privacera

WHITEPAPER

Transform, Automate, and Align Data Security Governance with the Business

privacera

contents

From brand to revenue growth, IT calamities negatively impact virtually all areas of the business. Look no further than Target and more recently, Southwest. Their data security and tech-debt issues proved there is a concrete connection between technology investment and the continuing success of a business franchise.

According to David A. Aaker, "brand equity is a set of brand assets and liabilities linked to a brand, its names and symbols that add to or subtract from the value provided by a product or service to a firm and/or to that firm's customer." Without question, controllable disaster subtracts from brand equity and impacts customer loyalty, perceived quality, switching costs, and brand associations. In consumer-facing enterprises and industries of compliance, data needs to be better managed and protected but remain accessible to those that need data to perform their jobs.

Done right, data security governance is an opportunity for IT organizations to gain business influence and relevance. However, the problem these days is not so much in making the business case, but the difficulty and expense of delivering data security governance systematically across the entire enterprise. To work, enterprises need to discover and understand their data, control its access, and ensure it is trusted, compliant, and fit for consumption.

The Value of Well-Managed Data Security Governance

Despite the historical difficulties, the business value of data security governance includes:

- Reducing the time to data and insights
- Industrializing creation of data products and business model adaption
- Minimizing business risks
- Avoiding penalties and fines
- Safely increasing data availability and accessibility
- Ensuring the right people are doing the right things at the right time with data
- Addressing regulatory requirements
- Formalizing controls, processes, and accountabilities
- Improving data compliance
- Improving data transparency
- Proving to auditors the right things were done

For the above reasons, data security governance should be a best practice for all organizations. And where this is not significant enough justification, there is always regulation. A minimalist list today includes GDPR, CCPA, HIPAA, GLB, and PCI-DSS. According to Jason James, former CIO at NetHealth, "The ultimate prize for threat actors is the data, so CIOs and CISOs must protect that data. Today, someone takes the fall for a breach and it could be the CIO, CISO, CEO, or all."

[1]Managing Brand Equity, David Aaker, page 15

Why Has the Journey Been So Difficult?

To be effective, data security governance needs to address a number of business questions.

- What data does our organization have?
- Where is this data?
- What do we need this data for?
- Who has access and owns it?
- How should it be controlled, protected, and maintained?

The problem is data security governance has been difficult, and data controls typically have only been managed system by system. And to achieve all the aspects mentioned above, several separate tools are deployed to discover, mask, or encrypt data. Even worse, data governance has failed organizations because it has typically been:

- Forced top-down
- Tedious and overly manual
- Manpower intensive
- The costs have been excessive and, in some cases, uncontrollable
- Lacking transparency—making auditing difficult
- Bureaucratic versus controls oriented

