# Data Access: The Blueprint for Controlled Usability

How intelligent organizations give the right people, systems, and AI tools the data they need—without losing trust.

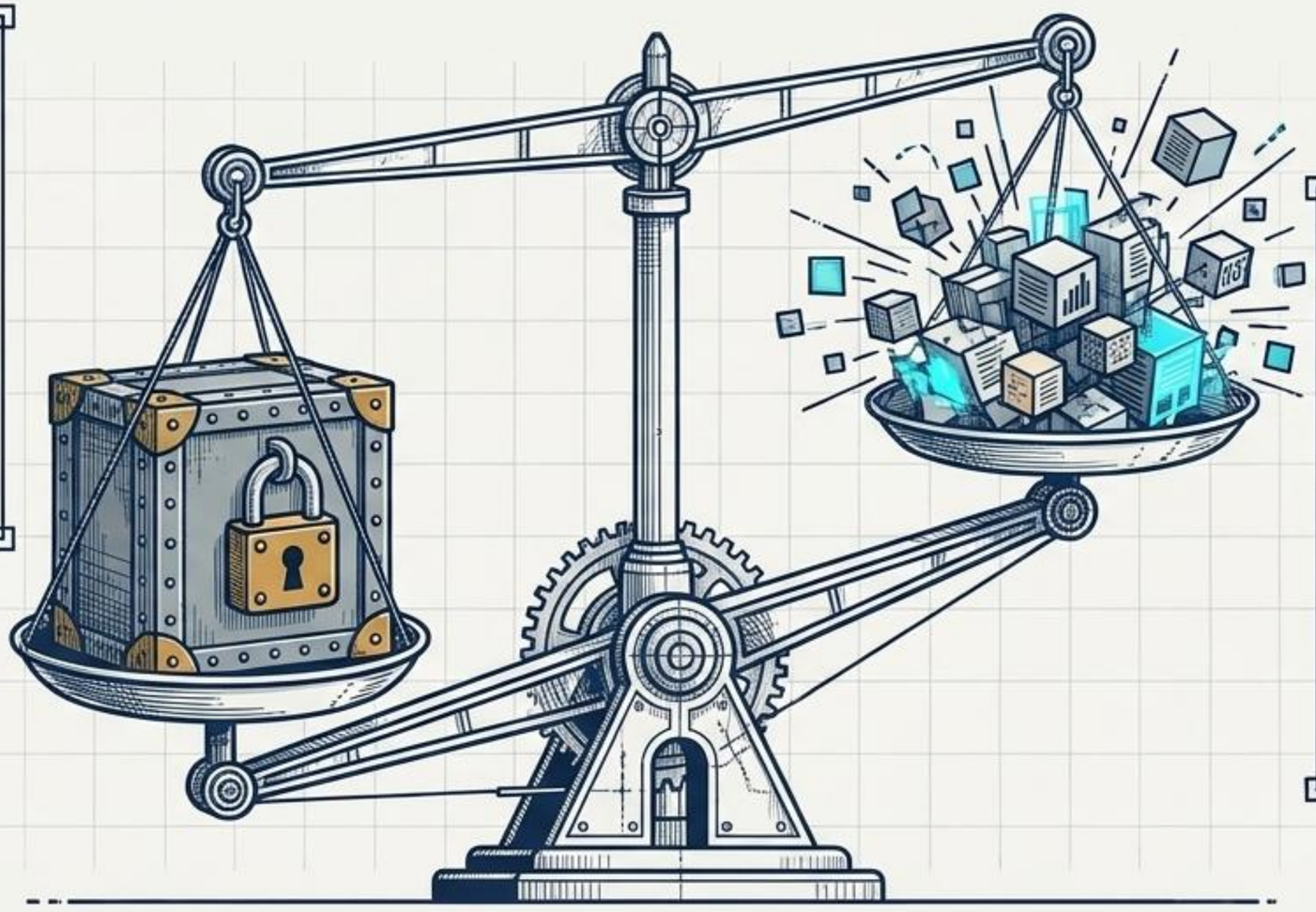
TIO Domain 2: Data | Capability 3: Access

# The Dual Threat of Modern Data

## The Lockdown Trap

**Too Hard to Get:** Locking data down kills value. Teams wait, duplicate work, create shadow spreadsheets, or make decisions from partial information.

AI initiatives starve.



