

Data Access Governance Maturity Model

Assess your maturity. Prioritize risk. Build a roadmap for governing unstructured data.



Contents

Executive summary	3
The model at a glance	4
How to use the model	4
Level 1 — Reactive/Unmanaged	5
Level 2 — Discover & Assess	5
Level 3 — Remediate & Enforce	6
Level 4 — Certify & Govern	6
Level 5 — Continuous Governance	7
Capability dimensions across the maturity levels	8
Turn the assessment into a roadmap	8
How OpenText supports the journey	9
Executive takeaway	9

Executive summary

Sensitive and high-value unstructured data is distributed across file shares, cloud repositories, and collaboration platforms, often without clear visibility into who can access it or whether that access remains appropriate. As regulatory scrutiny grows and organizations expand their use of data for transformation, analytics, and AI, governing access to unstructured data has become a business imperative.

This maturity model provides a practical way to assess capabilities, identify gaps, and prioritize the next steps toward stronger data access governance. It evaluates six capability dimensions independently because maturity is rarely uniform. The result is a directional view of overall maturity plus a more useful roadmap: where risk is concentrated, which capability should advance next, and what business outcome that advancement can support.

Capability and expertise advance together. Stronger governance requires not only technology and controls, but also the operating discipline, ownership, and cross-functional participation needed to sustain them.



The model at a glance

Level	Organizational state	Expertise applied	Business outcome
1	Reactive/Unmanaged	Incidental	Risk is difficult to quantify; audit response is reactive
2	Discover & Assess	Diagnostic	Sensitive data and access exposure become visible
3	Remediate & Enforce	Operational	Excessive access is reduced systematically
4	Certify & Govern	Cross-functional	Access is accountable, reviewable, and auditable
5	Continuous Governance	Strategic	Risk reduction is sustained and governance supports safer data and AI use

Discover → Assess → Remediate → Certify → Continuously Govern

Understand risk → Reduce exposure → Prove compliance → Enable trusted data use

How to use the model

Maturity may vary by capability. Assess each dimension independently to identify strengths, gaps, and the highest-priority next steps. The overall maturity level provides a directional view, not a requirement that every capability be at the same stage.

Sensitive-data awareness What sensitive and high-value content exists and where it resides.

Access visibility Who can reach that content and how access is obtained.

Remediation and enforcement How inappropriate or excessive access is corrected and controlled.

Drift and change control How permission changes and deviations from an approved state are identified and addressed.

Identity and lifecycle governance How access and groups are governed as identities and responsibilities change.

Accountability and certification How access decisions are owned, reviewed, certified, and evidenced.

Level 1 — Reactive/Unmanaged

State. Access governance is primarily reactive. The organization relies on unstructured data but lacks a systematic view of where sensitive and high-value information resides, who can access it, and whether that access remains appropriate.

- Unstructured data and permissions grow with limited oversight
- Data ownership is informal or unclear
- Access issues are commonly identified through audits, incidents, or requests
- Evidence gathering and remediation depend heavily on manual effort

Business impact. Reactive operations, elevated exposure to inappropriate access, and low confidence in audit readiness.

Key question: Can you confidently identify where your most sensitive unstructured data resides and who can access it today?

Level 2 — Discover & Assess

State. The organization can identify sensitive data and analyze who has access. Risk becomes visible and can be prioritized, but remediation and governance remain largely manual or point-in-time.

- Sensitive data is discovered and classified
- Permissions and group membership can be reported and analyzed
- High-risk repositories and access exposure can be prioritized
- Remediation remains largely case-by-case

Business impact. Better understanding of risk, more focused remediation, and faster preparation for audits and reviews.

Key question: Once you identify an access risk, how consistently can you resolve it?



Level 3 — Remediate & Enforce

State. The organization moves from identifying risk to systematically reducing it. Policies guide remediation and management actions, and access changes are monitored rather than addressed only through isolated cleanup projects.

- Excessive or inappropriate access is remediated systematically
- Policies support repeatable management and protection of files and repositories
- Permission and group changes are monitored
- Risk reduction can be tracked over time

Business impact. Reduced exposure, greater operational efficiency, and stronger control over sensitive and high-value data.

Key question: Can you demonstrate that access issues are addressed consistently rather than through one-time cleanup efforts?

Level 4 — Certify & Govern

State. Access governance becomes a formal, accountable process. Business data owners participate in access decisions, access reviews are conducted on a defined cadence, and evidence can be produced to support compliance and audit requirements.

- Data owners participate in stewardship and access review
- Access is reviewed and certified
- Policies and workflows support ongoing governance
- Access decisions and certification evidence are documented
- Accountability spans IT, security, compliance, and the business

Business impact. Greater accountability, improved audit readiness, and stronger evidence that access remains appropriate.

Key question: Can the organization show that the right people have appropriate access to sensitive data—and that accountable owners have reviewed it?

Level 5 — Continuous Governance

State. Governance becomes an ongoing, programmatic discipline. Discovery, access insight, remediation, monitoring, ownership, and certification operate as a sustained governance cycle that can scale as data and business requirements evolve.

