Automation first with IaC

The worlds first 100% automated Azure onboarding with CAF Governance, Risk & Compliance

.... as far as we know

Audience:
Platform Owners, Cloud Center of Excellence (CCoE), Security Teams, and IT Operations.

Scope:
This document provides a detailed explanation of the platform foundation, security guardrails, and operational tasks delivered by **MyPlatform**, contrasted with the responsibilities owned by customers and/or partners. **MyPlatform** refers to our managed cloud service platform. By outlining these roles and responsibilities, this document helps ensure smooth collaboration and clear accountability between MyPlatform and its customers or partners.

Introduction: The MyPlatform service model

MyPlatform is an automated, code-first managed service that deploys, operates, and maintains a secure and compliant Azure foundation ***within your own Azure tenant***. As a code-first managed service, **MyPlatform** uses automated scripts and infrastructure-as-code principles to streamline both deployment and ongoing management, reducing manual effort and increasing consistency.

Our core mission is to simplify Governance, Risk, and Compliance (GRC) for Azure environments by automating essential processes, enabling your organization to innovate faster and with greater confidence than traditional approaches. By managing the routine tasks involved in maintaining security and compliance, **MyPlatform** frees your teams to focus on delivering business value through your applications and workloads. What sets **MyPlatform** apart is our ability to deliver rapid, scalable, and standards-aligned cloud foundations, backed by deep expertise in Azure security and compliance frameworks.

This model is delivered in two distinct phases, each with a clear division of responsibilities:

The build phase:	The initial, automated deployment of your Azure foundation.
The operate phase:	The ongoing, evergreen management and maintenance of the platform.

This whitepaper will explore the specific tasks within each phase, clarifying the roles of both **MyPlatform** and the Customer to ensure a transparent and successful partnership.

The in-house GRC team challenge has a universal hurdle

Before diving into the specifics of the RACI model, it's important to understand why a managed GRC service is so critical. Building and retaining a capable in-house GRC team is a significant and persistent challenge for organizations of all sizes.

For example, according to a recent industry survey at Fortinet, 76% of organizations report difficulty in hiring qualified GRC professionals, resulting in project delays and increased risk exposure. The rapid evolution of cloud technology has created a hyper-competitive, candidate-driven market for specialized talent, leading to common issues that transcend company size.

Managed GRC services offer organizations immediate access to experienced professionals and scalable solutions, helping them overcome talent shortages and adapt quickly to evolving compliance requirements. This sets the stage for a deeper look at the specific hurdles faced by different types of organizations.

For small & medium businesses (SMBs) - the affordability and retention gap
The primary barrier for SMBs is financial. The specialized skills required for cloud security, policy-as-code (IaC), and compliance frameworks are rare, and the salaries for these professionals are enterprise-grade. An SMB faces a multi-faceted problem:

Prohibitive cost of entry
The cost of hiring even a single senior cloud GRC specialist can consume a disproportionate amount of the IT budget, let alone building a team with diverse competencies.

Key-person dependency
If they do manage to hire one expert, the entire security and compliance posture of their cloud environment rests on a single individual. This creates an enormous business risk if that person leaves, gets sick, or makes a mistake.

Inability to retain talent
Even if an SMB can afford the salary, they often can't compete with larger corporations on benefits, career progression, training budgets, or the allure of working on massive, complex projects. Talented engineers often view SMB roles as steppingstones, leading to high turnover and a constant, disruptive cycle of hiring and retraining.

For corporate organizations - the war for talent and the skills churn.
Mid-sized to large corporations may have the budget, but they face a fierce and unending battle for talent against the very hyperscalers and tech giants that build the platforms.

