

CODIFY

Understanding what “Good” looks like in modern Azure environments

AZURE BENCHMARKING AND CLOUD MATURITY GUIDE

© Codify 2026. All rights reserved.

EXECUTIVE OVERVIEW

Azure benchmarking is often misunderstood as a cost-cutting exercise. In practice, the most valuable benchmarks are not about spending less; they are about understanding **cloud maturity, risk exposure**, and whether investment aligns with what modern Azure environments require.

Mature Azure environments do not simply reduce spend.

They **spend differently:**

- Less on duplication
- Less on legacy patterns
- More on visibility, governance, and resilience

In this context, savings are not the finish line. They are the **funding mechanism for maturity.**

Codify's Azure Benchmark is designed to make this maturity visible, measurable, and explainable.

ABOUT AZURE BENCHMARKING

How Codify Measures Azure Cloud Maturity

Codify's Azure Benchmark evaluates environments across two complementary dimensions. Together, these dimensions provide a balanced view of how effectively an organisation is running, protecting, and governing its Azure environment.

1. Workload Investment

This dimension represents the cost of **running workloads** in Azure, including:

- Virtual machines
- Databases
- Storage
- Windows and SQL licensing



Most organisations focus optimisation efforts here first. While important, optimisation at the workload layer alone rarely delivers sustainable improvement. Without equivalent maturity in governance and protection, workload efficiency gains are often offset by increased risk or long-term operating cost.

2. Operational and Protection Investment

This dimension reflects how well the environment is **protected, governed, and operated,** including spend on:

- Network security and firewalls
- Microsoft Defender and Microsoft Sentinel
- Backup and disaster recovery
- Monitoring and operational tooling

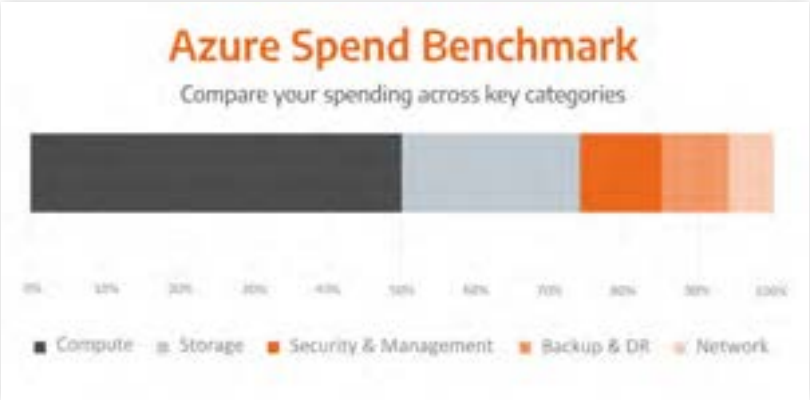
In mature environments, investment in these areas is **deliberate and proportionate to risk**, regulatory requirements, and business criticality.

By comparing workload and operational investment against Codify's benchmark baseline — and against peer environments of similar size and industry — clear maturity patterns emerge.

What “Good” Looks Like Through a Benchmark Lens

When environments are compared to Codify’s Azure Benchmark, consistent and repeatable indicators of cloud maturity appear. These indicators are not theoretical; they are observed across healthcare, manufacturing, retail, and government environments.

At a high level, good Azure environments demonstrate **balance, intention, and explainability.**



1. Balanced Investment Across Workloads and Operations

Mature environments allocate spend deliberately across both benchmark dimensions:

- Workload spend is right-sized, governed, and actively optimised
- Operational and protection spend is aligned to organisational risk and regulatory context

Less mature environments skew heavily to one side — either workload-heavy with minimal protection, or heavily protected with duplicated and inefficient tooling.

Benchmark observation

In multiple post-migration environments, workload optimisation practices such as Reservations and Azure Hybrid Benefit were well established. However, overall Azure spend still exceeded forecast when measured against benchmark peers.

Benchmark analysis revealed a disproportionate allocation toward operational tooling, particularly network security, without a corresponding reduction in workload or architectural complexity. In these environments, optimisation had occurred in isolation rather than as part of a balanced strategy across workloads and protection.

