V1.1

The REET Tests: Integrity & Closure

The Eight Structural Tests that Close Loopholes and Secure Remedy

Introduction

This pack is built around REET - Refusal, Escalation, Exit, and Traceability, each one of the basic four rights of system accountability.

If a system cannot guarantee them it fails.

The problem is simple. On the supply side, companies and governments design systems and say they are safe and fair. On the demand side, people, regulators and clients need proof that these claims are real. Too often there is a gap between what is promised and what actually happens.

That gap is where harm occurs.

This pack is made to close that gap. It is not about collecting opinions or impressions. It is about running clear tests that show whether safeguards really work.

Each test demands evidence and if the evidence proves the safeguard the system passes. If the evidence is missing or shows failure then the system fails.

The aim is straightforward: to give people a tool that turns claims into proof and proof into accountability.

Integrity & Closure

This volume closes the gaps that operators exploit. It tests whether safeguards act in time, whether consent is real, whether metrics measure resolution instead of performance theatre, whether responsibility follows the chain, whether jurisdictional shifts block enforcement, and whether harm is recognised in its full spectrum. Integrity means no loopholes, no delays, and no narrowing of remedy. Closure means that when harm occurs, there is nowhere for accountability to escape.

Loopholes multiply when several AI tools interact. Time, consent, metrics, liability, jurisdiction and harm must be tested across the whole system not piece by piece.

How to Use This Pack

Overview

This pack is not a simple checklist where you tick yes or no. It is a structured method for checking whether system safeguards actually work in practice. The aim is to look beyond what the system claims and to focus on the evidence that proves or disproves those claims. Every test is designed to show whether protections hold under real conditions.

Sequence

Each section follows the same fixed sequence so tests are consistent and comparable:

Covers - the safeguard being tested.
Why - the common failure or trick to look for.
Standard - the requirement the system must meet.
Evidence / Evidence location - the points where proof must be produced and recorded.

When You Work Through a Test

The steps are always the same:

1. Read the Standard carefully - know exactly what the system is expected to do.
2. Compare it to the system in front of you - check the requirement against the real implementation.
3. Ask for or locate the evidence - demand proof that the safeguard is working.
4. Record the result - mark whether the evidence meets the standard, fails it, or is missing.
5. Note simulated compliance - highlight where the system pretends to comply (for example, through menus or messages) but does not actually deliver.

Important Principles

These principles apply to every test:

A claim without evidence is a fail.
Partial or broken evidence is not enough.
Failures must be logged and reported, not smoothed over.
Passing a test means the safeguard has been proven in practice, not simply promised in words or policy.

Aim

The purpose of this pack is not to collect opinions, impressions, or frustrations. Its purpose is to create a clear and traceable record of what holds and what fails. If used consistently, the pack makes accountability visible and provides solid evidence for demanding structural change.

Integrity & Closure

This stage builds on the baseline by ensuring users are not trapped inside powerless processes. Escalation must lead to people with real authority, not loops back into automation. Access to safeguards must be equal across languages, geographies, and payment tiers. Evidence must be durable, verifiable, and admissible in disputes. Together, these measures create systems where users can challenge outcomes, demand fairness, and rely on records that stand up to scrutiny.

Time Suppression

Covers: A safeguard delayed is a safeguard denied. If complaint systems, appeals, or reviews take longer than the harm itself, rights exist only on paper. Delay must not be used as a tactic to let deadlines expire, evidence vanish or harm become irreversible. Safeguards must act fast enough to prevent lasting damage.

Question: Are refusal, escalation, and review completed within enforceable deadlines with auditable timestamps?

Why: Delays function as structural denials: remedies that arrive too late are effectively null, leaving users without timely relief or accountability.

What proportion of cases breached deadlines last quarter, and what automatic remedy was triggered?

Evidence

Evidence location

What interim measures halt ongoing harm while disputes are unresolved?

Evidence

Evidence location

How are regulators informed of systematic deadline breaches?

Evidence

Evidence location

Simulation Logic

Covers: A system must not pretend protections exist when they do not. Policies, dashboards, or safeguards that look good in design but do nothing in practice mislead users into false trust. If a right exists only on paper or in a menu, but never changes outcomes, it is a breach. Safeguards must be real, functional, and enforceable.

Question: Do all stated safeguards operate exactly as described when tested in live conditions?

Why: Many systems display confirmations such as 'your preference has been recorded' while leaving the underlying decision pathway unchanged, creating the appearance of compliance without impact.

Show one case where a safeguard directly changed an outcome — what counterfactual proves causality?

Evidence

Evidence location

Which safeguards are disabled in production but still advertised?

Evidence

Evidence location

How do you prove safeguards hold under adversarial or worst-case conditions?

Evidence

Evidence location

Simulated Consent

Covers: Consent must be genuine. If users are told they have a choice but refusal means losing essential services, being downgraded, or facing hidden costs, then the “choice” is a lie. Clicking “accept” under duress is not consent. Real consent means saying yes or no without fear of punishment.

