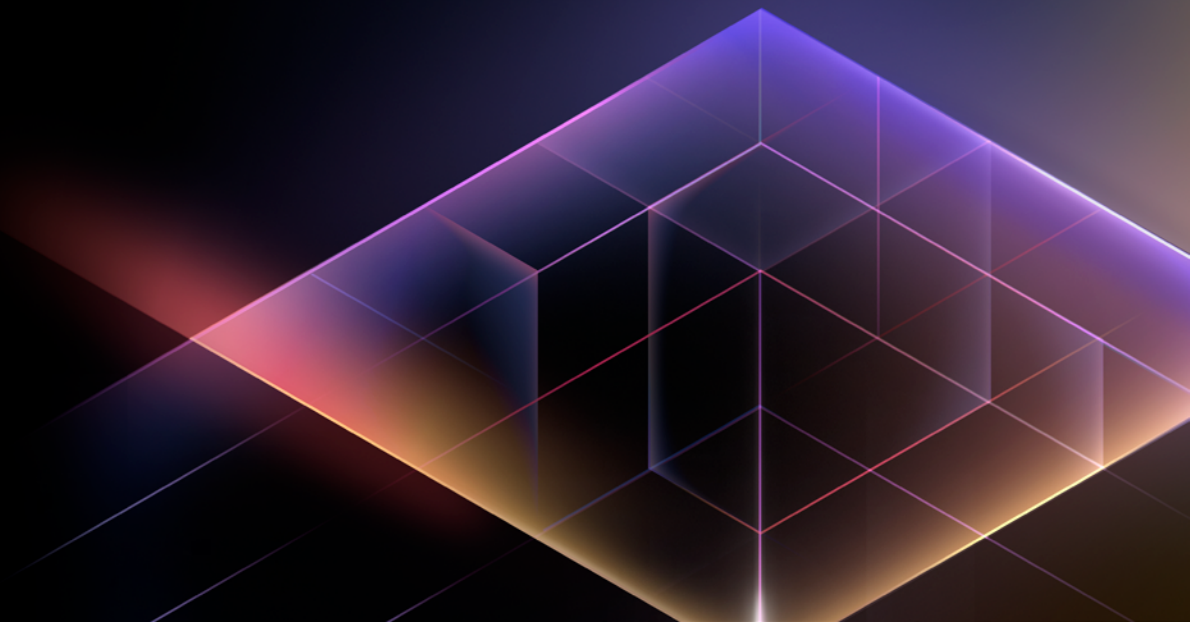




# Architecting resilience: mastering migration, cloud adoption, and scalability in regulated industries



# Overview

Staying ahead with advances in technology requires strategic foresight and meticulous risk management. IT leaders and architects must navigate a complex ecosystem of infrastructure, compliance, and security challenges while ensuring that digital transformation efforts drive real business and technical value. The risks of poorly executed migrations, cloud adoption missteps, and scalability bottlenecks can lead to performance degradation, security vulnerabilities, and wasted resources.

Despite the investment in digital transformation, success is far from guaranteed. Global IT spending is projected to reach \$5.61 trillion this year, a 9.8% increase from 2024. However, only 48% of digital initiatives meet or exceed their intended outcomes, often due to siloed leadership and inadequate risk mitigation strategies. This gap between investment and impact underscores the need for an infrastructure that is both scalable and cost-efficient yet resilient against emerging threats.

This case study digest presents real-world case studies from organizations that successfully addressed key technical challenges:

- Managing risks in complex migrations (Humana, Charlotte Tilbury)
- Optimizing cloud adoption (Deutsche Börse, AGL)
- Scaling infrastructure securely (Indeed)

These real-world examples provide actionable insights for CTOs, CIOs, and other engineering leaders who look to implement risk-aware digital transformation strategies.

## Managing risks in complex migrations

Infrastructure migrations are among the most technically complex and high-risk initiatives IT leaders face. Poorly executed transitions can lead to downtime, data loss, security vulnerabilities, and performance degradation, which can disrupt critical business operations.

To mitigate these risks, technical leaders must take a structured approach that includes comprehensive system assessments, phased rollouts, automation, and robust rollback strategies.

## CUSTOMER SPOTLIGHT

# Humana | A phased approach to scalability

Humana is a major healthcare insurer with more than 16 million members and 67,000 employees across the U.S. and Puerto Rico. The company wanted to transition from Terraform Enterprise to HCP Terraform to enhance its infrastructure as code (IaC) practices, improve collaboration, and strengthen security across its cloud infrastructure.

However, Humana had their work cut out for them — migrating 2,695 workspaces across five environments was not an easy task, particularly not in a tightly regulated industry like healthcare.

