFINE IMPACTS & BEHAVIORS

- Organizational strategy alignment
- Case for Change
- Business-process design
- Strategic Sponsorship
- Stakeholder & change-impact analysis
- Change-readiness interviews
- Gaps, risks & priorities
- Change-culture analysis
- Behaviors key to success, adoption

DESIGN & IMPLEMENT

- OCM strategy & governance
- Change Agent Network
- Guiding coalition
- Communications
- Engagement plan
- Training needs assessment
- Sustainment needs analysis
- Training design & delivery
- Feedback loops
- Readiness surveys

REFINE, ENABLE & SUSTAIN

- Support strategy & plans
- Embedded support model
- Coaching plan & execution
- Support material development
- Reinforce success behaviors
- Evaluate success behaviors
- Sustain success behaviors
- Readiness surveys
- Track, facilitate ROI realization

ONGOING STAKEHOLDER COMMUNICATION

PREPARATION PHASE | **ACCEPTANCE PHASE** | **COMMITMENT PHASE**

DMI

Through our numerous customer support engagements, DMI has developed and refined a human-centered OCM approach branded as TRANSCEND for enabling the successful adoption of transformative technologies. Details of this approach are provided below.

TRUST

Trust is the cornerstone of successful change and adoption. It hinges on transparency, organization-wide awareness, timely and accurate communication, candid discussions about change impacts, and empathy. Leaders who embody these behaviors inspire trust among emerging change leaders and validate the need for a cadence of consistent messaging and robust engagement activities focused on cross-functional stakeholder insights and contributions to transition tactics and OCM solutions.

Building trust starts with discovery and data-capture activities, encompassing alignment with strategic goals, business process design, strategic sponsorship, and cross-functional collaboration. Involving stakeholders, promoting activities, and translating them into action through timely communication and journey maps are vital steps in building and demonstrating trust.

READINESS ACUMEN

Having a keen sense of organizational readiness for change, both from a cultural perspective and specific to cloud migration and operations, is necessary to anticipate and address responses to change, including those that represent risks and resistance to change. Too often, organizations underestimate cultural resistance to change and overestimate how effective prior leadership has been. These discussions are often difficult, as they challenge convention, perception, and entrenched positions and biases regarding change. Nonetheless, the ability to sense and address the true health of an organization's change culture will surface issues early and demonstrate a willingness to have tough conversations about barriers associated with prior, failed change efforts. Subsequent sections will explore further how the TRANSCEND methodology facilitates this.

The willingness to have these challenging conversations, undertaken at the start of the engagement, goes together with building trust and comprises activities like stakeholder and change-impact analysis sessions and change-readiness interviews. Whenever possible, these activities should be conducted as part of a dynamic that encourages freely sharing information on organizational culture and change leadership, both good and bad. This analysis can be leveraged to prioritize OCM activities that mitigate risks, leverage resident force multipliers and influencers, and define the scope of OCM activities to focus on cultural dynamics without triggering change fatigue.

NETWORKING

Connections between people performing different but complementary functions hold the entire system together, whether it is a cloud-based ecosystem, or an organizational culture calibrated to support transformation and innovation. A robust, well-designed network of change agents and SMEs breaks down silos, creates holistic OCM solutions to resonate across all stakeholder communities, and enables an employee-centric approach to building those solutions. Change agents and SMEs, working with the OCM team, can create solutions and communications that will resonate and encourage individual change ownership and adoption by enabling transparency, communication, and stakeholder contributions to myriad solutions anticipating not only diverse stakeholder needs and experiences, but also different rates of change adoption.

Networking is an intentional activity that should be strongly embraced and actively orchestrated for any significant OCM effort, especially those as far-reaching and impactful as cloud migrations.

SUSTAINMENT CULTURE

Sustainment is essential to ensuring change adoption and that behaviors supporting project success and ROI actually “stick.” Sustainment culture provides the “muscle memory” necessary for change to take hold. Too often, sustainment is considered only after training design and delivery, versus occurring in tandem and far in advance of when impacted stakeholders must begin to internalize the change as part of their day-to-day work to ensure strategic goals. Given the far-reaching scope and impact of cloud migrations, and myriad challenges associated with the transition to cloud operations for daily users, a deliberate and detailed alignment of training and sustainment activities is critical to realizing the payoff of OCM efforts.

