

FIXED-SCOPE ASSESSMENT

AI Crisis Readiness Review

An independent, vendor-agnostic assessment of whether your organisation can contain, explain and recover from an AI crisis, with a plan built for your systems.

10 business days	Up to 3 critical AI systems	7 deliverables	US\$9,500 fixed fee
----------------------------	---------------------------------------	--------------------------	-------------------------------

Why this, why now

AI systems now act on your behalf: they move money, change records, talk to customers and run processes. When one goes wrong, the questions are new. What could it do, under whose authority, can we contain it without stopping the business, can we rebuild what it did, and which regulator clock just started? Most organisations find out they have no answers in the middle of the incident. This review finds out first, and gives you a plan that fits your systems.

What the review covers

- Review your priority AI systems (up to three) and your existing incident, crisis and continuity plans.
- Identify crisis owners and decision rights: who contains, who undoes, who notifies, who approves a restart.
- Define the containment options each system supports, from pausing actions to switching to manual.
- Customise the first-hour, first-day and restart procedures for your organisation.
- Map the notification triggers that may apply (for example EU AI Act, GDPR, NIS2, DORA, SEC) and what starts each clock.
- Identify your five most dangerous readiness gaps.
- Deliver a prioritised 30-day action plan and an executive readout.

What you receive

Deliverable	What it is
1. Readiness findings	For each AI system: what it can see, decide and do, under whose authority, and how ready you are to contain, reconstruct and reverse it
2. Decision-rights matrix	Named crisis owners and who decides what, ready to drop into your incident plan
3. Containment map	The containment options each system supports today, and the ones it should
4. Your procedures	Customised first-hour, first-day and restart procedures
5. Notification trigger map	Regimes that may apply and what starts each clock, as input for your counsel
6. Five most dangerous gaps + 30-day plan	Prioritised actions with owners, effort and the risk each one closes
7. Executive readout	60 minutes with your leadership team: findings, decisions needed, next steps

How it runs: 10 business days

When	What happens
Day 1	Kick-off with your sponsor. Confirm the three systems. Document request.
Days 2 to 5	Interviews (up to six people, about an hour each) and walkthroughs of each AI system
Days 6 to 8	Analysis, containment map, procedures and the 30-day plan
Day 9	Draft deliverables reviewed with your sponsor
Day 10	Executive readout and final deliverables

What we need from you

- A named executive sponsor and a day-to-day contact.
- Time with up to six people, for example the CISO, AI or platform lead, business owners, legal or privacy, and communications.
- Existing incident response, crisis and business continuity plans, and what you know about the three systems: vendors, models, integrations, data and permissions.
- Responses to requests within two business days, so the ten-day timeline holds.

Not included

- Technical testing, penetration testing or red teaming of the AI systems.
- Legal advice. The notification trigger map is input for your counsel, who confirms your obligations.
- Implementing the controls or changes in the action plan.
- More than three AI systems (additional systems can be quoted), and travel (the review runs remotely by default).

Commercial terms

Fixed fee of US\$9,500 plus applicable taxes. 50% to book, 50% at the executive readout. The review starts within two weeks of booking, subject to availability. Deliverables are yours to use internally. The review is an assessment and advisory service, not an audit, certification or legal opinion, and you remain responsible for your own decisions and compliance.

After the review

- **Rehearse it:** a facilitated tabletop exercise with your leadership team, using your new procedures.
- **Close the gaps:** help implementing the 30-day plan, built on the open AI Control Architecture.

Book a 20-minute call: hello@keystoneexecutive.ai. The method is built on the AI Control Architecture, the open, vendor-agnostic framework Ankush created, and the free AI Crisis Preparedness Handbook (aicontrolarchitecture.org/ai-crisis-handbook).