## The challenges

The sheer number of workspaces and environments created logistical complexities that had to be addressed without disruption to critical healthcare services. The business had to keep everything consistent across multiple cloud setups, as even minor discrepancies could introduce security gaps. Sticking to strict regulations was also a must to ensure security and avoid hefty penalties. Finally, aligning diverse stakeholders — cloud engineers, security teams, and business leaders — required impeccable team coordination.

## The solutions

Humana tackled its initially complex setup by adopting a phased migration strategy, ensuring incremental validation across its vast number of workspaces and environments while minimizing disruption to critical healthcare services. HCP Terraform's automation enforced configuration consistency across multiple cloud environments, reducing security gaps and operational drift.

HCP Terraform's policy as code streamlined compliance, ensuring adherence to strict regulations with real-time visibility into security policies. To align diverse stakeholders, Humana maintained open communication channels, enabling seamless coordination between cloud engineers, security teams, and business leaders—achieving a secure, compliant, and disruption-free migration.

## Key Outcomes

- Streamlined workflows and reduced the time required to manage complex cloud environments
- Improved overall infrastructure security with centralized control
- Automated and simplified IaC processes improved developer productivity
- Created a scalable and consistent infrastructure foundation



## CUSTOMER SPOTLIGHT

# CharlotteTilbury | Set the foundation for new infrastructure

Charlotte Tilbury, a luxury beauty brand founded by British makeup artist Charlotte Tilbury in 2013, has seen remarkable growth over the past decade. In June 2020, Puig, a Spanish fragrance and cosmetics giant, acquired a majority stake in Charlotte Tilbury for a reported \$1.3 billion — putting the brand on the global beauty map. All of this put added pressure on its IT infrastructure which was no longer compatible with its growth ambitions. The brand needed a new solution.

## The challenges

Charlotte Tilbury's rapid growth outpaced the capabilities of AWS CloudFormation, revealing major limitations in a multi-cloud environment. Rigid AWS dependencies slowed innovation, making IaC a strategic imperative for future scalability.

Furthermore, CloudFormation's manual processes further compounded the inefficiencies, increasing the risk of errors and inconsistent deployments as the business scaled. Charlotte Tilbury needed an agile, automated infrastructure solution — one that could be implemented without disrupting customer-facing services or compromising security.

## The solutions

Charlotte Tilbury relied on Terraform's IaC capabilities to standardize deployments across cloud platforms, decreasing manual efforts and minimizing errors. The company also used a phased approach — starting with critical services, validating Terraform's performance, and then scaling up once they were confident their approach worked.

Automation was central to the process, particularly automated validation which ensured configurations remained consistent and reliable. Terraform's policy ascode took care of security and compliance by aligning the infrastructure with industry standards. Continuous collaboration between technical teams and business leaders ensured the migration enhanced customer experience while supporting long-term strategic growth.

## Key Outcomes

- Enabled multi-cloud infrastructure management
- Improved infrastructure modularity
- Delivered consistent and repeatable infrastructure deployments
- Automatically enhanced security and compliance using policy as code





# Takeaways on migration risk management

Humana and Charlotte Tilbury's stories offer valuable lessons for navigating complex infrastructure migrations.

## Define clear goals

Begin by assessing your existing infrastructure and aligning it with your long-term business goals. A clear roadmap will ensure seamless execution without compromising performance or compliance.

## Adopt a phased approach

Incremental migrations minimize risk. Breaking the move into stages allows you to detect issues early, maintain operational stability, and adapt in real time — reducing the odds of encountering major challenges down the road.

## Lean into automation

Automation is the backbone of any smooth migration. Terraform's capabilities ensured consistent configurations, eliminated manual errors, and enforced security and compliance at every stage through automated testing and validation.

## Embed governance and compliance

Policy as code streamlines governance and security, enabling real-time policy enforcement without manual oversight. Automated compliance promotes regulation adherence — critical for organizations operating in highly regulated sectors.

## Get everyone on board

Seamless migration requires cross-functional collaboration. Keeping technical teams and business stakeholders in sync accelerates issue resolution and ensures the migration meets both technical requirements and strategic business objectives.

# Optimizing cloud adoption

Cloud adoption offers opportunities for increased agility, scalability, and cost efficiency. However, it also introduces unique challenges. Poorly managed transitions can quickly derail business objectives and lead to cost overruns, security breaches, and performance bottlenecks.

Successful cloud optimization demands a strategic focus on risk assessment, continuous monitoring, and well-defined governance. This is key to ensuring a smooth cloud journey and protecting valuable business assets.