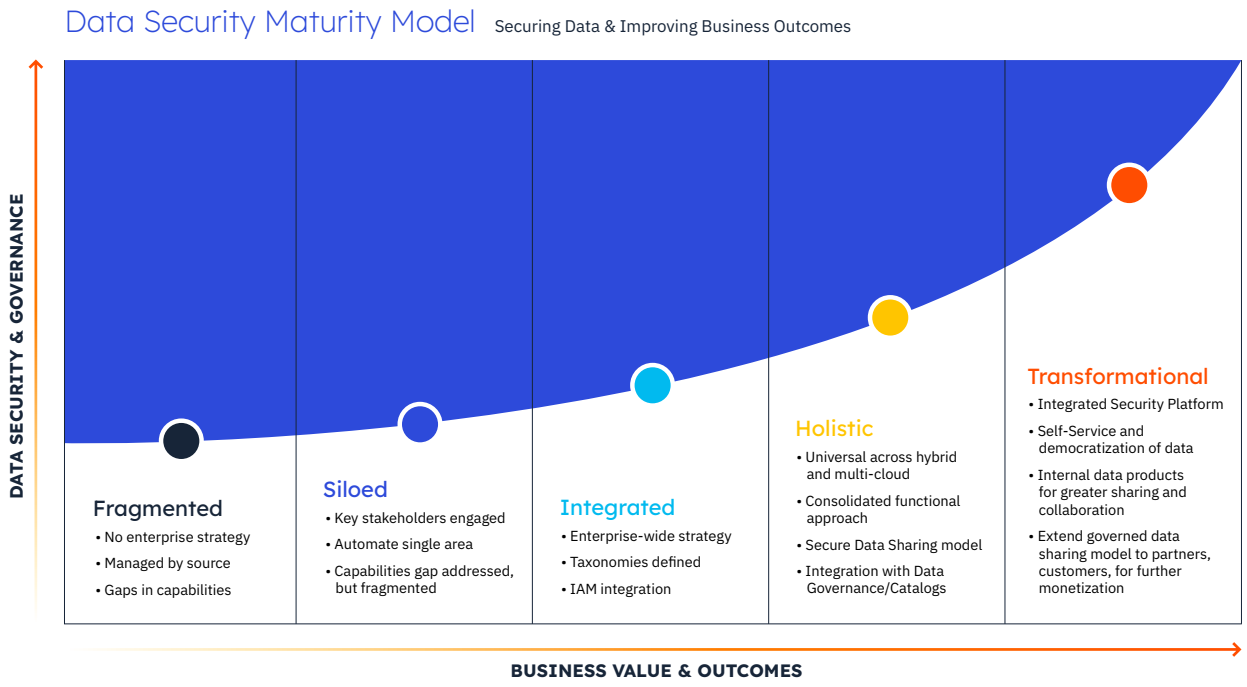
Former BusinessWeek CIO Isaac Sacolick says, "When governance is bureaucratic, it slows organizations down and creates tension." Controls and data security architectures have been typically implemented source by source, which increases costs. This means IT needs expertise and data security for each system in its growing hybrid data estate. For this reason, users are typically poorly educated about data governance, security, and risk.

These facts have led to unsuccessful data governance implementations and breaches. And this is not just an IT problem. If your definitions and discovery of sensitive data are poorly implemented, so is your governance, risk management, and security. Organizations shouldn't rely just on automation or use it as a crutch. However, if there was only one system for processes and systems for control to be mastered, it would be a gamechanger.

The problem is data security governance has been difficult, and data controls typically have only been managed system by system. Even worse, when done wrong, data governance has failed organizations.

Model for Data Maturity

Clearly, everything comes down to people, process, and technology. So, how do organizations move forward? The data security maturity model is an ideal source of truth to answer this question.



As you can see in the diagram, organizations typically fall in one of five states of maturity for data security and access. For this reason, it is critical that IT leaders evaluate their current state and determine their desired future state, including the steps required to achieve that future state.

Fragmented

When you're at this stage, there isn't an enterprise data security and access strategy. Data security and access is managed by the source system and sometimes even by the account. Here, there is likely some coarse-grained access that has been applied using an identity access management (IAM) system, which provides broad security, but it lacks agility and creates security gaps since it's an all-or-nothing type approach to security for each data system. Risk surface is large because anyone with access can be compromised by a phishing attack.

Siloed

This is a transitional stage. Here, key stakeholders in data, analytics, technical operations, and security are involved. And an initial framework is

being defined for a holistic enterprise approach to data security. The initiative has an executive owner. Ideally, the focus is rolling out a unified data security and access strategy, starting with an initial business area or function. The goal is to cover the entire data estate.

In many cases, this might be driven by a platform team responsible for a data or a cloud environment.

The approach is still siloed and might be different across silos. Some simplification and automation is taking place. There may be the emergence of a unified approach to create siloed security guardrails. In addition, there is planning to integrate IAM based on a user-attribute approach, including the initial steps of incorporating sensitive data tagging and classification, as well as integrated data masking and encryption.

Integrated

In this stage, there is an enterprise strategy with all stakeholders involved and a clear executive sponsor. With the success of the initial business area or data silo, the project is expanded to additional business areas or data silos. Tag and classification taxonomies, and where needed, data-naming taxonomies, are well-defined. And a standard approach to sensitive data identification and tagging is being rolled out using common taxonomies aligned with user attributes.