This observation reinforces that cloud maturity requires proportional investment across both dimensions. Optimising one layer while allowing the other to expand unchecked leads to cost drift and architectural imbalance.

2. Minimal Duplication in Security and Networking

Benchmark-aligned environments typically show:

- A single, consistent firewall and network security strategy across cloud and on-premises
- Controlled and intentional data ingestion into Microsoft Sentinel
- Clear ownership and purpose for each enabled security platform

Excessive tool overlap is consistently one of the strongest indicators of **low maturity,** not strong security.

Benchmark observation

Several benchmarked environments demonstrated elevated security spend driven by duplicated network security platforms. A common pattern was the deployment of Azure Firewall alongside an existing third-party firewall estate, resulting in overlapping controls across cloud and on-premises.

When compared to Codify’s benchmark baseline, these environments showed increased Microsoft Sentinel ingestion volumes without a corresponding improvement in detection outcomes. The issue was not under-investment in security, but duplicated architecture increasing cost and complexity.

This pattern consistently indicates **lower architectural maturity**, where tooling decisions are made incrementally rather than strategically.

3. Active Licensing and Consumption Management

High-maturity environments treat licensing and consumption as an ongoing operational discipline:

- Reservations and Azure Hybrid Benefit are actively managed
- Constrained vCPU SKUs are used where appropriate, particularly for SQL workloads
- Workloads are regularly right-sized based on utilisation data

Licensing optimisation is not a one-off exercise; it is continuous and measurable.

Benchmark observation

In cost-conscious environments, benchmark comparisons frequently revealed expired Reservations and under-optimised licensing models. Although overall Azure spend appeared reasonable at a surface level, licensing inefficiencies contributed to gradual and often unnoticed cost escalation.

Environments aligned to the benchmark demonstrated active management of Azure Hybrid Benefit, ongoing review of Reservations, and the use of constrained vCPU SKUs where appropriate. Environments that lacked this discipline consistently underperformed against maturity peers.

The benchmark highlights that **licensing optimisation is an operating discipline,** not a one-time exercise.

4. Security Capabilities Used — Not Just Enabled

Benchmark-aligned environments demonstrate:

- Defender and Sentinel configured and tuned, not passively collecting data
- MFA and Conditional Access applied consistently for both privileged and standard users
- Security tooling aligned to defined operational processes

Paying for security tooling without operating it is a common maturity anti-pattern uncovered during benchmarking.

Benchmark observation

Across multiple industries, environments were observed with Microsoft Sentinel and Defender enabled but not actively tuned or operationally integrated. In these cases, security platforms generated data and cost, but provided limited operational value.

Benchmark-aligned environments demonstrated clear configuration intent, controlled data ingestion, and alignment between security tooling and operational response processes. Conversely, passive enablement without ownership or tuning emerged repeatedly as a maturity anti-pattern.

This observation confirms that **security maturity is defined by operation, not activation.**

5. Alignment to a Modern Azure Architecture

Mature Azure environments typically demonstrate:

- Adoption of Azure landing zones
- Native backup, patching, and monitoring where appropriate
- Reduced reliance on legacy on-premises patterns post-migration

Lift-and-shift is treated as a **transition phase**, not an end state.

Benchmark Observation

In several lift-and-shift migrations, benchmark comparison revealed a maturity plateau following initial cloud adoption. Common characteristics included oversized virtual machines, orphaned resources, reliance on legacy operational tooling, and limited adoption of Azure landing zones.

Although migration objectives were technically achieved, these environments diverged significantly from benchmark peers that had progressed to modern architectures using native backup, patching, monitoring, and governance patterns.

The benchmark consistently shows **that migration is a starting point**, not an end state. Architectural evolution is required to realise sustained cloud maturity.