Intense recruitment competition
Top-tier GRC and cloud security architects are in extremely high demand. The recruitment cycle to find, vet, and hire a qualified candidate can easily stretch from six to nine months, delaying critical projects

High attrition rates
Specialized talent is constantly being poached by competitors, consulting firms, and cloud providers. This high churn rate leads to a significant loss of institutional knowledge, project continuity breaks, and a perpetual strain on HR and existing team members who must cover the gaps

The rapidly diminishing "skills half-life"
Cloud technology evolves at a blistering pace. A skill set that is cutting-edge today can be standard or even outdated in 18-24 months. This means companies are in a constant, expensive race to retrain and certify their in-house teams, a significant hidden cost of maintaining an internal GRC practice.

For enterprises - the strategic value proposition and opportunity cost
Even for large enterprises with the resources to build a world-class GRC team, the question becomes one of optimal value and strategic focus.

Undifferentiated heavy lifting
Managing foundational GRC is business-critical, but it is not a business differentiator. Like electricity or physical data center security, it is a form of "digital plumbing"—it must be perfect, but customers don't buy a product because of the company's Azure Policy implementation

The opportunity cost of talent
The most significant issue is opportunity cost. Every hour your most brilliant (and expensive) cloud architects spend on maintaining platform guardrails, tracking Azure service updates, or ensuring baseline compliance is an hour they are *not* spending on architecting the next-generation, revenue-generating workloads that create a real competitive advantage

Focusing on business innovation
By offloading the foundational GRC to a specialized service, enterprises can liberate their best minds. This allows top-tier talent to focus their energy on strategic initiatives—like building new AI platforms, modernizing legacy applications, or expanding global e-commerce systems—that directly drive business growth and innovation.

The consultant approach: the risk of fractional dependency

Many organizations attempt to bridge the gap by hiring external consultants or freelancers for fractional (e.g., 1-2 days per week) GRC support. However, this model introduces its own significant risks. For example, fractional consultants may lack deep organizational context, leading to misaligned priorities or inconsistent policy enforcement.

Other challenges include reduced availability during critical incidents and gaps in ongoing communication with in-house teams. In one case, a company relying on part-time GRC consultants experienced delays in incident response due to unclear ownership of responsibilities, highlighting the potential consequences of depending on external resources for essential functions.

Scarcity and inflexibility

Truly valuable, senior consultants are a scarce resource and rarely available for affordable, long-term, part-time contracts. They are incentivized to take on larger, more lucrative full-time projects, making it difficult to secure their commitment

"Golden handcuffs" dependency

When a company does find a willing consultant, they often become a single point of failure. All critical GRC knowledge, custom scripts, and operational history reside with one external individual. This creates a dangerous dependency, effectively "locking in" the company to that specific person. The cost and operational risk of them leaving or becoming unavailable are enormous, turning a perceived flexible solution into a significant liability

Part 1: The build phase - automated foundation deployment

The Build phase transforms a process that traditionally takes hundreds of consulting hours into a fully automated, repeatable deployment that completes in minutes. MyPlatform is **Responsible** and **Accountable** for the automated provisioning of the core infrastructure. The Customer is **Responsible** and **Accountable** for initiating the process and granting the necessary permissions.

1.1 Azure Marketplace purchase & tenant consent

What it is: The formal initiation of the MyPlatform service. This step contractually and technically links your Azure tenant to the MyPlatform service, enabling the automated deployment

MyPlatform's Role (Consulted): We provide the official offer on the Azure Marketplace. Our service validates the entitlement once you complete the purchase

Customer's Role (Responsible/Accountable): You initiate and complete the purchase through the Azure Marketplace using an account with Entra ID Global Administrator rights. This one-time action grants consent for the MyPlatform application to operate within your tenant under a least-privilege model

1.2 Automated bootstrap process

What it is: The core automated engine that builds the foundation. After consent is granted, this process runs to create the necessary service principals (Enterprise Applications) and assign them the minimal roles required for deployment

MyPlatform's Role (Consulted): We design, build, and maintain the automation sequence, ensuring it is secure, efficient, and aligned with Microsoft's best practices

Customer's Role (Responsible/Accountable): You trigger the bootstrap process from our portal. This is a self-service, seamless action that starts the foundational build-out.

