

WHAT TO ACTUALLY COMPARE WHEN EVALUATING RECOVERY OPTIONS

Recovery is one of the only capabilities that cannot be tested under real conditions until it is actually needed. Every technology provider can claim to offer proven recovery solutions. Almost none specify how that would actually be verified.

This framework sets out seven questions worth putting to any option under evaluation, including Evolution Systems.

**1**

TESTING CADENCE AND DOCUMENTATION

How often is recovery actually tested, at what scale, and is the outcome documented in a form that would satisfy an auditor or insurer on request? Anyone who cannot answer this with specifics has not been asked it enough.

ISOLATION AND IMMUTABILITY

Is the backup environment logically separated from production, with credentials managed independently? Does an immutable copy exist that cannot be altered even by someone with administrative access to the platform? This is architecture, not a checkbox.

**2****3**

RECOVERY ACCOUNTABILITY

When something goes wrong, who owns the outcome, and is that ownership documented before an incident rather than assigned during one?

RESTORE SCALE AND SPEED

If a significant portion of your environment needed to come back at once, how long would that take, and is there a documented result to back up the answer?



SOVEREIGNTY AND WORKLOAD COVERAGE

Where does the data actually sit, and under whose jurisdiction? Can the platform protect workloads consistently across on-premises, private cloud, and public cloud, or does coverage stop wherever is easiest to support?

MANAGED VERSUS SELF-MANAGED OVERHEAD

Is your team expected to operate the platform, or is outcome ownership genuinely transferred? These produce very different operational realities six months in.



ANOMALY DETECTION AND EARLY WARNING

Can the platform identify indicators of a ransomware event inside backup metadata before a recovery event is ever needed? A platform that only responds once data is already compromised is solving a different problem to one that can flag the compromise while there is still time to act.

Specific answers to all seven questions tell you more than any product name attached to them ever will.

USING THIS FRAMEWORK

Share it with whoever else is involved in the evaluation. The technical evaluator will read it differently to the risk approver, and that is the point. A framework that only makes sense to one person in the buying process will not survive the rest of it.

