V1.1

The REET Tests: Sovereignty & Evidence

The Four Structural Tests of Refusal, Exit, Memory and Traceability

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.

Sovereignty & Evidence

This volume contains the four baseline rights: the right to refuse, the right to exit, the right to memory, and the right to traceability. Without them, no system can claim accountability. These rights define user sovereignty: the ability to say no, to leave without penalty, to ensure harm is not erased, and to see how decisions were made. If any one is absent, all other safeguards collapse into theatre. This publication provides the minimum test of whether power rests with the user or with the system.

Even when safeguards exist in one tool, they can be undone by another in the chain. Refusal, exit, memory and traceability must hold across every component not just in isolation.

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.

Sovereignty & Evidence

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.

Refusal Prevention

Covers: A system must allow users to say no without penalty. Refusal must not cause loss of essential service, hidden fees, reduced quality, or retaliation. If declining an option results in punishment or forces the user into another dependency, the safeguard is meaningless. Refusal must remain a safe, equal, and respected choice.

Question: Can any user stop or redirect a decision at any point without penalty or loss of service?

Why: Refusal is frequently neutralised not only through explicit penalties but also through hidden costs, degraded service, covert re-enablement, or framing that ignores refusal altogether.

Which functions remain available if a user refuses non-essential processing?

Evidence

Evidence location

How is refusal recorded and protected from being silently overridden later?

Evidence

Evidence location

What independent process verifies refusals are honoured across downstream systems?

Evidence

Evidence location

Exit Obstruction

Covers: A system must allow users to leave without excessive cost, harm, or loss. Locking people in through data deletion, high switching fees, or withdrawal of unrelated services is not a free exit. If leaving exposes the user to new risks, the option is not real. Exit must be safe, practical, and non-punitive.

Question: Can any user leave the AI pathway and continue receiving the same core service without delay, cost, or requalification?

Why: Exit is often obstructed not just by fees or delays, but by lock-in architectures, circular deletion loops, withdrawal penalties, or the tying of exit to loss of unrelated essential functions.

What is the maximum number of steps required for a user to fully exit, and who approved that threshold?

Evidence

Evidence location

How do you prove that user data has been fully deleted after exit?

Evidence

Evidence location

How is continuity of unrelated services guaranteed once exit occurs?

Evidence

Evidence location

Evidence Erasure

Covers: A system must retain evidence of its past actions long enough to expose repeated harm. If records are deleted, fragmented, or hidden, patterns of abuse appear as isolated mistakes. Users and regulators must be able to see history, not just the present moment. Without memory, harm repeats without proof.

Question: Are harm events logged and retained long enough to detect and act on repeat or systemic failure?

Why: Vendors often fragment memory into isolated sessions, purge logs after arbitrary periods, or design resets that prevent reconstruction of responsibility.

What is the retention schedule for harm logs, and who can alter it?

Evidence

Evidence location

Are deletion events themselves logged immutably with actor, timestamp, and legal basis?

Evidence

Evidence location

Traceability Void

Covers: A system must keep records of how and why decisions are made. If no audit trail exists, or the process is too complex to reconstruct, accountability disappears. Users must be able to see what influenced a decision, regulators must be able to verify it, and operators must be answerable for it. Without traceability, trust collapses.

Question: Can the exact model, version, and decision chain be identified for every output?

Why: Firms frequently substitute dashboards, summaries, or partial disclosures that simulate traceability but conceal the actual technical lineage required for accountability.

If a regulator requests the full decision chain, can you reconstruct every step within 30 days?

Evidence

Evidence location

How do you preserve excluded or filtered data so its removal is auditable?

Evidence

Evidence location

Who signs off when traceability gaps are deemed “non-material”?

Evidence

Evidence location

What fallback reconstruction process is in place when logs are missing?

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.