Capability Guide: Data Access

Data Must Be Usable and Protected.

Document Version 1.0 FINAL | TIO-KR-2026.08.0 | August 2026

Table of Contents

1. Executive Brief	5. Outputs, Evidence, and Measures
2. The Problem This Capability Solves	6. Maturity: 0 to 5
3. What this Capability Is	7. How to Build and Mature the Capability
4. How the Capability Works	8. TSLA Support and First Moves
Appendix A. Source Note	

How to use this guide

Read Sections 1 through 3 for the executive view. Use Sections 4 through 7 to build and mature the capability. Use Section 8 to decide what to do next Monday morning.

01 Executive Brief

Data Access is the organization's ability to let the right people, systems, reports, automations, and AI Use Cases use the right data safely, appropriately, and efficiently.

Access is the third Data capability because Ownership assigns accountability, Quality proves the data is fit for purpose, and Access makes the data safely usable.

Capability ID	D3: Data Access
Domain	Data
Plain-English test	Can the right people, systems, and AI Use Cases get the data they need without exposing data they should not use?
Core point of view	Do not lock all data down. Do not open all data up. Make safe use easy and unsafe use hard.
Three practical outputs	Data Classification Guide; Data Access Rules; Access Review Process
Primary owner	Business data owners, supported by Technology, Security, Privacy, Legal, Risk, and Governance as needed.
First move	Pick priority data, classify it simply, define who needs it and why, then create safe approved access paths.

The Data domain story

Ownership assigns. Quality proves. Access enables. Flow connects. Insight informs.

2026.08 ALIGNMENT | Access in the refreshed TIO system

Primary outcome contribution: Intelligence and Enterprise Autonomy

- Access is purpose-bound and actor-specific across people, personal agents, enterprise agents, models, tools, services, and devices.
- Rights to read, retrieve, infer, combine, remember, train, disclose, and act are distinct and revocable.
- Approved access paths should make useful work easier and unsafe use harder, including cross-border and provider processing.

Evidence at managed maturity: Access is defined, owned, applied consistently, measured in operation, reviewed through evidence, and improved without weakening trust, accountability, or Enterprise Autonomy.

First refresh move: Define who or what may read, infer, remember, train, disclose, and act on one priority information set.

02 The Problem This Capability Solves

Most organizations have two access problems at the same time.

- Some people cannot get the data they need, so they wait, duplicate work, create spreadsheets, or make decisions from partial information.
- Some people, tools, vendors, automations, or AI systems can reach data they should not use, so trust, privacy, security, compliance, and client confidence are exposed.

Data Access solves that tension. It helps the organization use data for value without turning every dashboard, export, integration, automation, or AI experiment into a trust problem.

When Data Access is weak

- People copy data into spreadsheets because the official path is too slow or unclear.
- Leaders receive partial information because teams cannot safely combine the data they need.
- Sensitive customer, employee, financial, operational, client, resident, or regulated data moves into unsafe tools.
- AI Use Cases stall because nobody knows whether a model, assistant, workflow, or vendor can use the data.
- Access is granted once and rarely reviewed when roles, vendors, projects, or use cases change.
- Technology is blamed for access decisions that are really business, privacy, risk, or governance decisions.
- Managers do not know which data is public, internal, confidential, restricted, or prohibited for AI use.

Simple rule

Access should make useful work easier and risky use harder. It should not make every data request a committee decision.

03 What this Capability Is

Data Access is controlled usability. It is the practical ability to let data be used for the right purpose through the right path, with the right limits.

Access is not only a technical permissions issue. It is a business capability because every important access decision connects purpose, data sensitivity, role, tool, risk, trust, and value.

What Data Access owns

- Classifying important data by sensitivity and intended use.
- Defining who can access what data and why.
- Setting approved access paths for people, systems, reports, automations, vendors, and AI Use Cases.
- Restricting sensitive data from unsafe tools, exports, vendors, or unauthorized use.
- Reviewing and removing access as roles, projects, contracts, or use cases change.
- Making access decisions visible enough that they can be audited, explained, and improved.

What Data Access does not own

- Giving everyone access to everything.
- Blocking data use because risk exists.
- A one-time permissions cleanup.
- Only an IT security task.
- Only a privacy or legal review.
- A spreadsheet of theoretical roles that no one uses.
- A data lake, warehouse, identity platform, or security tool by itself.

Five core behaviors

Behavior	What it means
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 happen.
Limit	Restrict, mask, segregate, or prohibit access when the exposure is too high.
Review	Recheck access as roles, tools, projects, vendors, and use cases change.

