elastio™

WHITE PAPER

Ransomware Recovery & Resilience Maturity Model

Executive Overview for Board & Risk Committees

Ransomware recovery & resilience is underdeveloped and too often treated as a checkbox. Backup and recovery are assumed to work when needed, but are rarely validated and tested. In today's threat landscape, **you cannot be resilient if you cannot prove recovery**.

Provable recovery must be recognized as a **core security control**, a critical layer in the cybersecurity stack that directly impacts operational risk, regulatory exposure, and governance oversight.

Regulators **(NYDFS, DORA, PCI-DSS)**, insurers, and boards increasingly expect evidence that recovery is continuously validated, not assumed. This framework helps assess your current posture and provides a roadmap to ransomware readiness.

Level 1 **Initial** (Ad Hoc)	**Level 2** **Managed** (Developing)	**Level 3** **Defined** (Documented)	**Level 4** **Advanced** (Measured)	**Level 5** **Optimized** (Adaptive)
Backups exist but untested, no ransomware scanning, undefined recovery process.	Immutable storage used, 3-2-1-1-0 rule applied, initial recovery planning in place.	Behavioral detection in backups, SIEM/XDR integration, clean-copy identification.	Continuous validation via ML, real-time R-PRO tracking, audit-ready reports.	Autonomous backup validation and real-time scoring with zero-trust aligned recovery.

Board-Level Impact

1. Prove you can recover cleanly from ransomware *before an attack happens*.
2. Demonstrate regulatory readiness (NYDFS, DORA, CISA) with verifiable recovery controls.
3. Minimize downtime and data loss, protect revenue, brand, and operational continuity.

About the Model

This model incorporates industry best practices and frameworks. It aligns with NIST's Ransomware Framework Profile (CSF functions) and FS-ISAC crisis management guidance, while highlighting advanced controls emphasized in vendor research.

Structurally, it draws from the CMMI five-level maturity model to offer a clear, sequential roadmap for operational improvement. This hybrid approach bridges the gap between strategic **standards** and **practical execution**, enabling organizations to move from basic hygiene toward continuously measured and provable recovery readiness.

Level 1: Initial (Ad Hoc)

Organizations at this stage operate under the assumption that backups will work, but there is no structured effort to ensure they are recoverable. Recovery is untested, and ransomware resilience is reactive or nonexistent.

Capability	Description
Backup Hygiene	Backups are ad hoc, often unmanaged, stored on local or vulnerable media. There is no immutability, encryption, or isolation, leaving them open to compromise.
Data Integrity & Compromise Detection	No validation is performed on backup data. Scanning for ransomware encryption or corruption is nonexistent. Integrity is assumed, not proven.
Recovery Testing	Recovery has never been tested or measured. RTO/RPO are unknown, and no one is formally responsible for verifying backup recoverability.
Governance & Metrics	No metrics exist for resilience or recovery. Cyber risk is not reported to the board, and there's no visibility into the state of backups.
Regulatory & Compliance	There is no alignment to frameworks like NYDFS, DORA, or CISA guidance.
Culture & Ownership	Resilience is seen as a back-office IT concern. Backup and recovery are treated as infrastructure tasks, not as part of risk governance.

Risk of staying here:
You won't know backups are compromised until it's too late, and recovery will likely fail under ransomware pressure.

To progress to Level 2:
Establish consistent backups, introduce immutability, and begin implementing data integrity scanning and incident planning.

Board View: Key Questions & KPIs

- Are backups being created and stored securely across critical systems?
- Do we know our RPO/RTO targets and whether we can meet them?
- Who is accountable for validating our ability to recover from ransomware?

Level 2: Managed (Developing)

Organizations at this stage begin introducing structure and basic safeguards into their backup and recovery processes. While controls like immutability and scheduled scans are introduced, recovery is still largely unproven, and ransomware resilience remains immature.