## CUSTOMER SPOTLIGHT



DEUTSCHE BÖRSE  
GROUP

# Embrace the public cloud

Frankfurt-based Deutsche Börse AG is one of the world's leading financial exchanges, providing a marketplace for trading stocks, bonds, derivatives, and other financial instruments. As part of its modernization strategy, Deutsche Börse pursued a flexible public cloud strategy that would enable faster development cycles. This modernization effort aimed to streamline data analytics, real-time indices, and AI-driven solutions — like fraud detection and liquidity management — giving clients an edge in trading strategies.

## The challenges

Adopting public cloud solutions in the financial sector comes with stringent compliance challenges. Deutsche Börse needed a solution that secured sensitive financial data, enforced precise access controls, and maintained governance to enable rapid development without increasing regulatory or operational risks.

Ultra-low latency requirements posed another obstacle that exceeded current public cloud capabilities. This ruled out a full data center migration and required a hybrid approach. Alas, initial cloud explorations revealed cultural differences with U.S.-based hyperscalers, particularly concerning audit rights, access, and scope. Furthermore, the organization's custom-built applications lacked off-the-shelf alternatives, further complicating the migration process.

## The solutions

To address the complexities of cloud adoption in a highly regulated environment, Deutsche Börse turned to Terraform to serve as the backbone of its cloud control plane. IaC blueprints enforced standardized configurations and automated provisioning across their multi-cloud environment. Using Terraform's Sentinel, they were able to block non-compliant deployments, maintaining strict adherence to regulatory requirements and internal security standards.

Addressing security challenges, Deutsche Börse integrated Vault for dynamic secrets management, reducing exposure to static secret credentials while simplifying access control across its distributed environment. The integration of Vault into the workflow streamlined security operations and provided a centralized platform for managing sensitive data.

Finally, Deutsche Börse used Terraform's drift detection capabilities to gain real-time visibility into any infrastructure configuration changes. This allowed the business to swiftly identify deviations, enforce desired configurations, and sustain governance — ensuring a stable, compliant, and efficient hybrid cloud strategy.

## Key Outcomes

- Accelerated innovation through cloud-powered data analytics
- Strengthened compliance with a robust framework and policy as code
- Improved operational efficiency via centralized provisioning and standardized DevSecOps
- Enhanced security using Vault and temporary credentials





## CUSTOMER SPOTLIGHT



# Bet big on the cloud

Founded in 1837, AGL is one of Australia's largest energy providers, delivering electricity, gas, solar, and renewable energy to over four million homes. Considering its long history, the company has seen its technology infrastructure evolve significantly over the years. By 2017, AGL had migrated a few applications to the cloud, but the majority — two-thirds — still resided in company-owned infrastructure within two large, third-party data centers.

This posed a major problem: one of its third-party data centers was shutting down, and the other was aging. The company decided to vacate both and migrate all applications to the cloud.

## The challenges

Thus began a multi-year cloud adoption effort involving 50 teams made up of employees, contractors, and third-party partners. Commercial off-the-shelf software tools often lacked vendor documentation, installation materials, or even active vendor support. Many ran on 32-bit operating systems and needed to be modernized before migrating to the cloud.

Infrastructure provisioning posed another major hurdle. AGL's standard process could take up to a week to deploy a single virtual machine (VM), far too slow for the scale and speed required. The project demanded a tool to streamline collaboration, ensure secure and consistent cloud environments, and accelerate team efforts to meet the project timeline.

## The solutions

AGL made Terraform the foundation of its cloud adoption strategy. IaC helped teams define standardized configuration files, ensuring every environment adhered to policies while automating provisioning. Using Terraform, manual deployments were eliminated, and VM deployment time was reduced from weeks to just 10 minutes.

Faster deployments translated into greater efficiency. AGL migrated over 210 applications in just two years. Security was seamlessly integrated, with every new VM build automatically installing security agents and enforcing policies through Terraform's Sentinel. Today, AGL can rest assured that new resources are compliant as soon as they are deployed.

## Key Outcomes

- Created a module library for faster deployment
- Two large data centers exited in 24 months
- Deployment time for VMs went from one week to less than 10 minutes
- Enabled advanced collaboration and high availability
- Migrated 210+ apps to the cloud





## Takeaways on managing cloud adoption risks

Deutsche Börse AG and AGL's cloud migration journeys offer valuable insights for balancing innovation with security and compliance. These lessons offer a roadmap for navigating cloud adoption in complex, high-stakes environments.

### Embrace automation for speed and consistency

Terraform's infrastructure as code allows you to standardize deployments, accelerate migration timelines, and eliminate manual errors. Automation also ensures consistency across environments while boosting team productivity.

