tarmac

HAVI

Case Study

# Logistics giant, HAVI, achieved visibility & opportunity for >20% Azure cost savings with Tarmac

Empowering a global logistics leader to optimize cloud costs and strengthen security


**During a major business transformation, Tarmac helped HAVI, a leading logistics enterprise, overcome silos, improve visibility, and reduce cloud costs using Azure Resource Inventory, Azure Advisor, Terragrunt, GitHub, and GitHub Actions, all while mitigating security risks.**

## About Our Client

HAVI is a global logistics and supply chain company, particularly focused on the Food & Beverage industry. Currently, the company has over 10,000 employees and more than $1B in annual revenue.

## The Solution - Tarmac.IO comes to the game

A couple of years ago HAVI decided to conduct a rapid shift to the cloud. While the migration provided a working environment, the speed of execution led to a lack of best practices. When the company decided to transition from a centralized-governance model to business-unit-oriented operations, they also wanted to use this opportunity to modernize & catch up on the tech debt previously created. Joel Ferreira was brought on board in a role as Senior Manager of Cloud Engineering & Operations, to spearhead this massive undertaking. He quickly identified a lack of visibility as the company's biggest challenge.

The situation our customer was in isn't very unique - we often see smaller problems compound into this big unknown: a mix of complex systems, unstandardized tooling across multiple teams, lack of (proper) documentation, uncertainties of who owns what, an unknown number of resources and integrations...

But good visibility into a cloud environment isn't a "nice-to-have" in an enterprise organization. It is absolutely critical to making strategic business decisions; from compliance, security, and cost-efficiency, to stability and future-proofing.

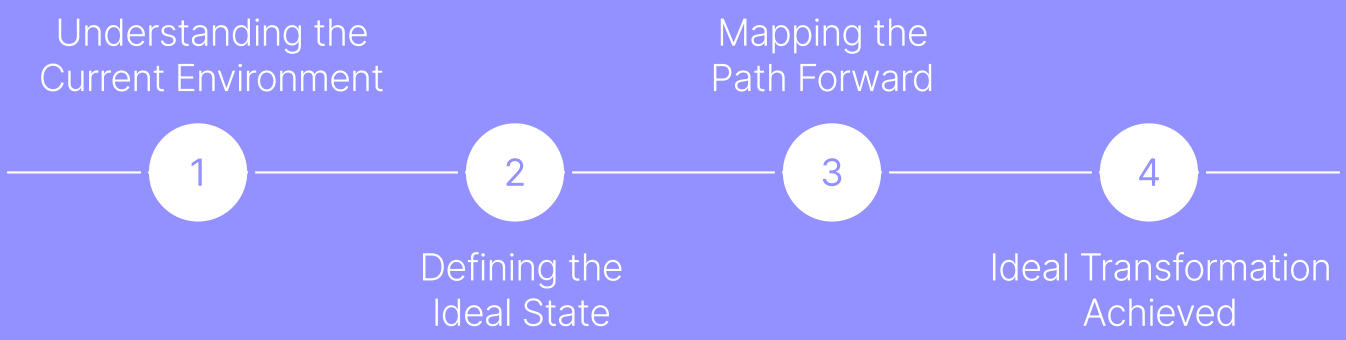
Joel Ferreira described their cloud environment as:

> *"More than just a 'black box'! Everything around it was also pitch black. We had zero visibility into things like: How many databases are there? How many servers do we have? Firewalls? What does our security look like? What are our risks?"*
>
> **Joel Ferreira, Senior Manager of Cloud Engineering & Operations**

That was the moment when HAVI reached out to Tarmac.

## Goal:

Goal: Enable HAVI *to define* and *map the path* from their "current" cloud environment to their "ideal" state. The "ideal" being a modernized, cost-effective, well-documented, and in-house managed Azure cloud environment.