Capability	Description
Backup Hygiene	Backups are now regularly scheduled and protected with immutable storage. The organization begins adopting the 3-2-1 rule, and encryption at rest is enabled for some workloads. Backup coverage may be inconsistent across systems. 3 – Keep **3 copies** of your data 2 – Store the copies on **2 different types of media or storage** 1 – Keep 1 copy **offsite**
Data Integrity & Compromise Detection	Prioritized backups are scanned for ransomware encryption or corruption on a schedule but not every backup is scanned automatically, leaving gaps in recovery visibility.
Recovery Testing	Basic recovery drills are conducted periodically for a few systems. Restore instructions exist, but testing is not yet systematic or logged. RPO/RTO targets are defined for some services, but they are not measured consistently.
Governance & Metrics	Initial reporting to leadership begins. Some recovery KPIs are proposed but not tracked in real time. Board awareness of ransomware risk remains limited.
Regulatory & Compliance	The organization begins to review NYDFS, DORA, or internal compliance requirements. Recovery policies are being documented but are not yet audit-ready.
Culture & Ownership	Cyber recovery is gaining visibility. However, ownership remains siloed, and executive sponsorship is informal. Funding is typically reactive.

Risk of staying here:
You may believe recovery is possible, but there's no proof and you may not be in a position to detect encryption-based attacks early, exposing business to greater downtime and data loss risk.

To progress to Level 3:
Document recovery workflows, introduce behavioral scanning for every backup, and establish measurable recovery metrics and team accountability.

Board View: Key Questions & KPIs

- Are our backups immutable and isolated from production?
- Are any backups scanned for ransomware or corruption?
- Have we conducted at least one ransomware recovery test?

Level 3: Defined (Documented & Integrated)

Organizations at this stage have formalized recovery as a cross-functional process. Backup policies, testing procedures, and detection controls are documented and integrated into broader operational and risk frameworks

Capability	Description
Backup Hygiene	A consistent backup strategy is implemented across all critical workloads. Backups follow the 3-2-1-1-0 model. 3 – Keep **3 copies of your data** 2 – Store the copies on **2 different types of media or storage** 1 – Keep 1 copy **offsite** 1 – Keep 1 copy **offline, immutable,** or **air-gapped** 0 – Zero errors after **data integrity** and **recovery** testing
Data Integrity & Compromise Detection	Backup data integrity scans are performed in alignment with company RPOs and become a core component of security telemetry. They provide visibility into the trustworthiness of data, informing detection, response, and recovery decisions.
Recovery Testing	Recovery processes are documented and scheduled. Restore success/failure is tracked and tied to SLA inputs. RPO/RTO performance is monitored and improved.
Governance & Metrics	Integrated dashboards visualize resilience, displaying metrics like "Ransomware Resilience Score," encryption activity, recovery assurance, and % of assets meeting RPO. Industry guidance highlights the value of such dashboards: unified security consoles let organizations "identify risk exposure and recover data" quickly. (See Figure 1 below for an example.)
Regulatory & Compliance	Processes are mapped to frameworks. Evidence of clean recovery is prepared for audit. Remediation of gaps is structured and managed.
Culture & Ownership	Recovery assurance is now a shared responsibility across business and technical teams with semi-regular cross-functional check-ins on status.

Risk of staying here:
You have structure but limited automation. Threats could still bypass detection, and slow recovery could still cause major disruption.

To progress to Level 4:
Automate testing, implement AI-powered detection, and begin treating recovery performance as a measurable control.

Board View: Key Questions & KPIs

- What % of our backups have been validated in the past 30 days?
- Is recovery performance (RPO/RTO) tracked and improving?
- Do our incident response plans cover ransomware-specific scenarios?