## The Exposure Trap

**Moving Too Freely:** Opening all data up kills trust. Sensitive customer, financial, or regulated information flows blindly into unsafe public AI tools, vendor models, and unapproved dashboards.

**Organizations have two access problems at the exact same time. Standing still is not an option, but moving recklessly destroys trust.**

# The Core Philosophy of Data Access

Do not lock all data down.

Do not open all data up.

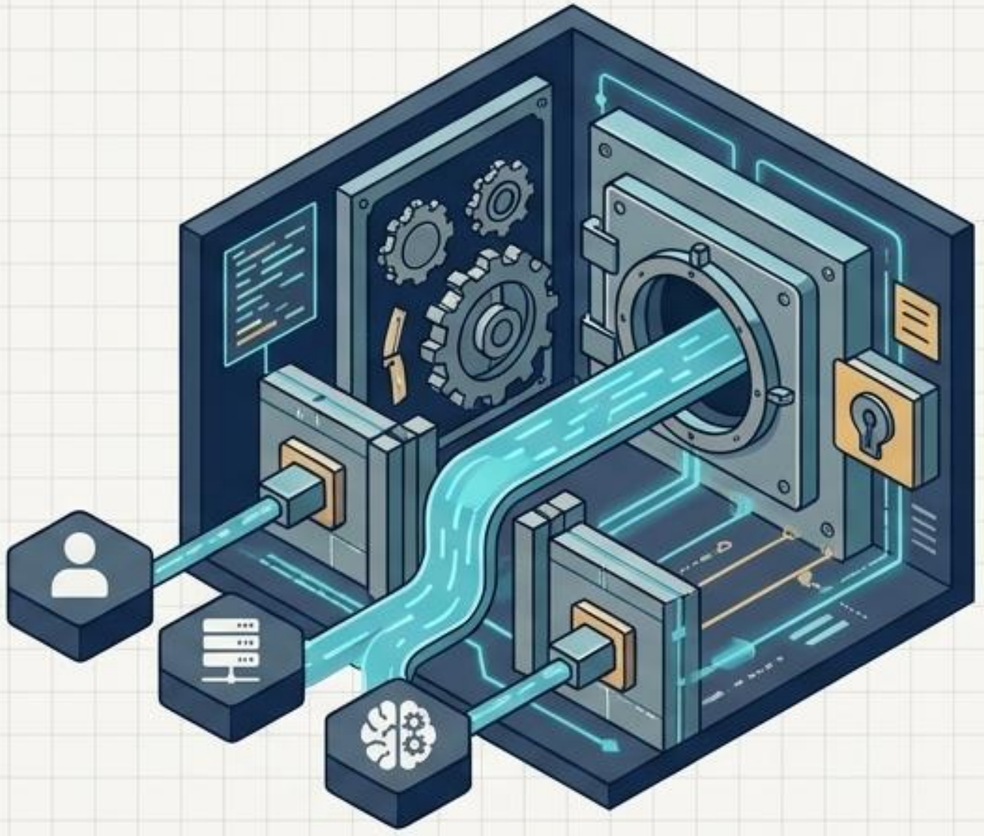
**Make safe use easy and unsafe use hard.**


Access should make useful work easier. It should not make every data request a committee decision.

# Redefining Access as “Controlled Usability”

## The TIO Definition

**Access is the organization’s ability to give the right** people, systems, reports, **automations,** and AI Use Cases appropriate access to the data they need, **while protecting sensitive information.**



