

Day-Zero Recovery Tracker

Organize the first week of recovery while responding immediately to urgent harm.

Use the days as a sequence, not a waiting period

1. Day 1 - Contain: name an owner, pause nonessential changes where appropriate, assess active harm, and set a communication channel. Preserve evidence where feasible without delaying necessary containment. Involve security and other responsible specialists as needed.
2. Day 2 - Investigate: examine access controls, important data flows, backup recovery, and monitoring. Start with the highest-consequence risks; these are starting points, not the only surfaces to inspect.
3. Day 3 - Inventory: identify AI-generated, human-written, and unknown code. Ask whether the team can modify it, whether tests cover failures, and whether malicious input can reach an unintended system.
4. Day 4 - Decide: choose stabilization, constrained operation, rebuilding, or retirement for each affected subsystem. Check whether a proposed wrapper actually controls the hazard; it is not an automatic safe default.
5. Day 5 - Communicate: state verified findings, uncertainty, business impact, actions, owners, and the next update. Make required notifications on the applicable timetable.

Interpret findings and act

1. A "no" to maintainability or failure testing identifies a gap. A "yes" to dangerous access identifies a different risk. Do not wait for all three answers to be concerning.
2. Avoid a broad rewrite before understanding the system. Make urgent repairs when the risk warrants them, using verified facts, appropriate review, and a recovery plan.
3. Keep a system map, prioritized findings, decision log, and communication record. Review progress daily.

Immediate risk: _____. **Containment / repair owner:** _____. **Next update:** _____.