Question: Can a user refuse consent and still access an equal-value, non-AI pathway?

Why: Consent is frequently simulated by tying acceptance to essential service, degrading functionality for non-consent, or burying consent under manipulative interface design.

How do you prove consent was informed, revocable, and specific?

Evidence

Evidence location

What is the process for revoking consent mid-session, and what happens to service continuity?

Evidence

Evidence location

What alternative pathways exist for users who decline consent, and how do they compare in quality?

Evidence

Evidence location

Metric Gaming

Covers: Metrics must measure real outcomes, not theatre. If an organisation tracks numbers that hide harm (like “tickets closed” instead of “problems solved”), the data is meaningless. When numbers are chosen to make systems look good while ignoring harm, they block accountability. Metrics must reveal reality, not disguise it.

Question: Do performance measures track verified harm resolution rather than proxy indicators?

Why: Firms often publish performance indicators that look favourable while concealing negative externalities, shifting the basis of evaluation from real-world harms to curated numbers.

Which metrics drive executive bonuses, and how do they correlate with verified harm resolution?

Evidence

Evidence location

Provide one random week of complaint narratives alongside dashboard KPIs; explain discrepancies.

Evidence

Evidence location

Which metrics were dropped or redefined last year, and what harm patterns triggered those changes?

Evidence

Evidence location

Cross-Accountability Gap

Covers: Accountability must follow harm across the chain. If every actor points elsewhere: the platform blames the vendor, the vendor blames the regulator, the regulator blames the law, harm becomes visible but no one takes responsibility. A system is in breach if it leaves users caught in this loop. Responsibility must remain clear, shared, and enforceable.

Question: Can every actor in the chain be named and held contractually responsible for repairing harm?

Why: Without a named liable actor, enforcement collapses into vagueness: no person or entity can be held to account for breaches.

For a typical harm, who is the single accountable owner across vendors/operators?

Evidence

Evidence location

What escalation path exists when two vendors dispute liability?

Evidence

Evidence location

Jurisdiction Displacement

Covers: A system must not move decisions or data into spaces where oversight cannot reach. Shifting storage overseas or routing appeals into jurisdictions without real enforcement, strips rights of their power. Protection on paper must equal protection in practice, wherever the system operates.

Question: Can local authorities compel the system to halt, change, or reverse harmful actions?

Why: Firms routinely shield themselves from domestic enforcement by shifting venue, restructuring liability, or exploiting corporate layering.

Where are data and decisions located for EU users, and what controls can EU regulators exercise?

Evidence

Evidence location

How do you prevent relocation of processing to weaker jurisdictions without explicit approval?

Evidence

Evidence location

What proportion of enforcement actions have been delayed by jurisdictional conflicts?

Evidence

Evidence location

Enforcement Bypass

Covers: A system must not be designed to step around the spirit of rules while obeying the letter. If protections exist but are neutralised by loopholes, technicalities, or proxy arrangements, enforcement has been bypassed. True compliance means obeying both the rules and their intent.

Question: Are there no architectural or contractual exemptions that remove applicable legal duties?

Why: By engineering loopholes into terms of service, interface design, or technical architecture, firms create the appearance of compliance while bypassing substantive enforcement.

Which carve-outs, exemptions, or pilot labels apply to this product, and for how long?

Evidence

Evidence location

How are bypassed obligations reinstated once the exemption ends?

Evidence

Evidence location

Harm Scope Narrowing

Covers: A system must recognise the full range of harm it causes. If it defines harm so narrowly that financial loss counts but emotional damage, dignity, or exclusion do not, users are denied real remedy. Harm must be defined as people experience it, not as systems prefer to record it.

Question: Does the harm definition include emotional, reputational, and cumulative damage with a route to redress?

Why: By restricting harm to quantifiable monetary outcomes, firms exclude structural injuries such as exclusion, manipulation, denial of recourse, or erosion of dignity, leaving non-financial harms unremedied.

When defining harm, which categories did you exclude, and why?

Evidence

Evidence location

Who decides which harms are material enough to trigger remedy?

Evidence

Evidence location

Have you ever compensated for a harm outside your official definition?

Evidence

Evidence location

How do you ensure collective or cumulative harms are recognised, not dismissed as diffuse?

Evidence

Evidence location

Contact

Russell Parrott
Email: parrott.russell@gmail.com

Copyright and Usage

Acknowledgement

This pack is based on the REET framework (Refusal, Escalation, Exit, Traceability) and the 15 Structural Tests developed by Russell Parrott. It is the reference version.

Support & Sustainability

The REET Tests are a public standard. They are free to use, copy, and distribute for oversight, audit, and regulatory purposes, and they will remain free. Support is voluntary: individuals can contribute if they value the work, and institutions may underwrite it as a public good. Contributions do not buy rights, licenses, or endorsements. They only ensure that the tests remain open, independent, and available to all.