1.3 Management group hierarchy

What it is: The organizational backbone of your Azure environment. A logical hierarchy is crucial for applying policies, managing access, and organizing subscriptions at scale

MyPlatform's Role (Responsible/Accountable): Our code automatically deploys a best-practice Management Group structure aligned with the Microsoft Cloud Adoption Framework (CAF). This typically includes roots for Platform, Landing Zones, Sandboxes, and Decommissioned subscriptions. This structure ensures that governance is inherited logically and efficiently

Customer's Role (Informed): You receive a fully structured environment ready for your subscriptions

A cautionary tale: the governance chaos

A company started its cloud journey without a structured Management Group hierarchy. Different teams created subscriptions as needed, leading to "subscription sprawl." When auditors asked for a list of all production databases, no one could provide a definitive answer. A critical security policy to enforce encryption was only applied to a few subscriptions, leaving sensitive data in others exposed. The lack of structure made governance impossible and turned a simple audit request into a months-long remediation project.

1.4 Core logging and diagnostics

What it is: The establishment of a centralized logging foundation. Capturing the right logs from the start is critical for security monitoring, auditing, and troubleshooting

MyPlatform's Role (Responsible/Accountable): We automatically deploy a central Log Analytics Workspace and configure your Entra ID Diagnostic Settings to stream all critical identity and access logs (like sign-ins and audit logs) to this workspace

Customer's Role (Accountable): You are accountable for the data within the workspace, including setting appropriate log retention periods to meet your specific compliance and privacy requirements (e.g., GDPR)

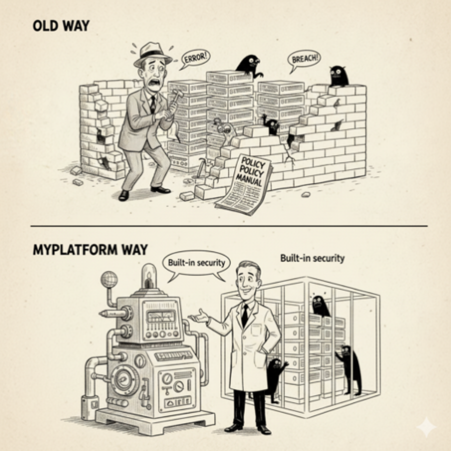
1.5 Privileged identity management (PIM) foundation

What it is: A foundational security service to manage, control, and monitor access to important resources. PIM provides "just-in-time" (JIT) privileged access, drastically reducing the risk of compromised administrator accounts

MyPlatform's Role (Responsible/Accountable): We create and PIM-enable the core administrative role groups for the platform (e.g., Platform Contributor, Policy Contributor). This means that instead of having standing admin rights, users must request, justify, and be approved for temporary elevated access

Customer's Role (Informed at build, Accountable in operate): You are informed of the groups created. Post-deployment, you are fully responsible for managing PIM policies (e.g., requiring multi-factor authentication for activation, setting maximum activation times) and managing group memberships

A cautionary tale: the compromised admin
An IT administrator with standing "Contributor" rights on a production subscription had their credentials compromised in a phishing attack. The attacker, now possessing powerful, always-on privileges, deleted a critical production database before the breach was even detected. Had the access been managed through PIM, the attacker would have gained nothing, as the administrator's account would have had no active roles. The need for the attacker to go through a PIM activation request with MFA and justification would have alerted the security team and thwarted the attack.



