V1.1

# The REET Tests: Authority & Fairness

*The Three Structural Tests of Escalation, Equal Access, and Durable Evidence*

# 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.

## Authority & Fairness

This volume establishes whether users can challenge decisions and be treated equally. Escalation must reach people with real authority, not dead-end loops. Safeguards must apply across languages, geographies, and payment tiers without discrimination. Records must be durable and admissible as evidence, not cosmetic logs that evaporate under scrutiny. These tests ensure that users are not trapped inside powerless processes and that protections hold equally for all.

Escalation and equal access often collapse where multiple vendors are involved. If authority or evidence stops at the product boundary fairness is lost.

# 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.

# Authority & Fairness

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.

# Escalation Suppression

Covers: A system must provide real routes of appeal when decisions are contested. An appeal that loops back to the same authority, or to staff without power to reverse outcomes, is not valid. If escalation is denied, delayed until meaningless, or designed to exhaust the user into giving up, the system breaches trust. Escalation must be independent, timely, and empowered to correct harm.

Question: Can any user trigger escalation to a human with authority, with that escalation logged to resolution?

Why: Escalation pathways are often blocked, simulated, or staffed by individuals without authority, leaving users trapped in cycles of repetition without resolution.

## What documented path guarantees escalation leaves automation for accountable human oversight?

Evidence

Evidence location

## Who has authority to reverse an automated decision, and how often has it happened?

Evidence

Evidence location

What SLA clocks start when escalation is triggered, and who owns them?

Evidence

Evidence location

# Access Gating

Covers: A system must ensure equal access to safeguards and protections. Making appeals, human review, or essential support available only to premium customers, certain languages, or those with specific IDs creates unfair barriers. Protection must not depend on wealth, geography, or privilege.

Question: Are safeguards and human alternatives available equally to all users, regardless of geography, payment tier, or identity verification?

Why: Safeguards are frequently limited to certain languages, jurisdictions, or high-paying users, creating systemic inequality and denying protections to those most at risk.

## Which safeguards vary by geography, language, or tier, and on what legal basis?

Evidence

Evidence location

## How do you guarantee parity of access (including accessibility support) across all user groups?

Evidence

Evidence location

# Evidence Nullification

Covers: A system must provide evidence that can stand up to scrutiny. Data that is incomplete, editable, unverifiable, or locked in inaccessible formats cannot be used to prove harm. If records exist but fail as proof, they serve the operator, not the user. Evidence must be durable, verifiable, and usable in disputes.

Question: Can harm records be exported and presented in a regulator- or court-admissible format?

Why: Evidence is frequently redacted, reformatted, or altered to obstruct regulators, making independent verification impossible.

## Can a user export their full case file and metadata in a tamper-evident bundle?

Evidence

Evidence location

## Which parts of the audit trail are write-once/append-only, and how is chain of custody proven?

Evidence

Evidence location

What immutable store ensures evidence cannot be selectively withheld?

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.