## The Data Domain Story

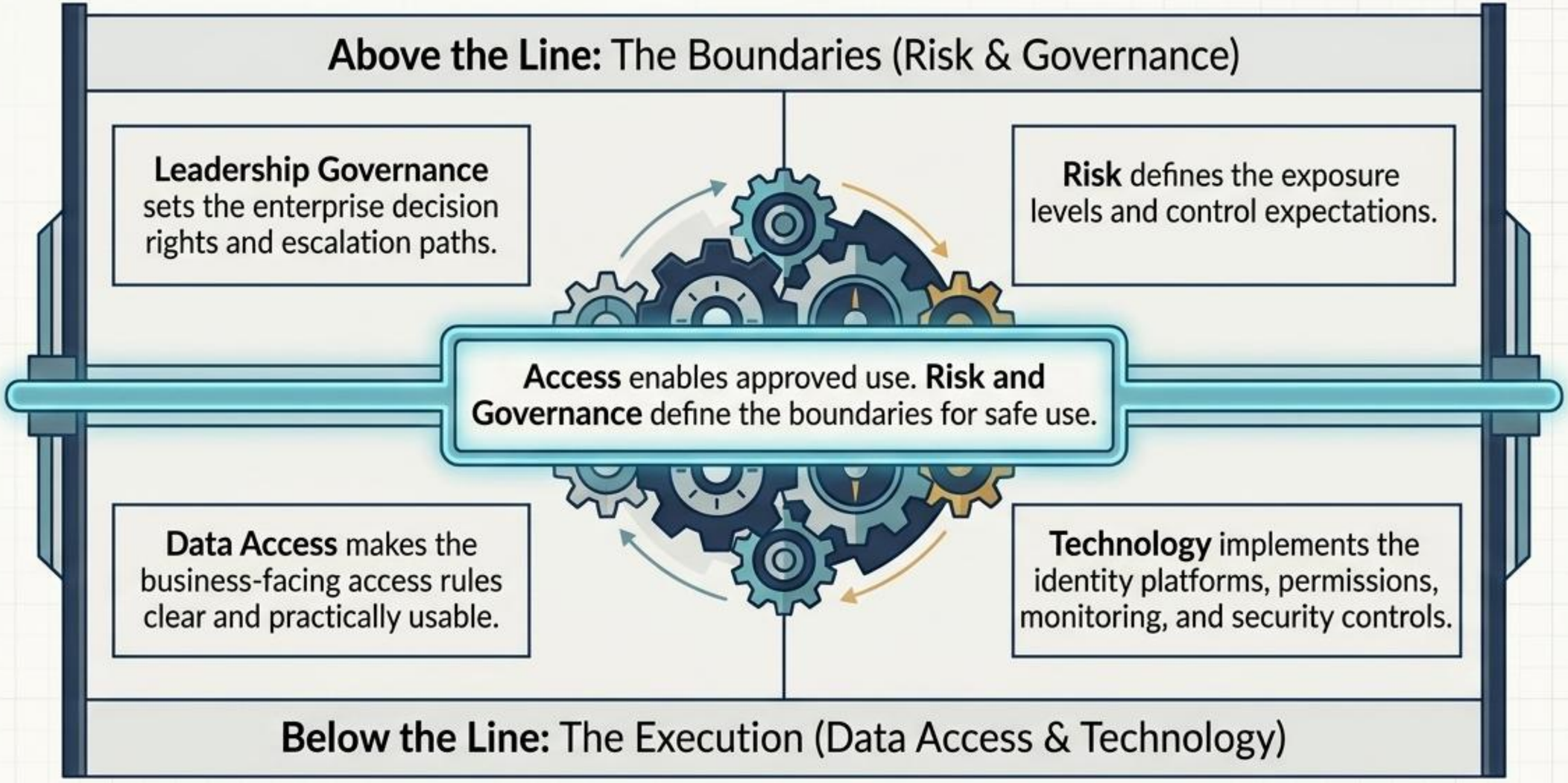
**Ownership** assigns → **Quality** proves → **Access** enables → **Flow** connects → **Insight** informs

Access is the third Data capability. Ownership names the accountable human, Quality proves the data is fit for purpose, and Access makes the data safely usable.

# Access is a Business Decision, Not an IT Ticket

| What Access Is NOT (The Old Mindset) | What Access IS (Controlled Usability) |
| --- | --- |
| Only a technical IT permissions issue. | A business capability connecting purpose, sensitivity, risk, and value. |
| A binary “padlock” (everyone gets everything, or no one gets anything). | A defined routing path for AI Use Cases, vendors, and automations. |
| A one-time permissions cleanup project. | A continuous rhythm of reviewing and adjusting permissions. |
| Only a privacy, legal, or security review. | Making access decisions visible enough to be audited and improved. |
| A spreadsheet of theoretical roles no one uses. | |

# The Boundary Line: Rules vs. Usability



# The Engine of Controlled Usability: 5 Core Behaviors


## Classify

Know what kind of data this is and how sensitive it is.

## Authorize

Decide who or what can use the data, for which purpose, and under which limits.

## Enable

Provide a safe, practical access path so useful work can (dashboards, APIs, approved AI environments).