1.6 Azure Policy and Defender for Cloud baseline

What it is: The automated deployment of "guardrails" that enforce your organization's standards and security policies across the entire Azure environment

MyPlatform's Role (Responsible/Accountable): We deploy a comprehensive suite of Azure Policy definitions and initiatives as code. These policies cover security, governance, and cost management. Examples include:
Security: Enforcing encryption, blocking public IPs on certain resources
Governance: Enforcing resource tagging, restricting deployments to approved regions. We also enable the foundational plans of Microsoft Defender for Cloud to provide a baseline of security posture management

Customer's Role (Informed): You receive an environment where security and governance are "built-in," not "bolted-on." You can later tune these policies by creating exemptions or adjusting parameters

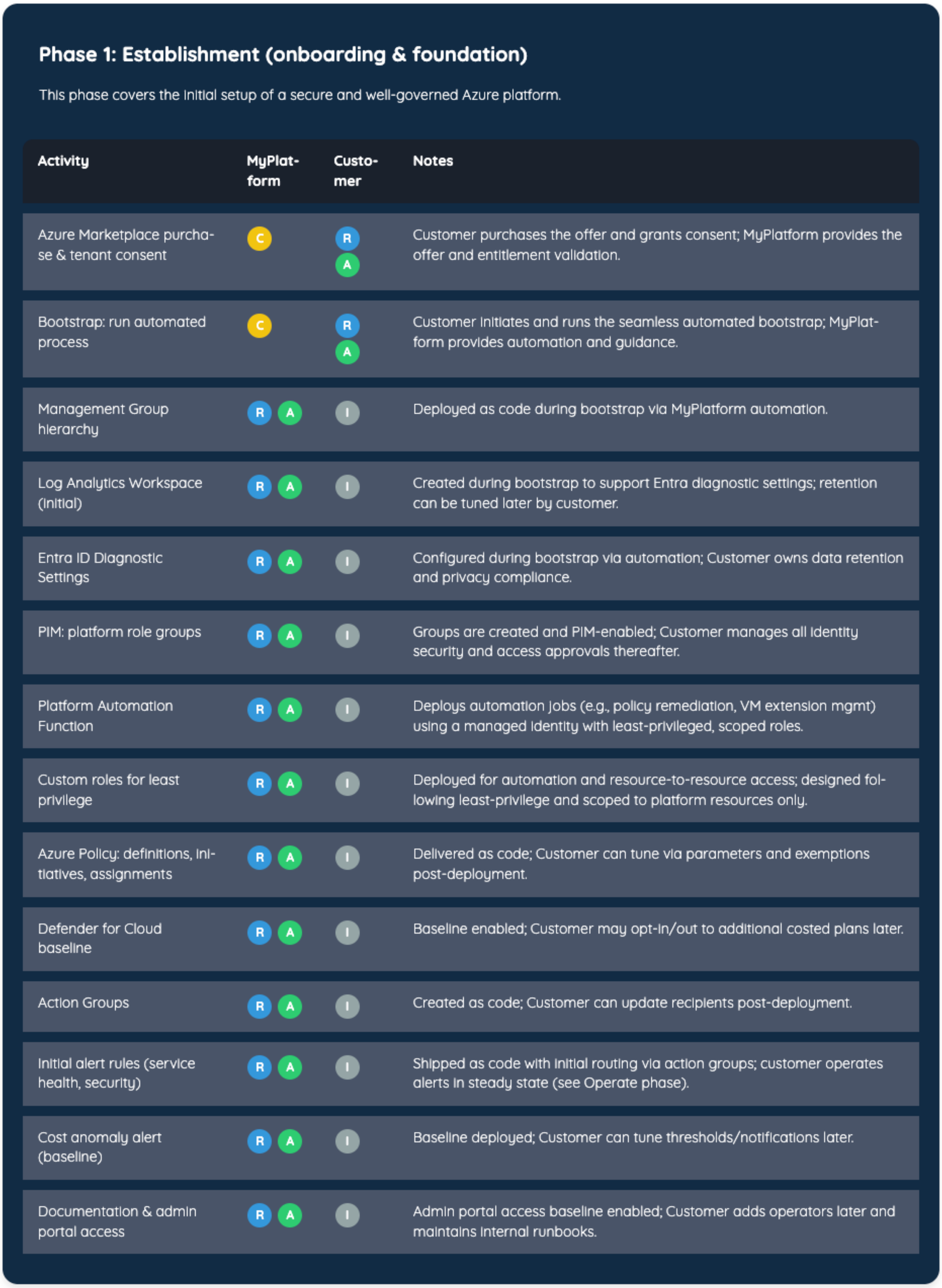
1.7 Initial alerting framework

What it is: A pre-configured set of alerts for critical events related to platform health, security, and cost