In our experience, the following are effective actions to foster sustainment culture:

1. Conducting targeted education workshops on business strategies, cloud service models, cloud management and cloud architecture best practices to stakeholder communities (both technical and non-technical).
2. Taking CSP provided trainings and getting certified.
3. Implementing a lab environment to promote hands-on learning, idea experimentation, simulation, and testing. Such a Dojo practice helps build the muscle memory and demonstrate the good and bad practices.

EMPLOYEE-ENABLED NORMALIZATION

When OCM is successful and effective, it will enable actions and outcomes that make good on the common organizational assertion “our people are our greatest asset.” Employee-enabled OCM converts this premise into action, by creating a dynamic that empowers employees to own the success of organizational transformation, as well as the associated goals and benefits. OCM builds awareness, competence, and confidence in a solution’s holistic and individual value and benefits, by making stakeholders key architects in the design and realization of that solution. Additionally, the disruption of day-to-day activities that can feed frustration with change and create resistance can be mitigated (1) by stakeholders who leverage OCM solutions and (2) by a network of peers building the muscle memory they will need to flex to sustain adoption, ownership, and support for change.

DISCIPLINE

It’s trite but true to say that change is hard -- something anyone who has ever experienced a significant period of innovation or transition knows all too well. In the end, the success of any OCM initiative, and the transformation it works to support, is largely dependent on the level of organizational investment. Before, during, and after the change, discipline is required to ensure everyone maintains focus on the goals and understands the value and how it is realized. Discipline is also necessary to address and resolve the issues likely to arise as the organization works to internalize new ways of working, achieving new goals, normalizing new processes, and using new technologies.

FORTIFYING YOUR CYBER SECURITY CULTURE: ADDRESSING THE SECURITY CHALLENGES

Securing the confidentiality, integrity, and availability of cloud environments requires a zero trust framework that encompasses the shared responsibility model between the CSP and customer, and all of the major pillars of zero trust (Identity, Data, Network, Endpoints, and Workloads). Full visibility in the cloud, least privilege access policies, policy enforcement, and automated actions are critical to protecting cloud environments..

CONTINUOUS RISK ASSESSMENT

DevSecOps principles including "Shift Left" where cloud environments and workloads are continually assessed for threats, vulnerabilities, risk, and compliance prior to implementation of changes in production environments is vital to maximizing the productivity and minimizing the risk of cloud-based applications.

PUBLIC CLOUD SECURITY METHODS

There are various cloud security tools and technologies that can be used to protect cloud resources. A combination of these tools needs to be leveraged to protect cloud environments. The tools and methods to secure cloud environments are described below.

1

IAM (IDENTITY AND ACCESS MANAGEMENT)

IAM controls authentication in the cloud environment and controls authorization for the use of various resources. CSPs provide SAML federation for their cloud platforms to integrate external identity providers if desired. DMI recommends that MFA (Multi Factor Authentication) and Privileged Access Management (PAM) for administrative users and service accounts.

2

DATA SECURITY

Data encryption at rest and in transit techniques including quantum and homomorphic, identification of sensitive data, least privilege access to data through Role-Based Access Control (RBAC), Attribute Based Access Control (ABAC) or Resource Tagging, There are multiple services available directly by CSPs or data security partners.

3

NETWORK SECURITY

There are multiple CSP-provided and third-party tools available to stop unauthorized access externally and internally to a customer's virtual private cloud (VPC). Blocking unauthorized users from entering the network is the best way to secure and ensure availability of an environment. Some of the most common methods for network security are DDOS protection, network and application layer firewalls, security groups, network ACL (Access Control List), and network security groups. Network environments should be segmented into public and private sub-networks for security enforcement. Unless an application needs to be opened for internet users, everything must be kept in private sub-networks.

Micro-segmentation of internal networks ensures that communication between VMs and/or containers are strictly controlled.

4

ANOMALY DETECTION

External and insider threats needs to be identified quickly via anomalous activity, reported upon, and actively managed through a CSP-provided or third-party SIEM (Security Information and Event Management) and SOAR (Security Operations Automation Response). Azure Sentinel an example of a CSP-provided SIEM and SOAR.

5

CLOUD WORKLOAD PLATFORM PROTECTION

Scanning the environment regularly to identify threats and vulnerabilities to workloads and containers is critical to ensuring that applications and properly secured, uncompromised, and only authorized functions are performed.

