IDΔAC™ · RESOURCE LIBRARY

Exposure Diagnostic Overview

A public overview of the 14-day Exposure Diagnostic, including scope, process, outputs, and typical use cases.

Public resource · Service overview · Version 1.0

IDΔAC™ Exposure Diagnostic is a bounded, evidence-first engagement for organisations that need to understand whether one AI-enabled decision route can be reconstructed and defended under scrutiny.

It is not a technical model audit, legal opinion, certification, conformity assessment, or enterprise transformation programme. Its function is narrower: to examine one representative route and determine where authority, evidence, intervention, escalation, and final organisational commitment may become exposed.

1. What the Exposure Diagnostic Is

The Exposure Diagnostic is a 14-day asynchronous diagnostic focused on one bounded decision route or representative decision pattern. It examines how a decision moves from technical influence to operational effect, and whether that route remains attributable, reconstructible, and defensible.

The diagnostic starts from a practical institutional question:

Can the organisation prove who committed the AI-enabled decision, with what evidence, under what authority, and through what route?

The answer is not derived from policy statements alone. A policy may assign responsibility, a workflow may show activity, and a reviewer may have clicked approve. Those facts matter, but they do not automatically prove that authority, intervention capacity, escalation, and final commitment remained clear before the outcome took effect.

The diagnostic therefore reconstructs the actual route, separates evidenced facts from assumptions and unknowns, and identifies the seams where organisational defensibility may weaken under board, audit, legal, regulatory, or client scrutiny.

Engagement element	Public baseline
Primary focus	One bounded AI-enabled decision route or representative pattern.
Delivery model	14 days · asynchronous · evidence-first.
Access posture	No full-system access required. The diagnostic uses enough attributable evidence to assess defensibility within scope.
Commercial range	€5,000-€7,500, depending on bounded scope and evidence readiness.
Primary next step	Request a Scope Review.

The diagnostic is useful when the organisation does not need a broad programme yet. It needs a disciplined answer on whether a specific decision route is ready for scrutiny.

2. Scope: What Is Examined

The unit of analysis is not the whole organisation and not the entire AI system. The unit of analysis is a decision route: the path through which system outputs, human review, evidence, escalation, and organisational commitment combine to produce an operational effect.

A suitable route is usually narrow enough to reconstruct and material enough to matter. Examples include an approval path, restriction decision, exception process, prioritisation flow, risk triage, complaint outcome, customer action, internal review, or any process where AI, automation, analytics, or technical recommendations influence decision formation.

Dimension	Public question	What the diagnostic looks for
Route	Can the actual decision path be reconstructed from input to effect?	The real sequence of system influence, human action, and operational consequence.
Evidence	Is the record contemporaneous, attributable, and sufficient?	What existed at the time, who had access, and what gaps weaken reconstruction.
Authority	Who had legitimate authority proportionate to the consequence?	Whether formal ownership matches practical authority and consequence.
Intervention	Could someone pause, refuse, modify, override, or request evidence?	Whether human oversight was usable before effect, not merely declared.
Escalation	Was escalation visible, usable, timely, and reconstructible?	Whether exposure could move upward before irreversibility or material harm.
Commitment	Where did the organisation become finally committed?	The point where workflow activity became attributable organisational commitment.

These public dimensions orient the diagnostic without disclosing internal scoring, thresholds, calibration logic, or proprietary control rules.

The aim is not to prove fault. The aim is to determine whether the route is structurally defensible on the evidence available within the agreed scope.

3. The 14-Day Process

The diagnostic is asynchronous by design. It is not an open-ended workshop sequence and not a full-system investigation. The process is bounded so that the organisation can receive a useful exposure determination without committing to a broad governance redesign.

Stage	Public description
1. Scope lock	Define the decision route or representative pattern, the operational effect, the sponsor, the evidence boundary, and the sample logic.
2. Evidence intake	Review the minimum attributable evidence pack and classify gaps, unavailable items, and acceptable equivalents.
3. Route reconstruction	Reconstruct what actually happened from system influence to operational effect.
4. Control-reality testing	Test whether evidence access, alternatives, intervention rights, timing, and escalation remained usable in practice.
5. Exposure determination	Separate evidenced facts, inferences, assumptions, and unknowns; determine whether attributable control is demonstrated.
6. Report and debrief	Deliver the executive diagnosis, route view, material findings, and a 30-day stabilisation framework.

4. Evidence Posture

The diagnostic does not require unrestricted access to all systems. It requires enough attributable evidence to test whether the selected route is reconstructible and defensible. Evidence may include governance records, workflow data, review notes, approval records, override or escalation material, sample decision records, incident or appeal material, and vendor or system documentation where relevant.

Missing evidence is not treated as automatic proof of misconduct or absence of judgement. It is treated as a fact about demonstrability. The diagnostic records what is evidenced, partially evidenced, withheld, unavailable, not retained, not verified, out of scope, or unknown.

5. What Leadership Receives

The output is designed for leadership, risk, legal, audit, AI governance, and operational owners who need a clear bounded answer before deciding whether deeper work is justified.

Executive diagnostic report

A bounded conclusion on whether the selected route is structurally defensible under scrutiny.

Decision-route reconstruction

A clear view of where AI output entered, who could act, and where operational commitment occurred.

Evidence sufficiency view

A classification of what is demonstrated, partially evidenced, unresolved, withheld, unavailable, or out of scope.

Material exposure findings

The seams that weaken attribution, authority, intervention, escalation, or reconstructibility.

30-day stabilisation priorities

Named actions tied to exposed seams, owners, and evidence or control outcomes.

The report does not pretend to solve every governance problem. Its value is focus: it turns a broad accountability concern into a bounded structural diagnosis of one route.

6. Typical Use Cases

- A high-impact AI-enabled route exists, but post-incident defensibility is uncertain.
- Legal or compliance teams need to know whether evidence, authority, explanation, or escalation can survive challenge.
- Internal audit can see designed controls, but the actual route and commitment act remain difficult to reconstruct.
- AI governance teams have declared human oversight, but live authority and intervention capacity are unclear.
- Operations leaders need to know whether a narrow structural fix is enough before funding broader redesign.

7. What This Is Not

The Exposure Diagnostic is intentionally bounded. Its credibility depends on not pretending to be a broader service than it is.

- Not a technical model audit.
- Not source-code review, model validation, cybersecurity testing, or data-quality assessment.
- Not legal advice or a legal opinion.
- Not a certification, conformity assessment, or public guarantee of compliance.
- Not an enterprise-wide AI governance redesign.
- Not a full-system investigation or transformation programme.

8. When to Request a Scope Review

A Scope Review is the correct next step when an organisation can identify one decision environment that matters and may be difficult to reconstruct or defend. The review determines whether the route is sufficiently bounded, material, and evidence-ready for a 14-day Exposure Diagnostic.

Do not submit confidential case files, personal data, or sensitive evidence through a public form. Evidence should be requested only after scope lock and information-handling terms are agreed.

Request a Scope Review	Describe the decision environment, why it matters now, the operational consequence, and the evidence currently available. IDΔAC™ will determine whether the Exposure Diagnostic is the right bounded engagement and what should be in scope.

IDΔAC™ Exposure Diagnostic helps organisations move from a vague concern - "AI was involved" - to a bounded answer: whether a specific decision route can be reconstructed, attributed, and defended.

To request information or assess whether a diagnostic fits your organisation: www.iddac.eu · contact@iddac.eu