Boundary rule

Leadership Governance sets the decision rights and escalation path. Risk defines exposure and control expectations. Technology implements identity, permissions, platforms, monitoring, and security controls. Data Access makes the business-facing access rules clear and usable.

04 How the Capability Works

Data Access should start with a real purpose. The question is not simply, "Can this person or tool see the data?" The better question is, "What data is needed, for what purpose, through what approved path, with what limits?"

Simple operating model

1. Start with the purpose: report, dashboard, workflow, automation, AI Use Case, vendor service, regulatory need, or client service.
2. Identify the data: fields, records, sources, systems, documents, files, or data products involved.
3. Classify the data: public, internal, confidential, restricted, regulated, or prohibited for certain uses.
4. Confirm the requester and use: role, team, system, tool, vendor, model, workflow, and reason for access.
5. Route the decision: standard access, manager approval, data owner approval, privacy or security review, risk review, or governance escalation.
6. Enable safe access: approved tool, approved system path, role-based access, masking, aggregation, retention limit, export restriction, or human review.
7. Record and review: keep a simple record of sensitive access decisions, exceptions, and access reviews.

Access lanes

Lane	Typical use	Access posture
Open	Public or approved non-sensitive data.	Easy to use through approved tools.
Internal	Internal operating data with limited sensitivity.	Available to the right roles through approved systems.
Controlled	Customer, employee, financial, operational, or confidential data.	Requires purpose, owner approval, and approved access path.
Restricted	Highly sensitive, regulated, legal, security, or commercially sensitive data.	Requires elevated review, strict limits, and stronger controls.
Prohibited	Data that must not enter certain tools, vendors, exports, or AI systems.	Blocked unless formally reclassified or approved through exception.

Example

A mid-sized field services company wants managers to use an AI-enabled dashboard that combines client, service ticket, technician, work order, and invoice data. The dashboard can create value, but it raises access questions. Should every manager see all client data? Should supervisors see invoice margin? Should an AI tool receive raw invoice data? Can the vendor use the data to train its model?

The team classifies the data, creates access rules, configures role-based permissions, restricts raw data export, and approves use only through the enterprise environment. Managers get the insight they need. Sensitive data does not move into unsafe tools. Access enables value without weakening trust.

05 Outputs, Evidence, and Measures

Data Access should produce a small number of useful outputs. More permissions, more committees, and more forms do not equal safer access. Three outputs are enough to start and mature the capability.

Output	Purpose	Quality standard
Data Classification Guide	Defines simple sensitivity levels and use restrictions for priority data.	Clear enough for managers to understand and apply without legal or technical translation.
Data Access Rules	Defines who can use which data, for what purpose, through which approved paths, and with what limits.	Focused on priority data, current use cases, sensitive data, and practical decisions.
Access Review Process	Reviews, confirms, removes, or narrows access as roles, systems, vendors, projects, or AI Use Cases change.	Regular, simple, owner-led, and connected to real access changes.

Evidence that the capability exists

- Priority data is classified by sensitivity and use.
- Access rules exist for high-value and sensitive data.
- Approved access paths are documented for people, systems, reports, automations, and AI Use Cases.
- Restricted and prohibited uses are clear, especially for public AI tools and external vendors.
- Access review responsibilities are assigned.

Evidence that the capability is used

- Access requests are routed to the right owner or review path.
- Sensitive access decisions are recorded.
- Access is removed or narrowed when roles, vendors, projects, or use cases change.
- AI Use Cases are checked against data access rules before use.
- Exceptions are visible and reviewed.

Useful measures

Measure	What it tells leaders
Priority data classified	Whether important data has a clear sensitivity and use posture.
Sensitive access requests reviewed	Whether high-exposure access decisions are visible.
Access review completion	Whether access is being rechecked and cleaned up.
Unauthorized or unclear access findings	Where the organization has exposure or confusion.

Measure	What it tells leaders
Time to approve standard access	Whether safe use is becoming easier.
Exceptions open and aging	Where risky access decisions remain unresolved.
AI Use Cases with approved data access path	Whether AI work can proceed safely.