MyPlatform's Role (Responsible/Accountable): We deploy Action Groups and a baseline set of alert rules as code. This includes alerts for Service Health events, high-severity security alerts from Defender for Cloud, and a foundational cost anomaly alert

Customer's Role (Informed): You receive a platform with proactive monitoring from day one. Post-deployment, you can customize the notification recipients in the Action Groups (e.g., routing alerts to your ITSM tool or on-call team)

Following is a complete list of **MyPlatform** services as defined by the RACI model.



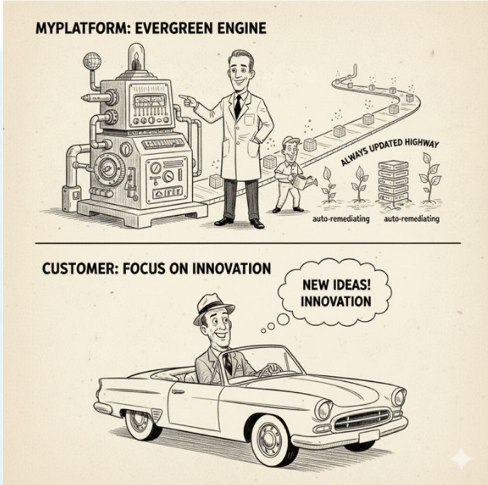
Phase 1: Establishment (onboarding & foundation)

This phase covers the initial setup of a secure and well-governed Azure platform.

Activity	MyPlatform	Customer	Notes
Azure Marketplace purchase & tenant consent	C	R A	Customer purchases the offer and grants consent; MyPlatform provides the offer and entitlement validation.
Bootstrap: run automated process	C	R A	Customer initiates and runs the seamless automated bootstrap; MyPlatform provides automation and guidance.
Management Group hierarchy	R A	I	Deployed as code during bootstrap via MyPlatform automation.
Log Analytics Workspace (initial)	R A	I	Created during bootstrap to support Entra diagnostic settings; retention can be tuned later by customer.
Entra ID Diagnostic Settings	R A	I	Configured during bootstrap via automation; Customer owns data retention and privacy compliance.
PIM: platform role groups	R A	I	Groups are created and PIM-enabled; Customer manages all identity security and access approvals thereafter.
Platform Automation Function	R A	I	Deploys automation jobs (e.g., policy remediation, VM extension mgmt) using a managed identity with least-privileged, scoped roles.
Custom roles for least privilege	R A	I	Deployed for automation and resource-to-resource access; designed following least-privilege and scoped to platform resources only.
Azure Policy: definitions, initiatives, assignments	R A	I	Delivered as code; Customer can tune via parameters and exemptions post-deployment.
Defender for Cloud baseline	R A	I	Baseline enabled; Customer may opt-in/out to additional costed plans later.
Action Groups	R A	I	Created as code; Customer can update recipients post-deployment.
Initial alert rules (service health, security)	R A	I	Shipped as code with initial routing via action groups; customer operates alerts in steady state (see Operate phase).
Cost anomaly alert (baseline)	R A	I	Baseline deployed; Customer can tune thresholds/notifications later.
Documentation & admin portal access	R A	I	Admin portal access baseline enabled; Customer adds operators later and maintains internal runbooks.