6

CLOUD SECURITY AND POSTURE MANAGEMENT

CSPM (Cloud Security and Posture Management) tools are designed to identify misconfiguration issues in the cloud to include exposure of cloud assets to the public internet, overpermissive access permissions, and asset vulnerabilities. Context awareness enables CSPM tools prioritize and rank the severity misconfigurations based on multiple data sources from the cloud environment.

7

WELL ARCHITECTED FRAMEWORK RECOMMENDATIONS FOR SECURITY

CSPs provide Well-Architected Frameworks that are sets of best practices for their cloud platforms. Security is a major component of well-architected frameworks. The cloud environment should be designed using the recommendations provided by the Well-Architected Framework.

8

SHIFT LEFT

DevSecOps has become the standard methodology for agile development of applications within the cloud. Shift Left ensure that security is enforced continually as applications are developed and enhanced and migrate from Development to Test to Production.

9

CONTINUOUS COMPLIANCE

Many critical services provided in-country are required to maintain compliance with industry standards, to include PCI, HIPAA, GDPR, NERC CIP, DOE C2M2, NIST 800-53v5, NIST 800-171, and SOC2. Continuously verifying compliance with these industry standards is mandated to maintain applications hosted in the cloud.

ZERO TRUST SECURITY POLICY, ARCHITECTURE, AND GOVERNANCE

USERS

- Multi-Factor Authentication (MFA)
- Contextual Access Control
- Enterprise Identity, Credential, & Access Management Integration
- Access Analytics
- Privileged Access Management
- Zero-trust Network Access

NETWORK

- Trusted Internet Gateway - Traffic Content Filtering
- NGFW, IDS/IPS
- Secure Access Service Edge
- Cloud Security Access Broker
- Service Mesh, mTLS, Sidecar Proxy
- Network Detection and Response
- Micro Segmentation

DEVICE & WORKLOADS

- Configuration Hardening
- Vulnerability Management
- Directory Integration
- Blocklisting, Allowlisting
- Endpoint Detection and Response - behavioral analysis, vulnerability shielding
- System Integrity Assurance
- Comply to Connect

APPLICATION

- DevSecOps & GitOps
- Application SAST & DAST
- API Security
- Service-to-Service Authentication & Authorization with dynamic secrets
- Runtime Security
- Software Bill of Materials (SBOM) security

DATA

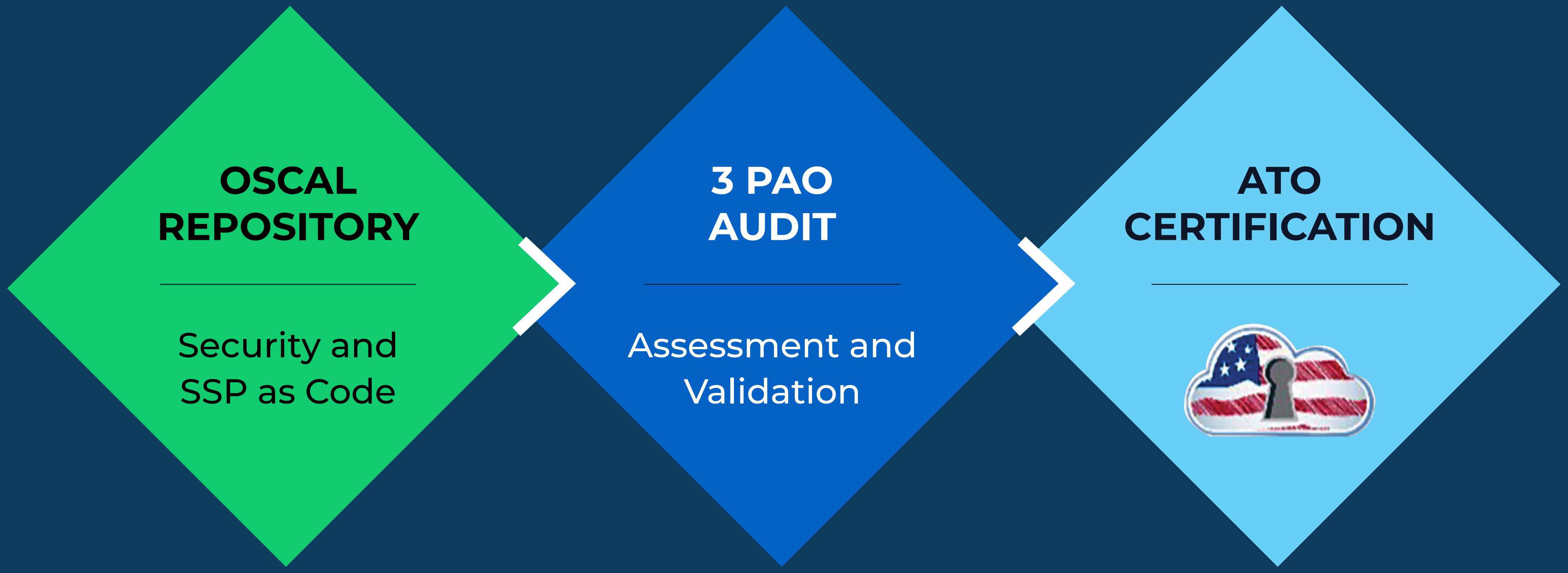
- Encryption at-rest & in-transit
- Classification & Obfuscation
- Access Control
- Data In-use Protection & Confidential Computing
- Data Loss Prevention
- Insider Threat Protection
- Cross-Domain Security
- Data Retention and Destruction
- Ransomware-proof Backup