06 Maturity: 0 to 5

Level	What it looks like	Evidence	Next move
0 Absent	Access is invisible, informal, inconsistent, or locked inside individual systems.	No classification, no clear rules, no owner path, no review.	Identify priority data and the highest-risk access exposures.
1 Initial	Some access rules exist, but decisions depend on individuals, tickets, memory, or local workarounds.	Ad hoc approvals, manual spreadsheets, inconsistent permissions.	Create simple classification levels and name owners for priority data.
2 Repeatable	Basic classification, access rules, and review paths exist for priority data and sensitive use.	Classification guide, access rules, approved paths, access requests.	Connect access rules to AI Use Cases, reports, automations, and vendor use.
3 Defined	Access is documented, owned, communicated, and used consistently across priority data domains.	Role rules, owner approvals, access review process, exception records.	Measure access speed, exceptions, review completion, and sensitive-use exposure.
4 Managed	Access is measured, reviewed, and connected to governance, risk, technology, privacy, and value decisions.	Dashboards, review logs, exceptions, incidents, AI access checks.	Use access evidence to improve tools, policies, workflows, and data products.
5 Optimized	Access continuously improves and makes safe data use fast, trusted, and scalable.	Automated reviews, adaptive controls, strong audit trail, low friction for safe use.	Keep improving access as AI, automation, regulation, vendors, and work change.

Maturity principle

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

07 How to Build and Mature the Capability

Start with the data that matters most. Do not try to classify everything at once. Build Access around current strategy, reporting, automation, AI Use Cases, regulatory exposure, client trust, and operational pain.

Minimum viable Data Access capability

- A short classification guide for priority data.
- A list of restricted and prohibited data uses, especially for public AI tools and external vendors.
- Named owners for priority access decisions.
- Simple access rules for the most important data domains.
- Approved paths for common reports, dashboards, automations, and AI Use Cases.
- A basic access review process for sensitive data and key roles.
- A decision and exception record for sensitive or unusual access.

First 30 days

- Pick three to five priority data domains, such as customer, employee, financial, operational, client, product, or service data.
- Identify where sensitive data is already being copied, exported, shared, or used in AI tools.
- Draft simple classification levels and examples.
- Name business owners for access decisions.
- Publish one temporary rule: sensitive or confidential data must not be entered into unapproved public AI tools.

First 90 days

- Create Data Access Rules for the priority domains.
- Define approved access paths for reporting, dashboards, automations, and AI Use Cases.
- Create a simple access request and routing path.
- Review the highest-risk current access, including broad shared drives, exports, vendor access, and AI tool use.
- Start a quarterly access review for sensitive roles, vendors, and priority data.
- Record exceptions and unresolved access decisions.

First year

- Expand classification and access rules to additional priority data domains.
- Connect access reviews to role changes, vendor changes, system changes, and AI Use Case approvals.
- Work with Technology to simplify approved access paths and reduce spreadsheet exports.
- Work with Risk, Privacy, Legal, and Security to improve rules for sensitive and regulated data.
- Use access evidence in Governance reviews and TIO maturity assessments.

What not to build too early

Do not begin with a complex enterprise-wide classification scheme, a large access committee, or a permission model no manager can explain. Start with priority data, current use, obvious risk, and practical rules.

08 TSLA Support and First Moves

The organization must own its data access decisions. TSLA can help leaders make those decisions clear, simple, practical, and connected to TIO.

Need	How TSLA can help
Classify priority data	Facilitate a practical Data Classification Workshop focused on business meaning, sensitivity, use, and risk.
Create access rules	Develop plain-English Data Access Rules for priority data, reports, automations, vendors, and AI Use Cases.
Define approval paths	Map standard, controlled, restricted, and exception access routes.
Connect Access to Governance and Risk	Clarify which decisions belong to data owners, governance forums, risk, privacy, security, legal, and technology.
Prepare for AI Use Cases	Define which data can be used in AI tools, under what conditions, through which approved environments.
Support maturity assessment	Use evidence to score Data Access maturity and define the next capability-building moves.

Monday morning moves

- Ask where sensitive data is currently being exported, copied, shared, or entered into AI tools.
- Pick the first priority data domain and name its business owner.
- Create simple classification labels that managers can understand.
- Write one-page access rules for that priority data domain.
- Define the approved path for common reports, dashboards, automations, and AI Use Cases.
- Review one high-risk access area, such as broad shared folders, vendor access, or customer data exports.
- Record open access exceptions and assign owners.

Closing point

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.

A Source Note

This guide is part of the TIO Library. It is aligned to the TIO Framework, the TIO Data Capability Domain Master, the TIO Capability Model and Maturity Assessment Tool, and the approved 8-section Capability Guide structure used across the TIO Library. It translates the Data Access capability into practical guidance for leaders and practitioners.

It is written as a practical executive guide. It is not a technical data-management standard, legal opinion, privacy assessment, cybersecurity review, or professional assurance report. Organizations should apply their own policies, obligations, accountabilities, and professional review where required.