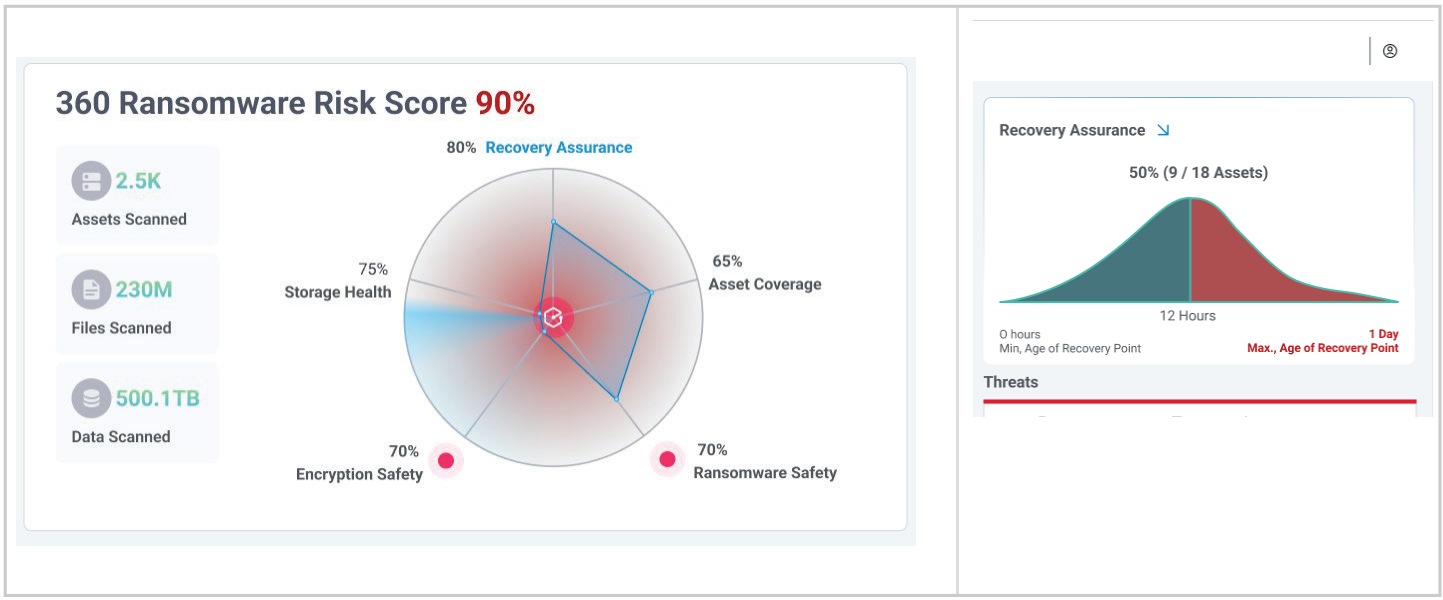

Figure 1: Ransomware Resilience Dashboard.

This dashboard shows unified metrics, "Ransomware Risk Score," percentage of assets within target RPO, and counts of assets/files/data scanned. It highlights how many systems meet recovery objectives and where shortfalls exist. Centralized dashboards like this are recommended for executive visibility: A single security dashboard allows admins to quickly identify risk exposure and recover data.

A graphic view lets executive teams immediately grasp recovery readiness and focus on remediation.

Level 4: Advanced (Measured & Verified)

Recovery is now a measurable control with continuous validation, behavioral scanning of backup data, and SLA-based assurance. Resilience is demonstrated through data, not assumptions.

Capability	Description
Backup Hygiene	All critical systems are covered by immutable, air-gapped, and scanned backups. Backup health is continuously assessed and prioritized by business impact.
Data Integrity & Compromise Detection	Every backup is scanned for malicious encryption and data corruption, using ML-based behavioral engines, to detect slow encryption attacks and maintain a continuous inventory of clean recovery points.

Level 4 continued

Capability	Description
Recovery Testing	Restore testing is automated, and failure is actionable. Metrics are tracked by service and environment (e.g. hybrid/cloud).
Governance & Metrics	Resilience KPIs, such as Ransomware RPO (R-RPO) metrics and compliance dashboards, are visible in real-time and used for executive and board reporting.
Regulatory & Compliance	Audit-ready recovery documentation is standard. Controls are mapped to frameworks and verified by internal/external stakeholders.
Culture & Ownership	Recovery assurance is part of organizational identity. It's funded proactively and reviewed consistently by leadership.

Risk of staying here:
You may still rely on static playbooks and slow decision cycles during high-impact events — limiting response speed.

To progress to Level 5:
Enable real-time threat-aware orchestration, predictive scanning, and integrate recovery confidence into executive and business KPIs.

Board View: Key Questions & KPIs

- Can we prove to regulators or insurers that our backups are clean and restorable?
- What is our Recovery Assurance % across mission-critical systems?
- How quickly can we recover cleanly from a ransomware event?

This diagram illustrates adding a dedicated scan layer between primary data and backup vaults. A service (e.g., Elastio) independently inspects each backup or snapshot ("Secondary Data") for ransomware encryption, unauthorized encryption, ransomware binaries, and corruption before it is stored in the air-gapped failover environment.

In advanced maturity, this data-integrity layer is core: it "fills a critical gap" by ensuring backups are clean. Any detections trigger alerts (to SIEM/SOAR). By proactively validating backups in this way, the organization can trust that its fall-back data is truly clean and restorable.