Part 2: The operate phase - evergreen governance

In the Operate phase, MyPlatform remains **Responsible** and **Accountable** for keeping the platform's GRC framework up-to-date ("evergreen"). The Customer is **Responsible** and **Accountable** for all aspects of day-to-day IT operations, including workload management, security incident response, and cost optimization.



2.1 Evergreen platform updates

What it is: The continuous delivery of updates to the platform's code, policies, and configurations to adapt to the evolving Azure landscape and emerging security threats.

MyPlatform's Role (Responsible/Accountable): We continuously maintain the platform's Infrastructure as Code (IaC). When Microsoft releases new best practices, a compliance standard changes, or a new threat emerges, we update the platform's guardrails and deploy them to your environment. You are always aligned with the latest GRC standards without undertaking costly consulting projects.

Customer's Role (Informed/Consulted): We provide release notes for all material changes. For significant updates, particularly those with potential cost impacts (e.g., enabling a new Defender plan), we will consult with you for approval before deployment.

2.2 Policy compliance and remediation

What it is: The ongoing process of monitoring for and responding to non-compliant resources within Azure.

MyPlatform's Role (Responsible - for automation): Our platform includes automated remediation tasks for certain policies. For example, if a resource is missing a required tag, an automation job can add it. This reduces manual toil for your operational teams.

Customer's Role (Accountable/Responsible - for workloads): You are ultimately accountable for the compliance posture of your environment. Your teams are responsible for fixing non-compliant workloads (e.g., redesigning an application that violates a policy) and for managing the lifecycle of any policy exemptions

2.3 Alert triage and incident response

What it is: The 24/7 operational process of monitoring, investigating, and responding to security and operational alerts.

MyPlatform's Role (Informed): For platform-specific service health alerts, we are informed to ensure our service is operating correctly.

Customer's Role (Accountable/Responsible): Your Security Operations Center (SOC) or IT Operations team is fully responsible for responding to all alerts, including security threats, performance issues, and cost anomalies. MyPlatform provides the alerting framework; your team operates it.

2.4 Identity and access management

What it is: The complete lifecycle management of user identities, group memberships, access rights, and security policies like Multi-Factor Authentication (MFA)

MyPlatform's Role (Informed): We have no role in managing your identities. The platform is designed to rely on your existing identity provider (Entra ID)

Customer's Role (Accountable/Responsible): You are solely responsible for all aspects of identity security. This includes enforcing strong MFA and Conditional Access policies, managing the PIM approval process, designing and assigning Azure RBAC roles for your workload teams, and conducting periodic access reviews