> “The benchmarking shows where you can safely cut — and where reinvestment delivers the biggest impact.”
>
> **Ben Parker**
>
> Director, Codify

WHY AZURE BENCHMARKING

Why Azure Benchmarking Is Becoming Essential

Azure benchmarking is evolving from a nice-to-have into a **core governance practice.**

For leadership teams, effective benchmarking enables:

- Evidence-based conversations between IT and finance
- Early identification of structural cost and security risk
- A measurable view of cloud maturity over time

In a landscape where cloud complexity grows faster than budgets, benchmarking is no longer about proving Azure is expensive. It is about ensuring Azure investment is **intentional, defensible, and mature.**



BENCHMARK OBSERVATIONS – CASE STUDIES

The following observations illustrate how real environments behave when measured against Codify's Azure Benchmark.

Benchmark Observation 1:

Security Spend Can Mask Architectural Duplication

In several post-migration environments, workload optimisation practices such as Reservations and Azure Hybrid Benefit were well implemented, yet overall Azure spend exceeded forecast.

When compared to Codify's benchmark baseline, this variance was traced to duplicated security architecture. In one environment, Azure Firewall was deployed alongside an existing third-party firewall platform, resulting in overlapping controls and duplicate telemetry feeding into Microsoft Sentinel. The outcome was elevated operational cost without a corresponding improvement in security effectiveness.

This pattern demonstrates that **security maturity is driven by architectural consistency,** not the volume of tools deployed.

Benchmark Observation 2:

Low Cloud Spend Often Indicates Under-Investment, Not Optimisation

In contrast, some benchmarked environments appeared cost-efficient when viewed purely from a billing perspective. However, deeper comparison revealed minimal investment in foundational protection and operational tooling.

Common characteristics included expired Reservations, the absence of a cloud firewall, and limited use of Defender or monitoring capabilities. Against the benchmark, these environments consistently under-indexed on operational maturity.

This observation reinforces a recurring theme: **low spend is not a reliable indicator of optimisation.** In many cases, it reflects deferred risk rather than efficient design.

Benchmark Observation 3:

Lift-and-Shift Creates a Maturity Plateau Without Intentional Progression

Government and regulated environments frequently demonstrate a post-migration maturity plateau. Benchmark comparisons often reveal oversized workloads, orphaned resources, and security platforms that are enabled but not operationalised.

In these environments, Sentinel was active but not tuned, and Microsoft 365 E5 security capabilities were licensed but underutilised. While migration objectives were technically achieved, the benchmark showed a clear imbalance between workload investment and operational maturity.

This pattern highlights that **migration alone does not equate to cloud maturity.** Without deliberate reinvestment and architectural alignment, environments stall at an intermediate stage.

NEXT STEPS

See the Benchmark in Practice

Azure benchmarking is most valuable when applied to real environments. While the principles outlined in this report describe what maturity looks like, the greatest insight comes from seeing how your own Azure environment compares.

Codify offers two low-friction ways to engage:

View an Example Azure Benchmark Report

Request a sample benchmark report to see how Azure environments are assessed against peer benchmarks, how maturity signals are identified, and how optimisation and reinvestment opportunities are presented in a clear, executive-ready format.