CONTINUOUS RISK ASSESSMENT, CONTINUOUS MONITORING, CONTINUOUS ATO (FEDERAL GOVERNMENT) - WITH POLICY AS CODE & SECURITY AS CODE

11

ACCELERATED AND CONTINUOUS ATO (FEDERAL GOVERNMENT)

For Federal Government organizations, DMI provides a set of proven modern solutions to achieve FedRamp ATO (Authority to Operate) for the target cloud environment and migrated applications. We apply Infrastructure as Code, SSP (System Security Plan) as code, Compliance as Code, and Automated Documentation as Code. These code sets are stored in the OSCAL (Open Security Controls Assessment Language) format. This allows our federal agency customers to achieve security ATO in a much shorter timeframe after 3PAO (Third Party Assessment Organization) audit.



OSCAL REPOSITORY

Security and SSP as Code

3 PAO AUDIT

Assessment and Validation

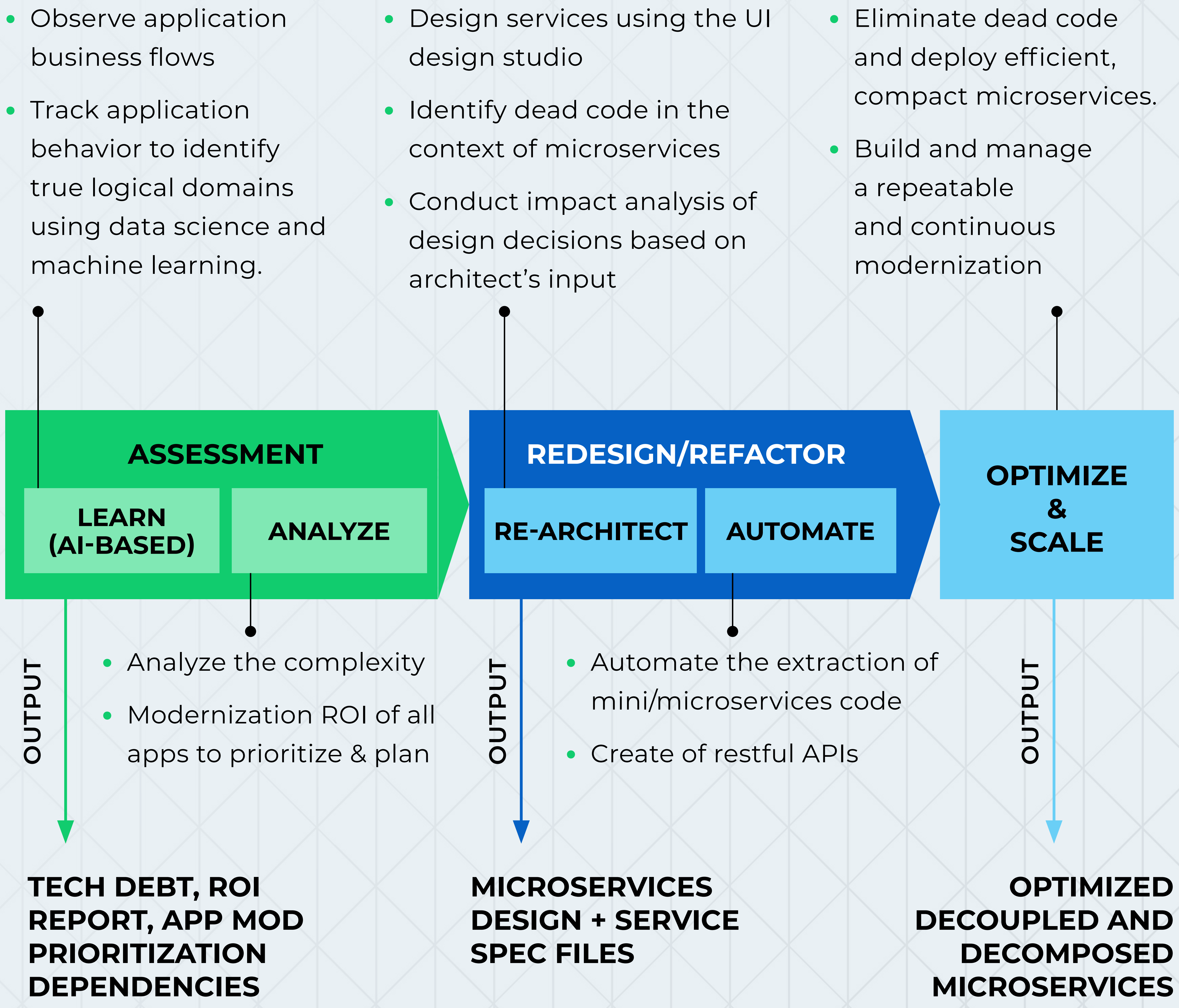
ATO CERTIFICATION

AI ENABLED APPLICATION MODERNIZATION FOR CLOUD MIGRATION: ADDRESSING APPLICATION READINESS CHALLENGES

Through our technology partnerships, DMI employs an AI-assisted application refactoring methodology to speed up legacy and monolithic application modernization. Our approach fully supports technical stacks such as Java and .NET for static and dynamic code analysis and reduces the delivery schedule and the overall technical risk for large and complex application refactoring. Our approach also provides dynamic and static analysis with applied graph theory and clustering algorithms to automatically identify optimal business-domain microservices and untangle deep dependencies across databases, classes, and resources. Our architects design services using an interactive UI design studio, which enables us to refine services and conduct impact analysis of design decisions based on the architect's input.

DMI's AI-assisted application refactoring methodology also provides comprehensive application assessment reports that recommend appropriate entities and services for data decomposition.

