

The MSP Practice Builder

Structuring a Scalable, Profitable Cyber Resilience Business on Rubrik

ACCOUNTABILITY NOW DEFINES CYBER RESILIENCE

Cyber resilience is no longer judged by the tools an enterprise owns; it is judged by whether resilience outcomes can be executed reliably under pressure. While recovery is the ultimate accountability moment, MSP-operated cyber resilience spans protection, detection, investigation, and recovery across hybrid and SaaS environments.

When ransomware spreads or systems fail, consequences are immediate: revenue interruption, regulatory exposure, executive scrutiny, and board-level escalation. In that moment, deployment checklists are irrelevant. Execution is decisive.

Responsibility is consolidating around providers trusted to operate resilience continuously. Enterprises are transferring outcome ownership and expecting MSPs to deliver:



Continuous Readiness

Maintaining protection integrity and recovery confidence as an operating state.



Cross-environment Consistency

Ensuring predictable lifecycle behavior across workloads.



Incident-time Decisiveness

Executing coordinated response without improvisation.

Demand is durable. Scrutiny is rising. The operating model must evolve.

WHEN ACCOUNTABILITY RISES, STRUCTURAL FRICTION EMERGES

Many MSP ecosystems were built for transactional resale—not lifecycle ownership. As responsibility increases, structural constraints surface:

- **Monetization lag**, delaying recurring revenue stabilization by three to six months when onboarding and tenant provisioning are fragmented.
- **Early-stage capital exposure**, compressing margin when licensing commitments precede validated demand.
- **Linear scaling**, forcing headcount to grow in parallel with revenue when centralized leverage is absent.
- **Diligence pressure**, lengthening sales cycles when execution maturity cannot be demonstrated.

These constraints are structural, not technical. As accountability rises, misalignment becomes financially visible through margin pressure and operational drag.

Scaling a profitable resilience practice requires structural alignment—not incremental optimization.

WHAT STRUCTURAL ALIGNMENT REQUIRES

Operating cyber resilience as a scalable business requires five elements to function as a system:

- **Governance aligned to service maturity**, rewarding operational excellence rather than transaction volume.
- **Economics aligned to growth**, protecting margin during validation and strengthening it at scale.
- **Platform execution aligned to lifecycle operation**, ensuring consistent behavior across tenancy models.
- **Incident reinforcement aligned to accountability**, supporting execution under pressure.
- **Trust signaling aligned to performance**, allowing credibility to compound through demonstrated maturity.

When these elements operate independently, friction accumulates. When aligned, scale becomes durable.

THE PRACTICE BUILDER: STRUCTURAL ALIGNMENT IN ACTION

Rubrik aligns governance, economics, platform execution, incident reinforcement, and trust recognition into a cohesive system built for MSP-operated cyber resilience.

This reflects sustained organizational investment in MSP-operated resilience as a long-term strategic direction—not a short-term commercial adjustment. It is a durable operating commitment.

GOVERNANCE ALIGNED TO SERVICE MATURITY

The Rubrik Transform Partner Program (RTPP) includes a formal MSP framework aligned to operational accountability.

- **Service-maturity tiering (Select, Expert, Master)** recognizing sustained delivery discipline.
- **Unified governance under an MSP Program Addendum**, preserving consistency within a single framework.

Governance reflects how services are operated—not simply sold.



ECONOMICS: START WITHOUT BETTING THE BUSINESS

Managed services grow incrementally. Economics must protect margin during validation.

MSP PayGo aligns cost to real consumption and removes front-loaded friction.



Activation-stage Flexibility

Enabling zero monthly minimum commitment



Scale-stage Efficiency

Introducing discounted pricing as usage stabilizes

A PRACTICAL ILLUSTRATION

Under a traditional license model, an MSP might commit \$25,000 per month before demand stabilizes. If utilization runs at 50% for four months, margin compresses during the most fragile stage of growth.

Under a consumption-aligned activation model, cost tracks actual usage. Capital remains available while packaging and demand are validated. As usage stabilizes, discounted tiers strengthen unit economics rather than strain them.

Commitment follows validation. Margin durability improves as the practice matures.