- Sensitive data and access are reassessed as environments change
- Policy-driven controls help maintain appropriate access over time
- Data owners remain engaged in stewardship
- Access reviews and evidence are integrated into the governance program
- Governance supports safer use of sensitive data for analytics, collaboration, and AI initiatives

Business impact. Sustained risk reduction, scalable governance, stronger compliance evidence, and greater confidence in using enterprise data for new business initiatives.

Key question: Can your governance program keep pace as data, access, and business use cases change?



Capability dimensions across the maturity levels

Assess each row independently. Uneven maturity is expected; the earliest-stage capability often indicates the most practical place to focus next.

Capability	L1 Reactive	L2 Discover & Assess	L3 Remediate & Enforce	L4 Certify & Govern	L5 Continuous
Sensitive-data awareness	Location and sensitivity largely unknown	Sensitive content discovered and classified	Sensitivity informs prioritization and policy	Sensitive data aligned to ownership and review scope	Discovery and governance are sustained as data changes
Access visibility	Effective access is difficult to answer	Access and permissions can be reported	Access gaps are measured and monitored	Entitlements are reviewable by accountable owners	Access insight is maintained as environments change
Remediation and enforcement	Primarily reactive	Manual, case-by-case cleanup	Policy-driven, repeatable remediation	Automated policy actions with governed exceptions	Ongoing policy-driven remediation and verification
Drift and change control	Changes may go unnoticed	Point-in-time reassessment	Permission changes monitored on a schedule	Approved state and exceptions are governed	Changes are continuously identified and addressed through policy
Identity and lifecycle governance	Access can persist beyond business need	Movers/Leavers reviewed manually	Lifecycle processes increasingly inform access	Groups and roles have defined ownership and review	Lifecycle governance is programmatic and sustained
Accountability and certification	Ownership unclear; evidence assembled reactively	Risk is visible but ownership remains developing	Roles and decisions are documented	Owners review and certify access; evidence is auditable	Certification and evidence are embedded in the governance program

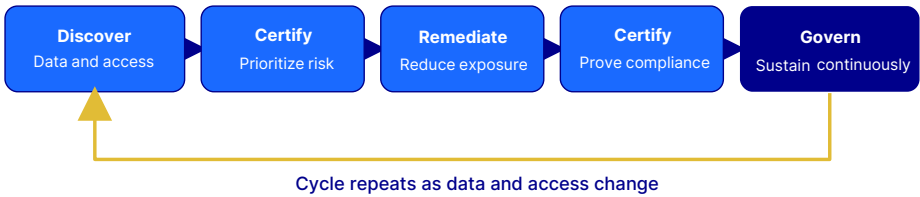
Turn the assessment into a roadmap

Use the assessment to convert maturity findings into a prioritized improvement plan:

- 1. Establish the current state.** Score each capability dimension independently.
- 2. Identify the priority gap.** Focus on the capability that is creating the greatest risk or constraining progress elsewhere.
- 3. Define the target state.** Set the maturity needed to support the organization's risk, compliance, and business objectives.
- 4. Select the next capability.** Advance the specific process, expertise, ownership, or control required to close the gap.
- 5. Measure the outcome.** Track improvements such as reduced exposure, faster remediation, stronger audit evidence, and broader governance coverage.



How OpenText supports the journey

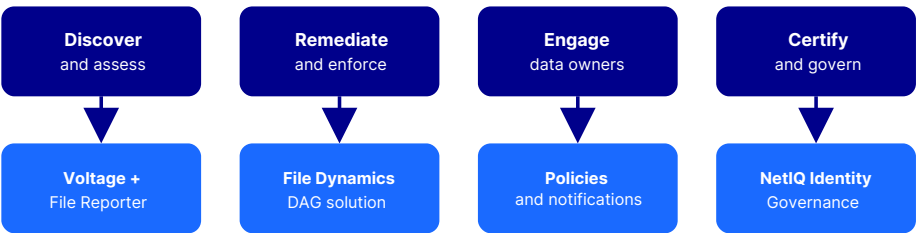


Discover and assess — OpenText™ Voltage™ Data Security Platform discovers and classifies sensitive data; OpenText™ File Reporter identifies who has access and how access is obtained.

Remediate and enforce — OpenText™ File Dynamics provides policy-driven capabilities to move, archive, delete, and protect files and repositories. OpenText File Reporter and OpenText File Dynamics make up the OpenText Data Access Governance solution.

Engage data owners — Policies and notifications can involve line-of-business data owners when access permissions change.

Certify and govern — OpenText™ NetIQ™ Identity Governance supports access reviews, certification, and attestation for governed access.



Executive takeaway

Data access governance maturity is not a single score. It is the ability to progressively understand sensitive unstructured data, determine who can access it, reduce inappropriate access, engage accountable owners, and demonstrate that controls remain effective. Organizations can use this model to identify the most important gap, define the next practical step, and build a governance program that reduces risk while supporting trusted use of data.

[Continue your journey >](#)