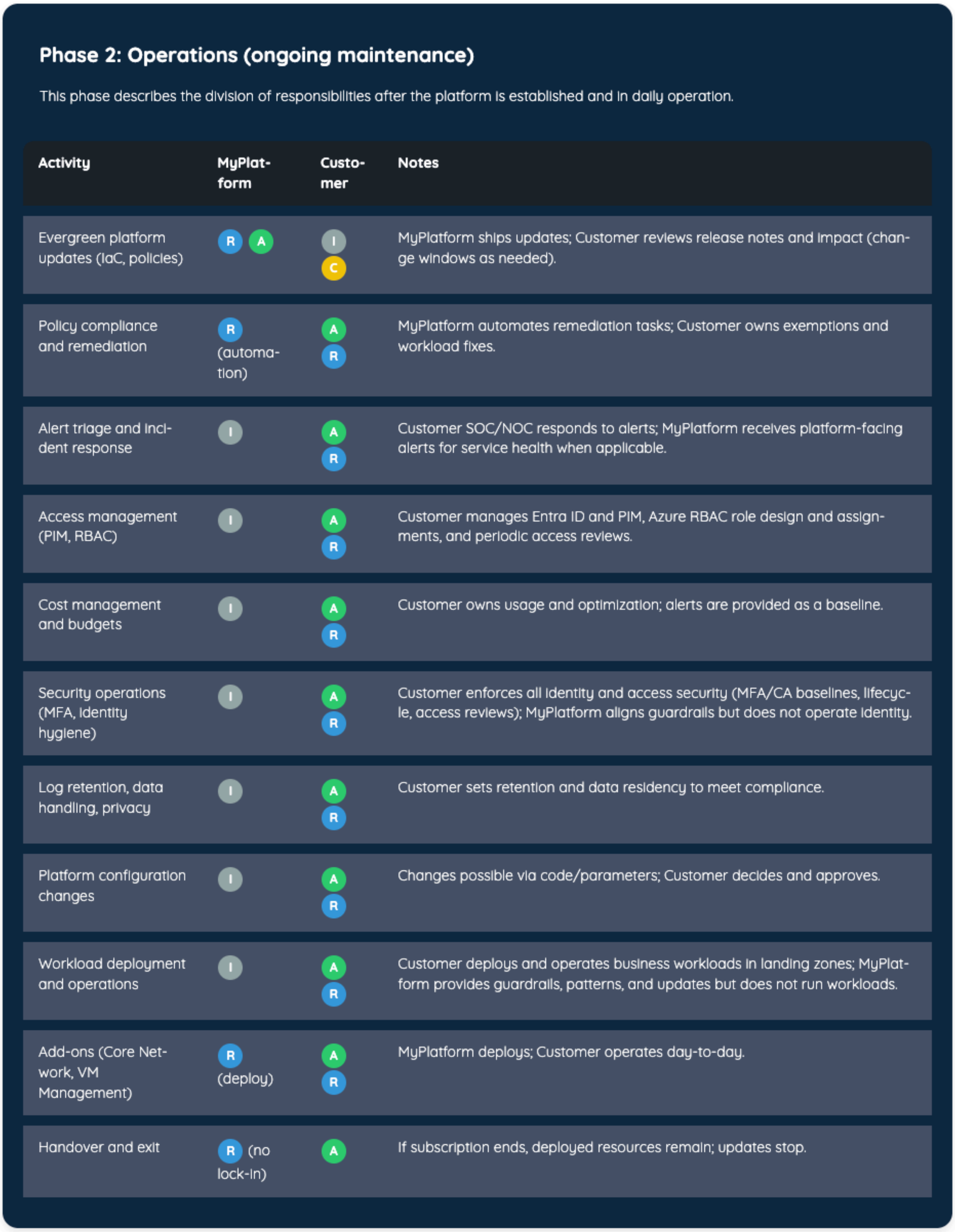
A cautionary tale: the lingering access
An employee left a company on amicable terms, but their user account was never properly de-provisioned from Azure. Months later, their old laptop was compromised. Because the account was still active and had access to sensitive code repositories and development environments, a threat actor used it to infiltrate the company's systems, steal intellectual property, and deploy ransomware. A rigorous identity lifecycle and access review process would have ensured the account was disabled on the employee's last day, preventing the entire incident.

2.5 Workload deployment and operations

What it is: The core purpose of your cloud adoption: deploying and managing the applications and services that run your business

MyPlatform's Role (Provides Guardrails): We provide the secure, compliant, and well-governed "landing zones" for your workloads. We ensure the highway is safe, well-lit, and has clear rules of the road

Customer's Role (Accountable/Responsible): You are fully responsible for designing, deploying, managing, and operating your business workloads within these landing zones. You drive the cars on the highway. This includes all aspects of application lifecycle management, patching, and performance



Phase 2: Operations (ongoing maintenance)

This phase describes the division of responsibilities after the platform is established and in daily operation.