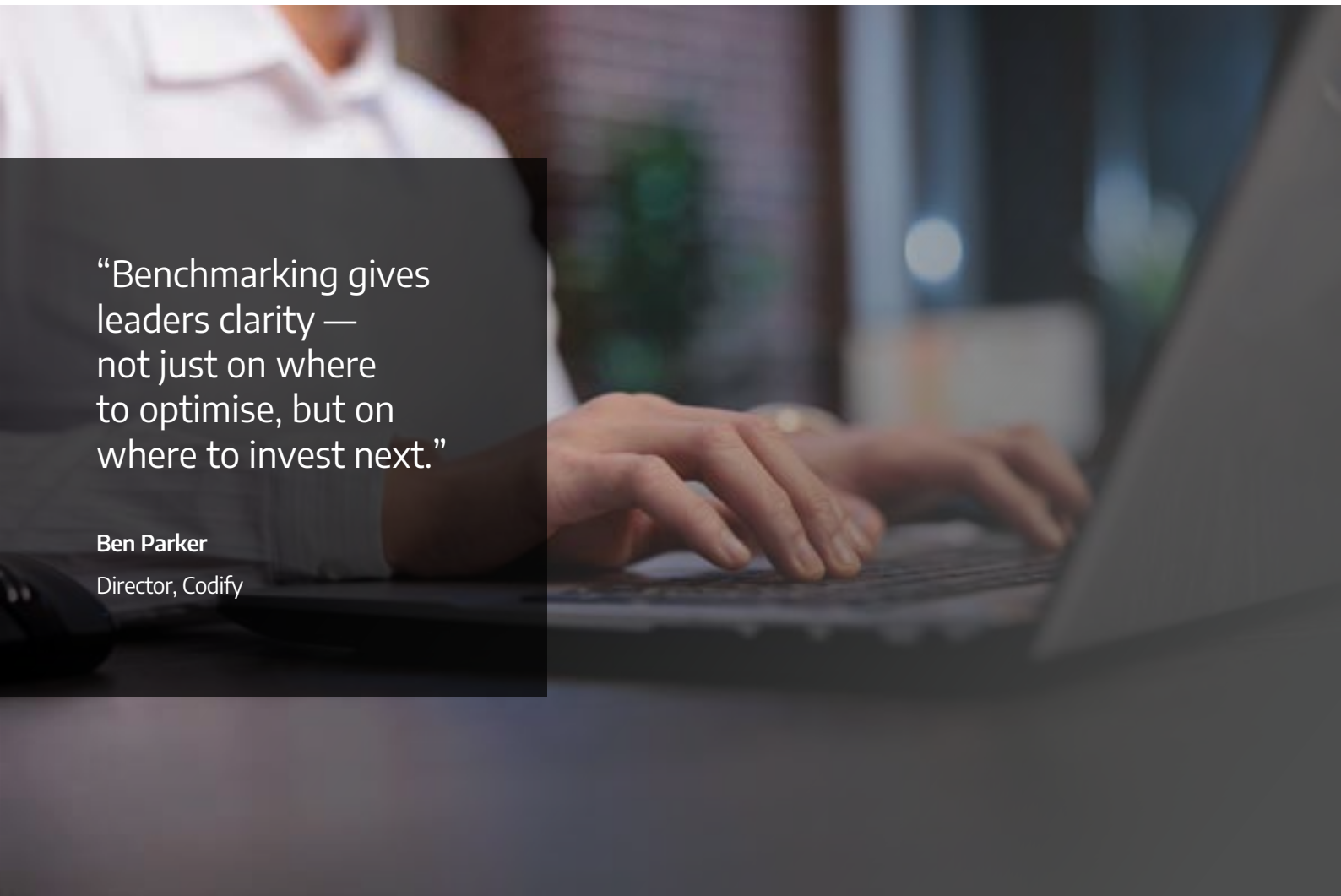
Order a Personalised Azure Benchmark

Organisations can also request a confidential, personalised Azure Benchmark based on their own live Azure consumption data. The report compares your environment against Codify's benchmark baseline and peer organisations of similar size and industry, highlighting:

- Where spend is well aligned
- Where duplication or imbalance exists
- Where optimisation savings can be safely realised
- Where reinvestment will deliver the greatest maturity uplift

The benchmark is evidence-based, anonymous, and designed to support constructive conversations between IT, security, and finance.

To request an example report or discuss a personalised Azure Benchmark, contact Codify at www.codify.com.au or speak directly with the Codify team.



"Benchmarking gives leaders clarity — not just on where to optimise, but on where to invest next."

Ben Parker

Director, Codify



Microsoft
Solutions Partner

Codify is a Microsoft Solutions Partner certified at the highest level in Azure Cloud Computing.

As one of Australia's leading Azure specialists, we bring deep technical expertise and a focused, proven approach to cloud transformation. We support organisations nationwide in maximising the value, performance, and security of their Microsoft Azure environment.

CODIFY

Call 1300 CODIFY
Visit Codify.com

COMPASS ASSURANCE SERVICES ISO 27001

COMPASS ASSURANCE SERVICES ISO 9001