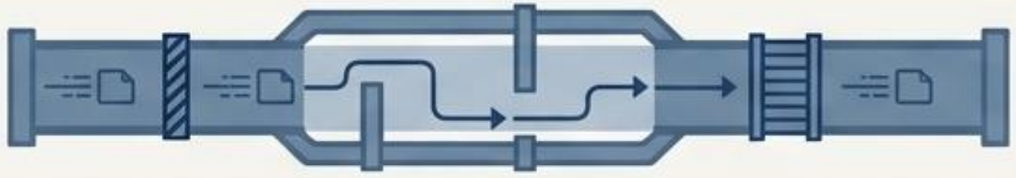
## Limit

Restrict, mask, segregate, or prohibit access when the exposure to public tools or vendors is too high.

## Review

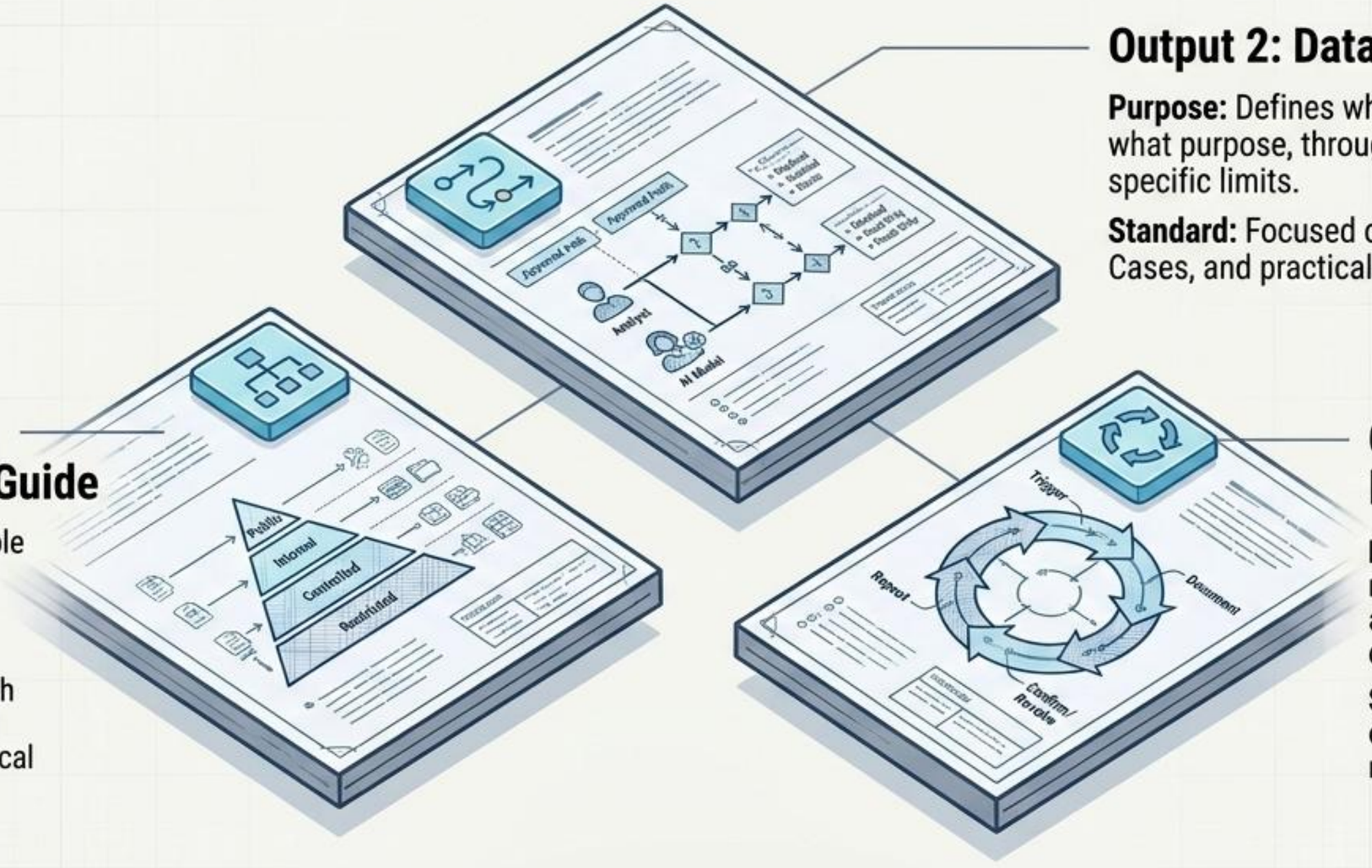
Recheck and clean up access continuously as roles, tools, projects, and use cases change.

