



Evaluating MSP-Operated Cyber Resilience

What to Look For in a RUBRIK VERIFIED™ Partner

ACCOUNTABILITY IS JUDGED UNDER PRESSURE

Cyber resilience is no longer judged by the tools an enterprise owns; it is judged by whether protection holds, threats are detected early, impact is investigated quickly, and recovery executes predictably under pressure.

When ransomware spreads or critical systems fail, consequences are immediate: revenue interruption, regulatory exposure, customer impact, executive scrutiny, and board escalation. In that moment, architecture diagrams are secondary; execution is decisive.

Enterprises increasingly engage Managed Service Providers (MSPs) to operate portions of the cyber resilience lifecycle. But transferring execution does not transfer accountability. Boards and regulators continue to hold the enterprise responsible for outcomes.

The evaluation question therefore becomes:

Can this provider demonstrate sustained operational maturity across the full lifecycle of protection, detection, investigation, and recovery?

WHY EVALUATION STANDARDS MUST RISE

As accountability increases, traditional MSP selection criteria are no longer sufficient.

Common gaps include:

- Revenue-based qualification, which reflects sales performance rather than operational discipline.
- Feature-based positioning, which describes platform capability but not execution maturity.
- Reference-led validation, which reflects isolated experiences rather than sustained lifecycle rigor.

Operated resilience requires structural alignment — not just tool familiarity.

As board scrutiny increases, evaluation rigor must increase with it.

FIVE CRITERIA FOR EVALUATING AN MSP-OPERATED MODEL

When assessing a provider to operate cyber resilience, evaluate five dimensions.

1 Governance and Operational Discipline

Look for clearly defined ownership across protection, detection, investigation, and recovery workflows.

A mature partner demonstrates:

- Documented 24x7x365 first-line support obligations

- Structured escalation and incident playbooks
- Defined RPO and RTO governance
- Executive-ready reporting visibility

Operational maturity must be measured by discipline — not tier alone.

2 Lifecycle Integration Across Environments

Protection, anomaly detection, impact analysis, and recovery workflows must operate as a coordinated system.

Assess whether the provider can demonstrate:

- Consistent execution across hybrid, cloud, and SaaS workloads
- Defined workflows rather than ad hoc cross-team coordination
- Validated clean recovery point identification

Lifecycle cohesion reduces improvisation under pressure.

3 Architecture and Tenancy Alignment

Execution maturity must align to architecture.

Evaluate whether the MSP's deployed tenancy model matches your isolation and oversight requirements:

- Shared tenancy models should demonstrate disciplined isolation and consistent service execution within architectural constraints.
- Dedicated tenancy models should demonstrate mature lifecycle governance across isolated environments with centralized oversight.

Operational discipline must be evaluated within the architecture actually deployed — not assumed beyond it.

4 Incident Reinforcement and Recovery Execution

Execution credibility is tested during disruption.

Assess whether the provider:

- Maintains continuous readiness validation
- Demonstrates defined restore workflows
- Coordinates effectively with Rubrik's 24x7 Ransomware Response Team (RRT) during active incidents

Recovery performance is the accountability moment. Preparation determines outcome.

5 Demonstrated Operational Maturity—RUBRIK VERIFIED™

Rubrik Verified is an earned designation within the Rubrik Transform Partner Program (RTPP) for MSPs. It reflects an MSP's operational maturity.

RUBRIK VERIFIED:

- Is not automatic upon reaching a partner tier
- Requires meeting defined minimum operating standards
- Applies within the capabilities of the deployed tenancy architecture
- Reflects that those standards were met when reviewed by Rubrik.



RUBRIK VERIFIED is not:

- a certification, compliance accreditation, warranty, or guarantee of recovery outcomes.
- An endorsement of an MSP's services by Rubrik.

Customers should not rely on the VERIFIED designation alone when evaluating an MSP and should conduct their own due diligence. Learn more about VERIFIED, including what the designation covers and its limitations: <https://www.rubrik.com/content/dam/rubrik/en/resources/policy/rubrik-verified-designation-disclaimer.pdf>

HOW RUBRIK VERIFIED™ COMPLEMENTS ENTERPRISE DUE DILIGENCE

The comparison below separates what your own due diligence covers from the specific items Rubrik's review adds.

Evaluation Lens	Standard MSP Due Diligence	Covered by Rubrik's Review (RUBRIK VERIFIED™)
Qualification basis	Provider documentation, references, and program status	Review against Rubrik's defined operating standards
Support and recovery testing	You assess support coverage and how recovery is tested	24x7x365 support with Rubrik-certified staff, and restoration drills at least twice a year
Service commitments	You review contractual service levels and reporting	Contractual RTO/RPO commitments with performance reporting
Security controls	You evaluate the provider's security posture	MFA for administrative access, retention lock, audit logging, and role-based access controls
Architecture and escalation	You assess available capabilities, isolation, and escalation paths	Services reviewed within the deployed tenancy architecture, with a defined path to Rubrik support
Role in the decision	Core customer due diligence	Additional input, not a substitute for due diligence

Each row maps to a defined standard the MSP met at review, giving the enterprise specific, verifiable inputs to weigh.

OPERATING MODEL FLEXIBILITY—WITHOUT ARCHITECTURAL RESET

Enterprise accountability remains constant regardless of operating model. What changes is who executes day-to-day workflows.

Rubrik supports:

- Self-Managed execution by enterprise teams
- Co-Managed execution shared with a partner
- MSP-Operated execution under enterprise-defined policies

In all models:

- Data ownership remains with the enterprise
- Recovery objectives remain enterprise-defined
- Reporting and validation remain enterprise-visible

Transitioning between models does not require replatforming. Tenancy and governance structures evolve without architectural redesign.

THE GOVERNANCE-LEVEL DECISION

Cyber resilience is evaluated at the moment of recovery. That moment reveals whether lifecycle discipline has been sustained long before disruption occurs. Selecting an MSP-operated model requires evaluating more than capability. It requires assessing execution maturity within the platform being operated.

RUBRIK VERIFIED reflects that an MSP met defined operating standards when reviewed, within the capabilities of its deployed tenancy architecture. It does not replace enterprise due diligence or ongoing oversight. As accountability intensifies, evaluation standards must rise with it.

NEXT STEP

Engage your Rubrik account representative to:

- Identify RUBRIK VERIFIED partners aligned to your operating model
- Review governance structures, tenancy alignment, and lifecycle discipline
- Assess whether your current MSP-operated approach meets board-level accountability expectations

Predictable resilience is not a feature decision. It is an operating model decision — and it is evaluated under pressure.



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

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

Rubrik (NYSE: RBRK) the Security and AI company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn. Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

brf-evaluating-msp-operated-cyber-resilience / 20260821