Here, we illustrate our three-phase approach for application refactoring: Assessment, Redesign/Refactor, and Optimize and Scale. Our approach decouples and converts business components to shared and common services for independent and autonomous deployments. This helps identify reusable and shared components early during application optimization for seamless integration of business services with other layers, such as UI, Data, and Integration.



- Observe application business flows
- Track application behavior to identify true logical domains using data science and machine learning.

- Design services using the UI design studio
- Identify dead code in the context of microservices
- Conduct impact analysis of design decisions based on architect's input

- Eliminate dead code and deploy efficient, compact microservices.
- Build and manage a repeatable and continuous modernization

- Analyze the complexity
- Modernization ROI of all apps to prioritize & plan

- Automate the extraction of mini/microservices code
- Create of restful APIs

TECH DEBT, ROI REPORT, APP MOD PRIORITIZATION DEPENDENCIES

MICROSERVICES DESIGN + SERVICE SPEC FILES

OPTIMIZED DECOUPLED AND DECOMPOSED MICROSERVICES

ADDRESSING DATA MIGRATION CHALLENGES

Data migration is a crucial aspect of cloud migration, presenting various challenges that need careful consideration. The primary challenges associated with data migration include:

- **Network Bandwidth Bottleneck**: Large transfers between on-premise systems and the cloud can face constraints due to network bandwidth limitations.
- **Business Continuity**: Migrating data without disrupting or causing downtime for production workloads is essential.
- **Data Synchronization**: Mission-critical production systems often require seamless data synchronization between on-premise and the cloud during cutover, especially when downtime is not an option.
- **Security and Compliance**: Ensuring security and compliance both during and after migration is a critical concern.
- **Data Integrity**: Maintaining data integrity throughout the migration process is imperative.