# The Access Lanes: Routing Data by Sensitivity and Purpose

| 5-Tier Diagnostic Table | Title | Use | Posture |
|---|---|---|---|
|  | Lane 1: **Open** | Public or approved non-sensitive data. | Easy to use through approved tools. |
|  | Lane 2: **Internal** | Internal operating data with limited sensitivity. | Available to the right roles through approved systems. |
|  | Lane 3: **Controlled** | Customer, employee, financial, or operational data. | Requires specific purpose, data owner approval, and approved access path. |
|  | Lane 4: **Restricted** | Highly sensitive, regulated, legal, or commercially sensitive data. | Requires elevated review, strict limits, masking, and stronger controls. |
|  | Lane 5: **Prohibited** | Data that must never enter unapproved public AI tools, vendor exports, or shadow IT. | Blocked entirely unless formally reclassified or approved via strict exception. |

# The 3 Practical Outputs

More permissions forms do not equal safer access. Three outputs are enough to start.




## Output 2: Data Access Rules

**Purpose:** Defines who uses which data, for what purpose, through approved paths, with specific limits.

**Standard:** Focused on priority data, AI Use Cases, and practical business decisions.

## Output 1: Data Classification Guide

**Purpose:** Defines simple sensitivity levels and use restrictions for priority data.

**Standard:** Clear enough for managers to apply without legal or technical translation.

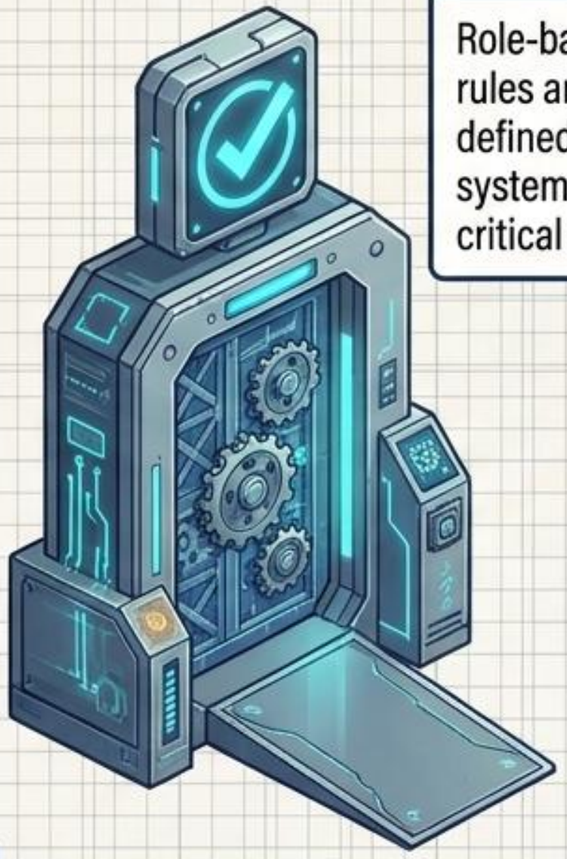
## Output 3: Access Review Process

**Purpose:** Confirms, removes, or narrows access as roles, vendors, or systems change.

**Standard:** Regular, simple, owner-led, and connected to real-world access changes.

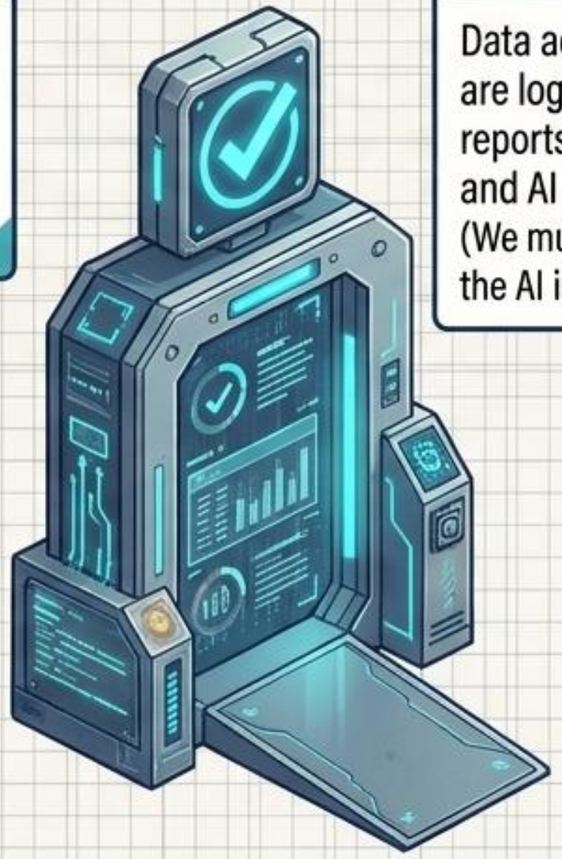
# Executive Evidence: Proving the Gateway Works