Activity	MyPlatform	Customer	Notes
Evergreen platform updates (IaC, policies)	R A	I C	MyPlatform ships updates; Customer reviews release notes and impact (change windows as needed).
Policy compliance and remediation	R (automation)	A R	MyPlatform automates remediation tasks; Customer owns exemptions and workload fixes.
Alert triage and incident response	I	A R	Customer SOC/NOC responds to alerts; MyPlatform receives platform-facing alerts for service health when applicable.
Access management (PIM, RBAC)	I	A R	Customer manages Entra ID and PIM, Azure RBAC role design and assignments, and periodic access reviews.
Cost management and budgets	I	A R	Customer owns usage and optimization; alerts are provided as a baseline.
Security operations (MFA, identity hygiene)	I	A R	Customer enforces all identity and access security (MFA/CA baselines, lifecycle, access reviews); MyPlatform aligns guardrails but does not operate identity.
Log retention, data handling, privacy	I	A R	Customer sets retention and data residency to meet compliance.
Platform configuration changes	I	A R	Changes possible via code/parameters; Customer decides and approves.
Workload deployment and operations	I	A R	Customer deploys and operates business workloads in landing zones; MyPlatform provides guardrails, patterns, and updates but does not run workloads.
Add-ons (Core Network, VM Management)	R (deploy)	A R	MyPlatform deploys; Customer operates day-to-day.
Handover and exit	R (no lock-in)	A	If subscription ends, deployed resources remain; updates stop.

MyPlatform- a summary of advantages

For customers: accelerate and secure your cloud journey

MyPlatform provides a direct path to a mature, secure, and efficient Azure practice, allowing you to focus on business outcomes, not infrastructure complexity.

Radical acceleration (from months to minutes): Bypass 200-500 hours of traditional consulting. Our automated deployment delivers a best-practice Azure foundation in about 15 minutes, enabling you to start your projects immediately

Built-in governance, risk & compliance (GRC): We deploy a comprehensive security and governance framework from day one. This proactive approach ensures you are secure and compliant by design, eliminating the risks of manual misconfiguration

Reduced total cost of ownership (TCO): Shift from unpredictable, high upfront capital expenditure (CAPEX) on consulting to a predictable, transparent operational expenditure (OPEX) subscription model. Our automation dramatically lowers the ongoing cost of maintaining GRC

Operational efficiency: We manage the complex GRC settings and keep the platform evergreen. This liberates your internal IT staff from foundational maintenance, allowing them to focus on high-value business workloads and innovation

Enhanced security posture: Benefit from our deep expertise in security. We implement foundational controls like PIM, centralized logging, and Defender for Cloud, providing a robust security posture from the start

Full ownership and control: MyPlatform deploys all resources directly into your Azure tenant. You retain 100% ownership of your data and infrastructure. There is no vendor lock-in; you can unsubscribe after your term and keep everything we've built

For partners: build your business on a foundation of trust

MyPlatform acts as a strategic accelerator for our partners, removing roadblocks and enabling you to deliver your specialized services faster and more securely.

Focus on your core value: Stop spending non-billable time on foundational Azure setup. We handle the complex GRC infrastructure, allowing you to immediately start deploying your high-value Data & AI, ERP, or Modern Work solutions

Accelerate project delivery & time-to-value: Eliminate the number one cause of project delays: waiting for a secure and compliant environment. With MyPlatform, your client's foundation is ready in minutes, enabling you to deliver your solutions faster and recognize revenue sooner

Enhance client offerings & mitigate risk: Confidently offer a complete, end-to-end solution built on a professionally managed and secure Azure platform. This enhances your credibility and reduces the risk of infrastructure-related issues impacting your application

Scale your business efficiently: Our standardized, code-first landing zone allows you to replicate successful deployments across multiple clients with ease. This consistency reduces support overhead and enables you to scale your practice more effectively

Competitive differentiation: Stand out from the competition by offering a solution that is faster, more secure, and more cost-effective. You become a strategic advisor who de-risks the cloud journey for your clients

Tap into new markets: Our affordable OPEX model makes enterprise-grade GRC accessible to the SMB and mid-market segments. This opens up new revenue streams and allows you to deliver your advanced solutions to a previously underserved market