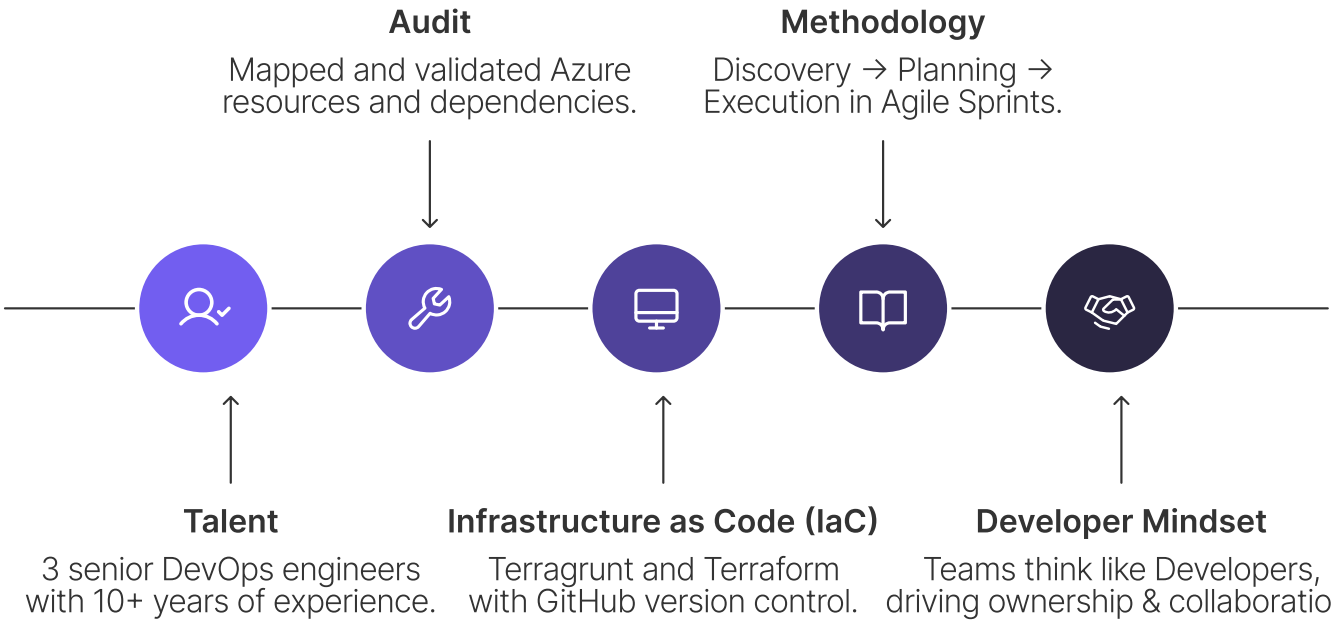
## Solution:

The proposed solution was to conduct a comprehensive, yet easily consumable DevOps Audit. The report was to incorporate proper documentation alongside graphs, network maps & images. Furthermore, it would include short-term "quick wins" (3, 6, 12 months) as well as a long-term roadmap (3-5 years).

The company's restructuring and instability meant that this would not be a "simple" consulting project following a "Requirements → Proposal → Delivery" model. Joel Ferreira did not want to rely on traditional consulting; he needed people who would "wear the shirt of the company".

Having worked with Tarmac successfully on another project at a previous company, he knew Tarmac was well-equipped to handle the complex situation:

> *"There was a lot of uncertainty, a lot of things that needed to be done to chart our path. It was never like 'Tarmac is coming here to do this, this, and this.' It was a lot of mutual exploration and discovery. From my experience with other companies, when a consultant is in an environment where they have to sink or swim, they usually sink. With Tarmac, it was the opposite."*
>
> **Joel Ferreira, Senior Manager of Cloud Engineering & Operations**



The Tarmac team combined deep expertise, structured methodologies, and industry-leading tools to ensure every step of the project was clearly scoped, validated, and executed. From auditing resources and dependencies to implementing Infrastructure as Code with Terragrunt and Terraform, every phase was planned and executed in alignment with Agile practices and a developer-first mindset.

This approach allowed for efficient collaboration, clear visibility across the environment, and ensured that the internal teams were empowered to take ownership of the cloud infrastructure.

Initial meetings to get to know their internal teams helped us get an overview of their company structure as well as current landscape, including the cloud environment(s), tooling & processes.

A Global Read-Only access allowed for a non-intrusive discovery phase.
We conducted a structured Azure DevOps and cloud environment audit using a phased, evidence-based approach. We performed a full inventory and configuration review using the following:

- Azure Resource Inventory and Azure Resource Graph to map all resources and dependencies
- Manual validation through Azure Portal and Command Line Interface (CLI) for accuracy
- Azure DevOps review of pipelines, repositories, service connections and governance controls
- Security posture checks across Rule-Based Access Control (RBAC), Azure Policy, Defender for Cloud and identity configuration

Technical sessions with the team helped us understand the operational context. We covered workflows, infrastructure dependencies, and runtime environments, including Virtual Machines where applicable.