To address the challenge of migrating large amounts of data in an offline mode, one effective solution is to load the data into an appliance and physically ship it to the Cloud Service Provider's (CSP) facility. Examples of such appliances include AWS Snowball and Azure Data Box, which can scale up to a petabyte of data. These appliances, when on-premise, allow data upload, and after uploading, the physical appliance is sent to the CSP, ensuring data security through strong encryption and restricted access to authorized personnel.

Additionally, various third-party tools in the marketplace offer ongoing data syncing between on-premise and the cloud. These tools employ Change Data Capture (CDC) to track changes in data sources, enabling data integrity and consistency across systems and deployment environments. CSPs also provide native solutions for live data migration, such as AWS Database Migration Service, ensuring minimal downtime during the migration process.

For file data type migration, several third-party and CSP-provided tools, such as Azure File Sync and AWS Data Sync, facilitate ongoing sync for file system data, minimizing downtime. Many data migration tools leverage data virtualization, allowing migration without compromising data integrity and application availability. Data virtualization maintains data in source systems while defining a virtual layer for unified data access, ensuring flexibility, security, and compliance.

Key features of selected tools for data migration should include:

- **Removal of Network Bottleneck**: The selected tool should be able to bypass network bottleneck for large data transfers between on-premises and cloud.
- **Flexibility and Ease of Access**: Real-time or near-real-time access to data.
- **Unified View**: Integration across disparate data sources without the need to move or copy data.
- **Incremental Approach**: Incrementally copying data from on-premises to cloud in order to keep data in sync and minimize migration downtime.
- **Shared Data Access Layer**: Establishing a layer that logically relates to data, irrespective of data sources.
- **Modern, Scalable Architecture**: Positioned to support customer data and analytics needs.
- **Continuous Security and Audit**: Ensuring data quality, robustness, and security throughout the process.

REVIEWING THE ROADMAP OUT OF THE MIGRATION MAZE

Every cloud migration comes with challenges and requires considerations that span technical, financial, and organizational change management spheres.

Besides a partner who can design, engineer, deploy and monitor scalable cloud applications and infrastructure, organizations also need FinOps experts to ensure the organization is maximizing ROI and configuring cloud infrastructure and applications to optimize cost savings.

OCM experts are needed to help prepare and equip employees for the organizational transformations that happen amid cloud migrations and new application rollouts.

Organizations also need to establish policies and strategies for securing data in the cloud and leveraging artificial intelligence.

By focusing all at once on the technical, strategic, and human aspects of infrastructure and application modernization and transformation, your organization will be far more likely to achieve your business objectives – now and in the future.

DMI

DMI is a leading global provider of digital services working at the intersection of public and private sectors. With broad capabilities across IT managed services, cybersecurity, cloud migration and application development, DMI provides on-site and remote support to clients within governments, healthcare, financial services, transportation, manufacturing, and other critical infrastructure sectors.

CONTACT US TODAY TO LEARN MORE.

Engage@DMInc.com
P 240-728-7168
Learn more at
https://dminc.com/services/cloud-services/

This message is produced and distributed by
DMI | https://dminc.com/policies/privacy/

ADDITIONAL RESOURCES

DMI

REAP THE BENEFITS OF CLOUD MIGRATION WITH DMI AND AWS

ABOUT DMI

BENEFITS

MORE SECURE SYSTEMS

IMPROVED CUSTOMER AND CITIZEN EXPERIENCES

REDUCE UP-FRONT AND LONG-TERM COSTS

Reap the benefits of cloud migration with DMI and AWS

DMI

CASE STUDY

CLOUD MIGRATION POWERS FEDERAL CLIENT'S EFFICIENCY LEAPS

EXECUTIVE SUMMARY

THE CHALLENGE

Case study on DMI’s cloud modernization solution for a federal government client

DMI

A PHARMACEUTICALCOMPANY USES AWS TO ELEVATE ITS CUSTOMER EXPERIENCE - OFFERING SPEEDY ACCESS TO MEDICINES

EXECUTIVE SUMMARY

THE CHALLENGE

Case study on DMI’s cloud modernization solution for a leading global pharmaceutical company

REFERENCES

[1] Source: Forrester - https://www.forrester.com/blogs/predictions-2024-cloud/

[2] Source: Gartner, “6 Ways Cloud Migration Costs Go Off the Rails”; link: https://www.gartner.com/smarterwithgartner/6-ways-cloud-migration-costs-go-off-the-rails

[3] Source: Workspace.com; Retrieved 16 October 2023