PLATFORM EXECUTION ACROSS THE FULL LIFECYCLE

Rubrik supports consistent lifecycle execution across hybrid and SaaS environments.

- **Dedicated Tenants with MSP Console**, providing tenant-level isolation and centralized oversight.
- **Shared cluster multitenancy**, per-tenant activation of premium capabilities, while supporting multiple customers on a single Rubrik cluster

Standardized lifecycle behavior and centralized visibility ensure scale increases leverage rather than complexity.

SERVICES ENABLED ACROSS THE LIFECYCLE

Structural alignment translates directly into recurring service revenue. Rubrik enables MSPs to design and operate lifecycle services such as:

-  **Managed Data Protection Services**, covering backup operations and SLA enforcement.
-  **Ransomware Detection and Coordinated Response Services**, integrating anomaly detection and threat hunting with recovery execution. With replication between Rubrik clusters, MSPs can offer disaster recovery as a value add.
-  **Identity and Access Resilience Services**, protecting critical identity infrastructure.
-  **Recovery Orchestration Services**, delivering validated, predictable restoration.
-  **Investigation and Forensics Services**, accelerating analysis through integrated telemetry.
-  **Isolated Recovery Environments (IRE)**: MSPs can now provision a recovery environment for a tenant and operate it as a recurring managed service. With replication to the IRE, data is scanned for malware indicators before recovery begins, giving MSPs a provable clean copy during an incident before any workloads have to be restored.

These offerings are monetized as ongoing lifecycle operations—not one-time project deployments.

INCIDENT REINFORCEMENT UNDER PRESSURE

Execution credibility is tested during disruption.

- **24x7 Ransomware Response Team (RRT) support**, reinforcing MSP-led execution during active incidents.
- **Coordinated response capability**, strengthening enterprise confidence.

Recovery is the accountability moment. Lifecycle discipline determines performance when it arrives.

CREDIBILITY THAT COMPOUNDS WITH PERFORMANCE



RUBRIK VERIFIED™ is an earned designation available to eligible Expert and Master tier MSPs within RTPP who demonstrate:

- **Operational maturity.** Rubrik validated minimum operating standards in delivering Rubrik-based cyber resilience services.

Why Verified? An **enterprise-visible differentiation**, reducing diligence friction and accelerating evaluation.

THE ECONOMIC IMPACT OF STRUCTURAL ALIGNMENT

Dimension	Traditional License Model	Rubrik MSP-Aligned Model
Upfront Risk	High commitment before validation	\$0 Minimum Activation (PayGo)
Revenue Stabilization	3 – 6 month lag	Monetization aligned to activation
Unit Economics	Margin compressed during ramp	Strengthens at scale via PayGo
Operational Scaling	Headcount-driven growth	Software-driven operational leverage
Credibility Signal	Reputation-based differentiation	RUBRIK VERIFIED™ designation

The difference is structural. It reshapes profitability as accountability increases.

DEPLOYMENT CLARITY AND SHARED RESPONSIBILITY

Rubrik operates within shared-responsibility models while preserving MSP ownership.

- **Single MSP PayGo agreement**, simplifying administration.
- **Telemetry-driven SaaS billing**, increasing transparency.
- **Non-disruptive tenancy evolution**, allowing service maturity without replatforming.

Growth does not require architectural reset.

THE STRATEGIC PLATFORM BET

The market has shifted from tool ownership to outcome accountability across the cyber resilience lifecycle. Enterprises select providers based on execution reliability, operational maturity, and sustained readiness.

As accountability rises, structural alignment determines which MSPs scale profitably—and which encounter structural ceilings.

Rubrik is built for MSPs who intend to operate cyber resilience as a long-term business—and to perform when it matters most.

NEXT STEP

Engage your Rubrik partner or account representative to evaluate how your governance model, commercial structure, and service maturity align to rising enterprise accountability expectations.



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) is the Security and AI Operations Company, delivering one platform built at the intersection of data, identity, and AI. The platform enables agentic cyber resilience and trusted AI operations for enterprises worldwide, built to recover before disruption strikes and stay a step ahead, so security is never the reason ambition stalls. For more information, please visit www.rubrik.com and follow Rubrik on LinkedIn and X.