Based on our findings, we developed a prioritized remediation plan aligned to Azure and DevOps best practices. Work was executed in incremental phases:

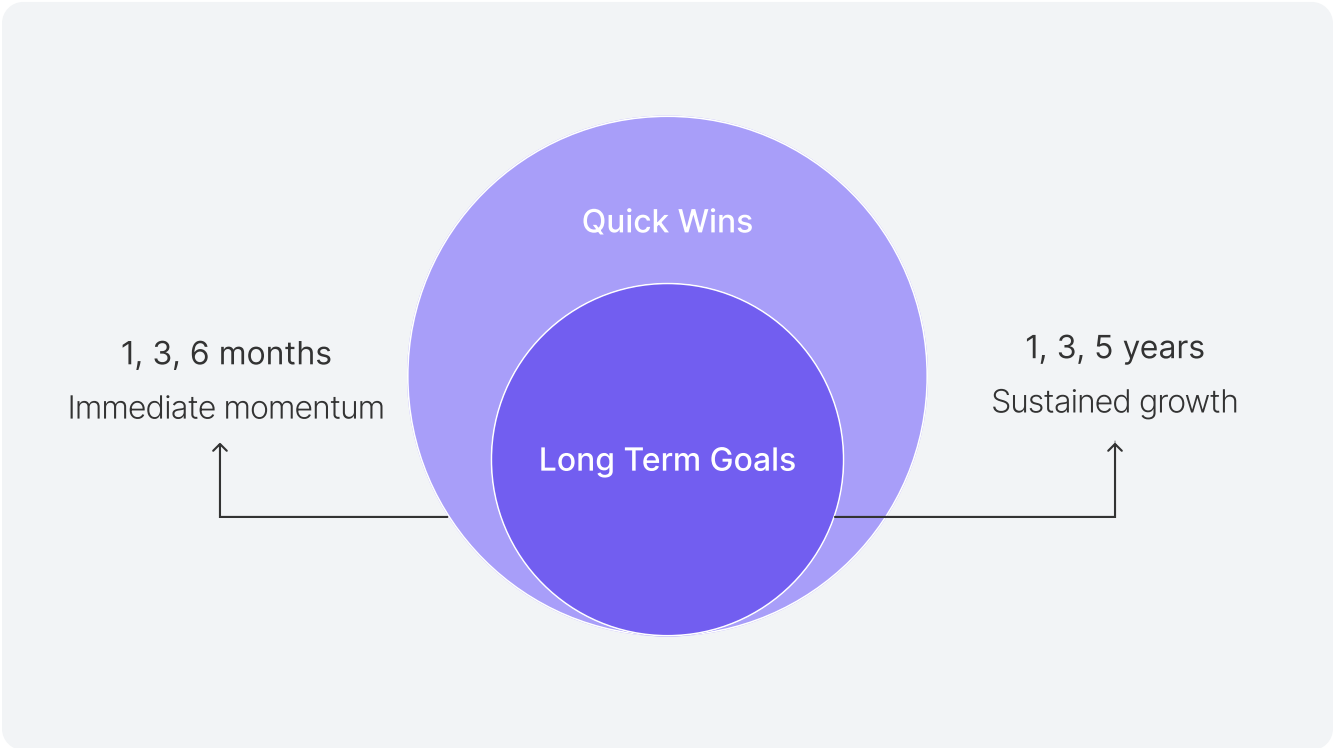
- Critical risk reduction (identity, access, exposed assets)
- Stability and consistency improvements
- Governance and automation enforcement
- Scalability and operational optimization

The methodology used ensured a comprehensive assessment, validated insights, and measurable improvements without disrupting ongoing operations.

## Result

The audit was the first step to gaining visibility and control over a disorganized and siloed environment. The comprehensive assessment covered Tenant and Subscription Structure, Operational Management, Identity and Access Management, Network, Monitoring and Alerting, Security, and Privacy.

During the early stages of our work together, we surfaced critical security risks and misconfigurations that had previously gone undetected. We also identified cost inefficiencies from outsized systems and end-of-life draining resources.