### Embed security and compliance from the start

Use purpose-built tools like Vault and Sentinel to hardwire security and compliance into your workflows. These types of proactive security measures reduce risk exposure and prevent costly fixes later. Adapt to regulatory and technical constraints

When full cloud migration isn't feasible due to regulatory or technical limitations, flexibility is key. Features like Terraform's drift detection can help maintain compliance by continuously aligning configurations with security and governance standards across environments.

### Rethink processes, not just tech

Compliance-heavy workloads often require reimagining operational processes. Collaborating with hyperscalers and regulators to establish clear audit rights can smooth the path for regulatory approval and long-term cloud success.

### Tackle legacy complexity head-on

Outdated applications and unsupported off-the-shelf software can complicate migrations. Addressing modernization challenges upfront, supported by a multi-team effort, ensures a smoother transition — even for the most complex IT projects.

## Scaling infrastructure effectively

As businesses expand, scaling infrastructure becomes a critical challenge. Without a proactive strategy, rapid growth can lead to resource bottlenecks, operational inefficiencies, and security vulnerabilities — all of which threaten system reliability and customer trust.

Organizations operating at scale must ensure that distributed architectures remain performant, resilient, and secure, even during unpredictable demand surges.

## CUSTOMER SPOTLIGHT

### | Scale to new heights

As the world's leading job site, Indeed connects millions of job seekers and employers daily. With a global user base relying on them to secure their livelihood and fill open positions, site reliability is a major priority. With surging demand, Indeed needed to scale operations without compromising performance, efficiency, or system resilience.

## The challenges

To support its hyper-growth, Indeed had to meet the demands of its massive, globally distributed microservices architecture without sacrificing performance or security. This meant building a HashiCorp Vault infrastructure capable of scaling while remaining accessible to engineers who weren't necessarily Vault experts.

Additionally, engineers faced the constant threat of "thundering herd" scenarios, where sudden surges in secret requests could overwhelm their clusters. Rapid deployment cycles added another layer of complexity, requiring solid security measures to protect sensitive employment data without slowing down development.

## The solutions

Indeed's approach to tackling these challenges was to build a self-healing Vault infrastructure. Using immutable infrastructure, automated unsealing via AWS KMS, and EC2 lifecycle events triggering Lambda functions, the system could scale dynamically, replace failed nodes, and remove them from the Raft cluster — all without human intervention. To prevent cluster overload, engineers implemented rate limiting and used Vault Benchmark to simulate realistic traffic patterns, ensuring they could handle peak loads.

Observability into user experience was key, so they defined clear service level objectives (SLOs) to monitor user experience, built dashboards with contextual metrics, and created detailed runbooks to empower their "Vault-adjacent" engineers to troubleshoot efficiently. Regular operational reviews turned every incident into an opportunity for refinement, driving continuous improvements in system reliability.

## Key Outcomes

- Built a resilient Vault with automated defenses and self-healing
- Gained clear observability through defined SLOs and contextual dashboards
- Streamlined incident response by empowering engineers with clear guidance
- Achieved operational excellence with continuous improvement and automation

## Takeaways on scaling securely

Indeed's journey to building a highly resilient and observable Vault infrastructure offers best practices for organizations managing critical systems at scale.

### Automate for resilience

Embrace immutable infrastructure and automate key operational tasks, like unsealing and health checks. This allows for rapid recovery from failures. Cloud provider features like AWS EC2 lifecycle events and Lambda functions can trigger automated actions, creating a self-healing system.

### Prevent overload

Implement quotas and rate limits to protect Vault clusters from excessive traffic. Vault Benchmark allows you to simulate realistic traffic patterns and stress test clusters in lower environments to achieve peak performance.

### Prioritize observability

Define clear SLOs to track reliability and user satisfaction. Generate dashboards with contextual metrics and detailed runbooks, which can empower responders to diagnose and resolve incidents efficiently. Empower teams with controlled access

Role-based access control (RBAC) ensures responders have secure yet limited access to Vault endpoints. Runbooks with step-by-step troubleshooting guidance enable confident, effective incident response.

### Commit to continuous improvement

Implement regular operational reviews to analyze incidents and identify improvement opportunities. These reviews ensure continuous iteration on platform reliability and resilience.

## Beat the odds with HashiCorp

Every company's digital journey is unique, but the lessons from those who have successfully navigated transformation offer a clear roadmap. Aligning technical solutions with business goals, adopting a strategic, phased approach, and prioritizing security and compliance from the outset are universal success factors.

Whether migrating infrastructure, adopting cloud technologies, or scaling operations, HashiCorp provides the tools to make it seamless. Ready to future-proof your organization? [Send us a message](#) and we'll be in touch.