Score concrete artifacts and system logs, not aspiration.



### Gate 1: Defined Rules

Role-based access rules are actively defined for priority systems and critical data.



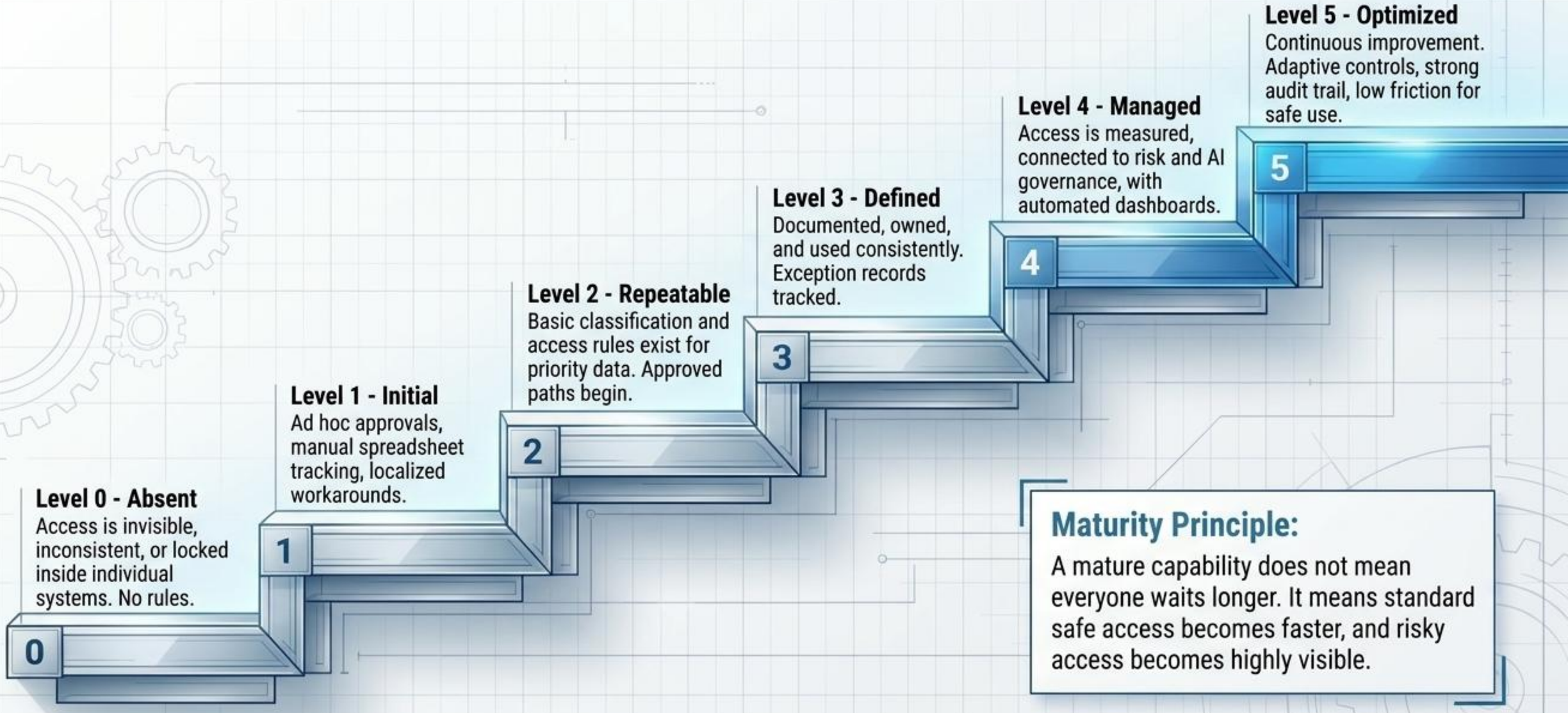
### Gate 2: Logged Use

Data access records are logged for priority reports, automations, and AI Use Cases. (We must know what the AI is looking at).

