CONCENTRIC Ai

Data Security Governance Checklist

Data Discovery

Your data is everywhere, and it's multiplying. Most legacy tools need a rulebook just to start searching — regex, data samples, manual configurations — sound familiar? There's a solid chance you'll still miss sensitive data and spend your day chasing false positives.

What you need is smarter discovery — a solution that autonomously finds and categorizes data everywhere, understands what it's looking at, and can tell a pay stub from a partnership agreement without handholding. Context is everything, and your data deserves a security solution that gets it.

Classification

Now that you've got eyes on your data, it's time to classify it. Why? Because your security tools like DLP, ZTNA, and CASB can't do their job effectively without this.

Start by creating a classification policy that makes sense for your organization then configure labels in the systems that manage access and sharing. Map your data to the right labels, classify existing data, and set rules to ensure anything new gets sorted automatically.

Once your classifications are in place, your DLP tools can begin enforcing your access policies. Congratulations, you just turned visibility into control.

Data Access Governance

Your data is nicely labeled and organized. Now you need to make sure that the right people (and only the right people) have access. Just like with classification, it starts with a solid policy — one that spells out what acceptable use looks like, how you'll detect and deal with unauthorized sharing, how you'll communicate expectations to users, and how you'll handle exception requests (because there will be some). This gives you a framework to audit and remediate access.

At this point, you focus on the details. Which types of data need protection, and who should have access? HIPAA-regulated records, intellectual property, and PII all need to be locked down. If a user left the company six months ago and still has access to your product roadmap, that's a problem. Publicly shared folders? Personal email and file sharing? Those need to go too.

Access should be intentional, not accidental, and good policies make that happen.

Data Retention

You've classified your data and locked it down. Now it's time to clean house.

Data retention is key to staying compliant, cutting storage costs, and reducing your risk surface. Plus, nobody likes version chaos.

Start with — you guessed it — a solid, documented retention policy that maps your data accordingly. Then, lay out your cleanup game plan, including how you will handle exceptions.

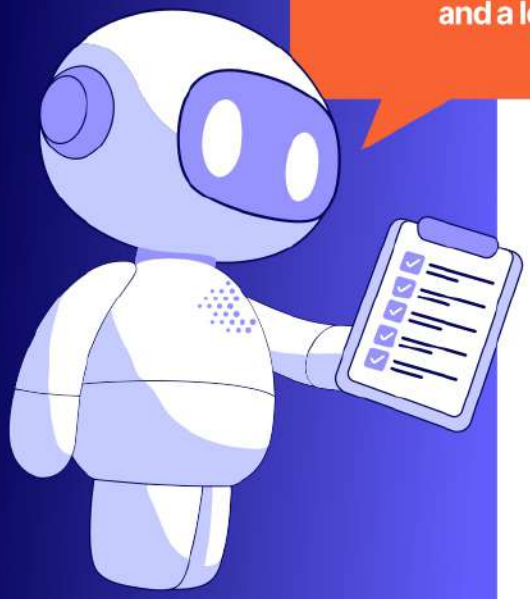
Apply retention labels on data, delete or archive anything past its expiration date, and set up your systems to enforce the rules automatically. Finally, kill off those duplicate files because nobody needs eight copies of the same quarterly report.

Monitoring and Control

Data security isn't a slow cooker that you can set and forget. Even with automation doing the heavy lifting, you still need to stay alert.

Set up notifications for anything suspicious, like files being overshared, misclassified data, and expired records. Monitor user behavior for anything out of the ordinary and keep tabs on your email and collaboration channels. And if you've got compliance requirements (spoiler alert — you do), set those violation alerts. This final step of monitoring and control is what keeps everything in check.

An effective data security governance finally gives you the clarity you've been chasing. Less risk, fewer compliance headaches, and a lot more ROI on your security tools. It's a no brainer.



About Concentric AI

Concentric AI is intelligent data security made easy. We help businesses discover, secure, and organize their data, cutting through the chaos with AI-powered clarity and control.

Request a Demo

Requirements for an Effective Data Security Governance Solution

Requirement	Included
Platform & Deployment	
Prevents GenAI assistants and proprietary GenAI from leaking sensitive data to unauthorized users	✅
Broad integration across SaaS, collaboration, messaging, and cloud services	✅
Scalable architecture with low false positives/negatives	✅
Heavy infrastructure or endpoint agents required	❌
Secure API-based access with minimal infrastructure overhead	✅
Data Discovery & Classification	
Automatic discovery of sensitive data across cloud, on-prem, SaaS, and messaging apps	✅
Support for both structured and unstructured data	✅
AI-driven, context-aware discovery and classification	✅
Reliance on end-user tagging and manual classification	❌
Reliance on rules, regex, and other pattern-matching methods	❌
Requires submission of data samples to train LLMs	❌
Risk Identification & Monitoring	
Identifies unclassified and misclassified records	✅
Catches data stored in the wrong location	✅
Flags overly broad or excessive permissions	✅
Exposes unsafe or unauthorized sharing practices	✅
Detects unusual or anomalous behavior around sensitive data	✅
Manual rule-writing or regex to find data risks	❌
Continuous monitoring of data lineage and movement	✅
Remediation & Enforcement	
Automated remediation of permissions, entitlements, and sharing	✅
Policy enforcement without manual rule writing	✅
Integration with ITSM/incident response workflows	✅

Reliance on large security teams to investigate risks	✗
Configurable protections for sensitive data handling	✓
Data classification	✓
Managing permissions and access	✓
Relocating data to secure locations	✓
Deleting or archiving sensitive data	✓
Blocking data from being shared	✓
Masking/redacting sensitive data	✓
Governance & Compliance	
Centralized visibility into access policies	✓
Automated access reviews and certifications	✓
Mapping of controls to compliance frameworks (GDPR, HIPAA, SOX, etc.)	✓
Retention policy enforcement and defensible deletion	✓
Manual compliance reporting with spreadsheets	✗
Supports custom/proprietary frameworks	✓
Enables the processing of DSAR requests	✓
GenAI & Emerging Use Cases	
Identification of shadow GenAI	✓
Continuous risk monitoring	✓
Prevents GenAI assistants and proprietary GenAI from leaking sensitive data to unauthorized users	✓
Blocks or redacts sensitive data from being shared with public GenAI	✓
Trains proprietary GenAI workloads on a curated dataset	✓
Monitoring AI agents' access and activity	✓
Manual blocking of GenAI access without context awareness	✗
Data Lifecycle Management	
Deduplication and near-duplicate detection	✓
Archiving and cold storage recommendations	✓
Expiration, retention, and defensible disposal automation	✓
Dependency on storage vendor-specific retention tools	✗
Support for both business and regulatory retention schedules	✓