# Blog Post 7: Operational Resilience – Maintenance, Auditing, and Recovery

Keeping the System Alive A digital twin for disaster management must be resilient itself. We have established robust operational procedures to ensure availability, traceability, and recovery.

The "Scenario as a Workspace" Concept To manage the complexity of thousands of simulations, PANTHEON uses a Workspace model. Every executed scenario (e.g., `scenario_2025_ath_eq001`) creates a unique workspace ID that tags all related inputs, outputs, logs, and messages. This allows us to snapshot, backup, and restore a specific disaster simulation as a single coherent unit.

No Data Loss (NDL) Policy We implement a strict backup strategy to prevent data loss:

- Daily: Incremental backups of changed files and database transactions (WAL logs).
- Weekly/Monthly: Full snapshots of all storage systems.
- Verification: Backups are cryptographically hashed and regularly tested in staging environments.

Auditing & Compliance Every interaction with the repository is logged to an immutable audit trail.

- What we log: User logins, API data exports, simulation triggers, and security alerts.
- Why: To support post-incident forensics ("Who authorized this route?") and regulatory compliance.

Monitoring Stack We use Prometheus and Kibana to visualize system health in real-time. DevOps teams monitor technical metrics (CPU, Kafka lag, Disk I/O), while business dashboards track scenario usage and data throughput, ensuring PANTHEON is always ready for the next emergency.