Level 5: Optimized (Adaptive & Resilient)

Recovery is now a proactive, predictive, and continuously assured control. Ransomware resilience is embedded in operations, governance, and strategy. Recoverability is no longer assumed — it's proven.

Capability	Description
Backup Hygiene	Backups are policy-driven, autonomously validated, and prioritized by SLA risk. They are integrated with DR orchestration and scored for resilience.
Data Integrity & Compromise Detection	Backups are not considered valid unless proven clean. Continuous, policy-driven integrity validation becomes a foundational requirement for ransomware resilience and compliance.
Recovery Testing	Testing is continuous, risk-driven, and built into daily workflows. Clean recovery points are always available, logged, and auditable.
Governance & Metrics	Resilience is a board-level metric, updated live and aligned with SLAs. Recovery Assurance is benchmarked and improved continuously.
Regulatory & Compliance	Recovery evidence is generated continuously and aligned to global frameworks. Reporting is automated and on-demand.
Culture & Ownership	Recovery assurance is owned at the highest levels. Resilience is part of strategic planning and external influence (e.g. policy, vendor collaboration).

What's Next: Beyond Level 5

Leading organizations are beginning to explore autonomous recovery orchestration, predictive analytics to pre-scan at-risk workloads, and resilience testing across supply chains and partners. These next-generation capabilities turn recovery from a reactive failsafe into a dynamic strategic advantage.

Board View: Key Questions & KPIs

- Is recovery readiness tracked in real-time alongside other business KPIs?
- How much ransomware risk have we eliminated through provable clean backups?
- Are we continuously validating recovery across changing infrastructure and threats?

Appendix

NYDFS Mapping

Maturity Level	Relevant NYDFS Section(s)	Mapping Language
Level 1 – Initial	*500.02, 500.06*	At this stage, recovery capabilities are untested, and organizations lack a defined incident response plan, falling short of NYDFS 500.06, which requires formalized incident response procedures.
Level 2 – Managed	*500.02(b), 500.06, 500.14*	Organizations begin to align with NYDFS requirements by introducing immutable storage and establishing initial recovery processes. However, testing and board oversight remain informal.
Level 3 – Defined	*500.02, 500.06, 500.07*	With behavioral backup scanning and recovery planning in place, the organization begins meeting NYDFS expectations for programmatic response plans, documentation, and board-reportable cyber risk posture.
Level 4 – Advanced	*500.07, 500.16, 500.17*	Continuous validation, R-RPO metrics, and audit-ready recovery evidence directly support NYDFS's call for tested, provable, and board-reviewed cybersecurity programs.
Level 5 – Optimized	*500.02(c), 500.17(b)*	Autonomous, adaptive recovery capabilities fulfill NYDFS's highest standards for maturity, accountability, and measurable cyber resilience under the revised 2023 amendments.

EU DORA Mapping

Maturity Level	Relevant DORA Article(s)	Mapping Language
Level 1 – Initial	*Art. 5, 11*	Basic backups exist, but without ICT risk governance or structured response, falling short of DORA's Article 5 mandate for comprehensive risk management frameworks.
Level 2 – Managed	*Art. 6–8, 17*	Early planning and immutable storage have begun to address DORA requirements for risk ownership and critical service mapping but lack testing and cross-functional readiness.
Level 3 – Defined	*Art. 9–11, 18–19*	Integration with SIEM/XDR and clean copy verification aligns with DORA's obligations for detection, response playbooks, and initial incident reporting structure.
Level 4 – Advanced	*Art. 12, 20–24*	Real-time validation and R-RPO metrics fulfill DORA's demands for ICT resilience testing, response tracking, and audit support across regulated environments.
Level 5 – Optimized	*Art. 25–44*	Automated recovery, Zero Trust alignment, and telemetry integration map to DORA's most advanced requirements: threat-led penetration testing, third-party oversight, and continuous operational resilience assurance.

About Elastio

Elastio is the leading provider of provable recovery and the control point for cyber resiliency. By continuously validating the data integrity of backups, detecting ransomware, and ensuring day-zero detection, Elastio eliminates the risk of encrypted data blocking recovery. Trusted by AWS, Deloitte, IBM, NetApp, Azure, and more. www.elastio.com

Sales: 833-435-2784 | sales@elastio.com
Sales Office: 120 Causeway Street Boston, MA 02114
Corporate Headquarters: 11921 Freedom Drive, Two Fountain Square, Suite 550 Reston, VA 20190