The roadmap blended immediate security remediations with long-term architectural shifts, including:

1. Establish cloud foundations using Azure Blueprints and enforce security/ governance guardrails
2. Create a report of vulnerabilities, organize by criticality & start resolving them
3. Implement privileged access management and identity frameworks
4. Build detailed documentation and architectural definitions for future scaling
5. Use Infrastructure-as-Code to manage the infrastructure
6. Provision monitoring and alerting to ensure key components work as expected
7. Launch cost-optimization initiatives to shrink and rationalize infrastructure

**Highlighted below are 3 key areas that our client was able to achieve major improvements in:**

## Security:

During the initial phase of the audit, several critical security vulnerabilities were discovered across identity management, access control, and cloud configuration. While some basic safeguards were present, the environment contained multiple exposure points that significantly increased the risk of unauthorized access and service disruption.

**Key findings included:**

- As high as 27% percent of users and service principals had excessive or unnecessary permissions, violating the principle of least privilege.
- Multiple applications and services were operating without proper network segmentation, exposing them to lateral movement risks in the event of compromise.
- Sensitive resources (incl. databases and storage accounts) were lacking required security controls such as encryption enforcement, private endpoints, or role-based access permissions.
- Limited visibility into identity and access activity, due to insufficient logging and alerting across Azure Active Directory and Azure resources.
- Minimal Disaster Recovery and business continuity planning increased the likelihood of extended downtime in the event of an incident.

These combined issues resulted in a heightened overall security risk, particularly around identity compromise and data exposure.

We organized the security risks into threat levels and presented the findings to our customer. From there, we worked with the corresponding teams (networking, product owners, security, and access and identity teams), initiating immediate remediation efforts to address the most severe vulnerabilities. We also established processes and policies to maintain those changes and ensure compliance.

Resolving the most concerning findings, the director was now positioned to also introduce organizational changes, such as implementing a new "Joiners, Movers, Leavers (JML)" process, and other similar IT Service Management (ITSM) procedures.

## Cost Savings

The initial rapid shift to the cloud didn't allow for the most ideal or efficient migration.

Part of our engagement was therefore to remedy issues that had surfaced. Our goals were to: rightsize provisions, transition off end-of-life services, cut costs where applicable, ensure all cloud services were up-to-par in terms of security, and document *everything*.

Utilizing Azure Resource Inventory and Azure Advisor we tracked down overprovisioned and/or outdated resources, as well as deprecated runtimes or services that needed attention. From there we created a plan incorporating quick wins (e.g. unused "extra" resources, end-of-life services, updating operating systems on VMs), and long-term plans (e.g. implementation & migration to IaC).

We were able to identify opportunities that would reduce costs by 22% once fully implemented. Additionally, further cost savings and efficiency gains were achieved by implementing Infrastructure-as-Code frameworks, which transformed what had previously been an entirely manual and third-party-supported process.

## Infrastructure-as-Code (IaC)

HAVI struggled with an entirely manual "Clickops" infrastructure process. Being a global enterprise, this approach was not only incredibly taxing to manage but also prone to errors, difficult to duplicate, and lacked scalability. Ultimately, it became too heavy a lift to manage in-house, which led to them outsourcing their infrastructure management to a 3rd party.

By implementing an IaC approach, using Terraform and Terragrunt, with Github as version control, the following was achieved:

They can now create/manage/ decommission resources in seconds, with all resources following the same guidelines

Resources created with modules and wrappers to reduce code volume and improve clarity

Improved processes with Github pull-requests, code reviews, and roll-back options to reduce the chance for manual errors

As a result, the time required to manage and maintain their Azure Infrastructure was significantly cut down. **This enabled our clients' in-house team to retake ownership of these tasks, eliminating the need for third-party support in this area.**

"I have multiple examples of working with Tarmac that whatever we throw at them, they would figure it out. This is exactly where Tarmac shines for me - the capability of their people that are externals, to behave like internal employees. I think that's the great differentiator.

Everyone here recognizes how important you guys were...there is an awareness that anytime we need something...to augment a team, to bring new capabilities on board...*Tarmac is that partner for us.*"

**Joel Ferreira, Senior Manager of Cloud Engineering & Operations**

## Have a project you think Tarmac could help with?

**Find us here.**