### Gate 3: Active Removal

Removed or changed access is documented when people, roles, vendors, or business needs change. (Access is not a lifetime appointment).

# The Maturity Scale: From Ad Hoc to Optimized

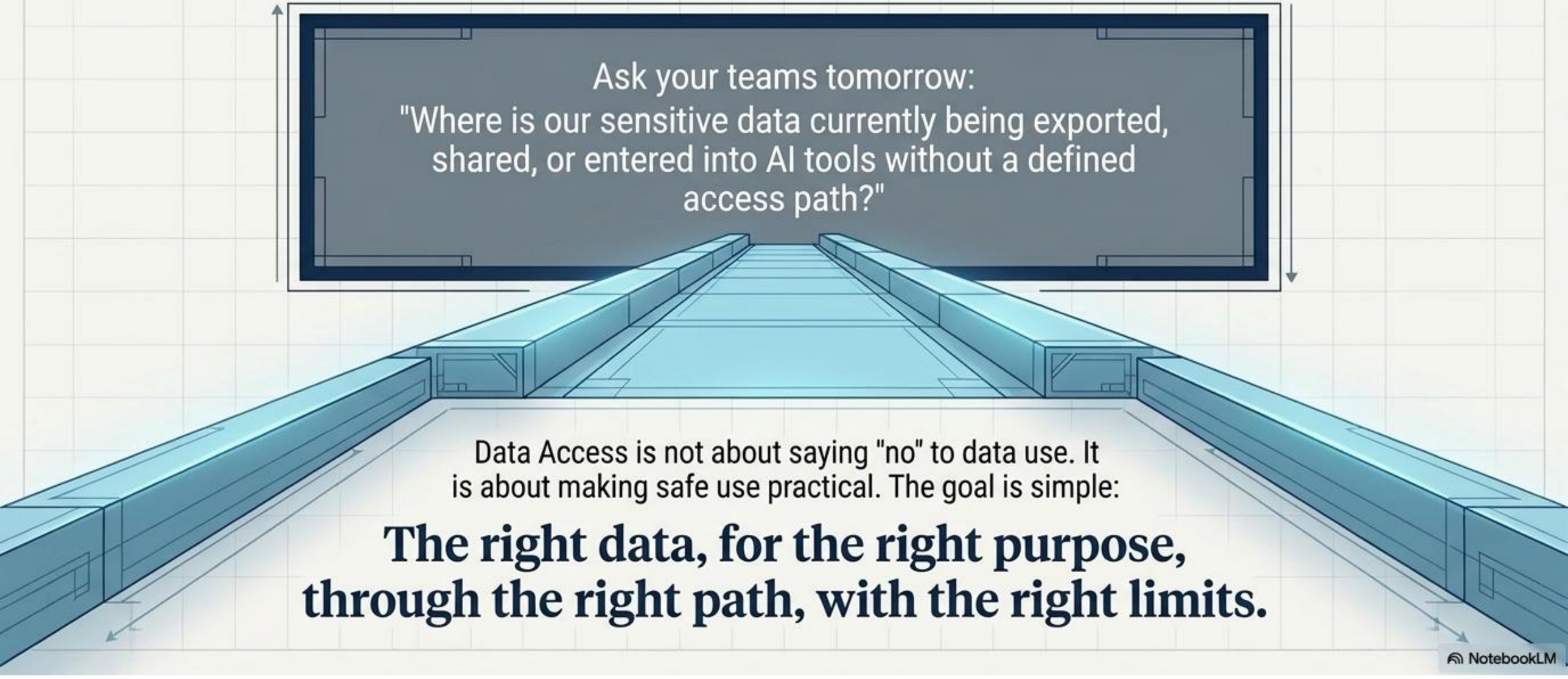



## Maturity Principle:

A mature capability does not mean everyone waits longer. It means standard safe access becomes faster, and risky access becomes highly visible.

# First Moves: Activating the Capability

# The Starting Conversation




Data Access is not about saying "no" to data use. It is about making safe use practical. The goal is simple:

**The right data, for the right purpose, through the right path, with the right limits.**