Holistic

The enterprise data security and access strategy is rolled out. It is expanded to even more business areas and data, consistently covering hybrid and multi-cloud. A consolidated, standardized approach for a unified data security platform is systematically incorporated across the enterprise. This ensures consistent rules are applied to sensitive data discovery, tagging, classification, as well as masking and encryption. This is integrated with universal data access controls.

Ideally, the focus is rolling out a unified data security and access strategy, starting with an initial business area or function. The goal is to cover the entire data estate.

Global enterprise guardrails have been established and data access and security can be delegated across the enterprise to data owners and stewards. Guardrails ensure the consistent application of data security policies are universally followed. Exception workflows can be established where data consumers require access beyond their classification level. Time-based or project-based access can be granted to provide timely data access while minimizing security risks. Unified data security is fully integrated into the approach to data cataloging, creating a comprehensive data governance life cycle approach.

Transformational

In the transformational stage, the data governance model can be extended out to data products, partners, and customers, fully incorporating data monetization into your data security framework.

Depending on a range of factors—age of the enterprise, specific industry, size and available resources, stakeholder buy-in—companies find themselves at different stages, and in some cases, they have elements of multiple stages, while missing certain components within the same stages. This is normal.

This maturity model is meant to be a tool to identify gaps and prioritize further work, including the identification of end goals.

Principles of Effective Data Security Governance

Effective data security governance should be transparent, establish accountabilities, and involve standardization.

As with other forms of data governance, organizations need to start with vision, goals, current state, and future state. According to former CIO of Palo Alto and author of "Data Governance for Dummies," Jonathan Reichental says this includes the desired outcomes and the metrics for managing success.

This means the starting point for a data security governance program is ensuring everyone understands what success is. This is critical to putting a data culture in place, where everyone understands the value of data and why it needs to be protected. This means understanding why data security governance is instantiated into policies, processes, and standards that guide behavior.

Effective data security governance should be built on the principle of inclusiveness. In other words, doing the right thing well. The foundation for doing this is the establishment of data security policies that provide conditions under which team members are granted access. This should be built on appropriate privilege, ensuring the processing of personal information is authorized, fair, and legitimate.

As a goal, data security governance should enable data ownership without data stewards needing to take on another job to manage data access. Tools should take the work out of being a data steward. This is accomplished by making it easier to:

- Identify sensitive assets.
- Determine what to do with them.
- Create policies and controls without coding.
- Support workflows.
- Monitor performance.

At the same time, data security governance should be built on modern data principles, including DataOps and continuous improvement. It should address the entire cycle, including managing and

auditing. As such, it should reflect the principles of Data Governance Ops—automated and continuous governance. From a practical perspective, it should also eliminate siloed management, auditing, and monitoring.

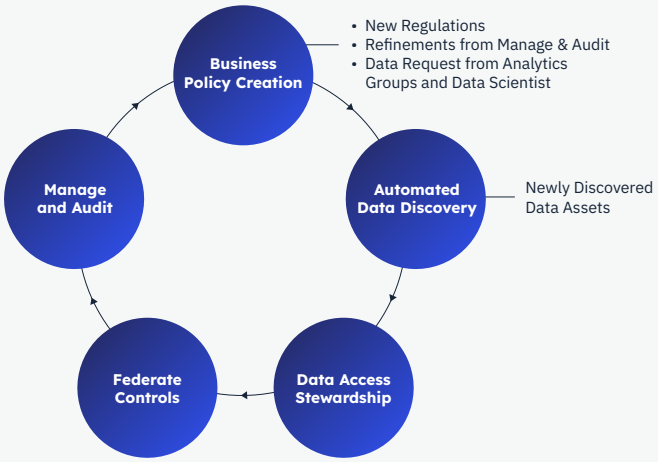
It should be simpler to go from business policy to holistic data discovery to stewardship functions around policies, centralized controls, and then measuring and managing the process. In the past, policies have needed to be extremely detailed before discovering sensitive data. Critical measurements should include the percentage of policies developed, disputes resolved, compliance issues, reduction of risks events, and reduction percentage in security incidents.

How Privacera Delivers

Privacera provides an end-to-end solution for managing data security governance processes. This solution provides holistic data visibility, secure access, and compliant collaboration across an increasing hybrid IT data estate.

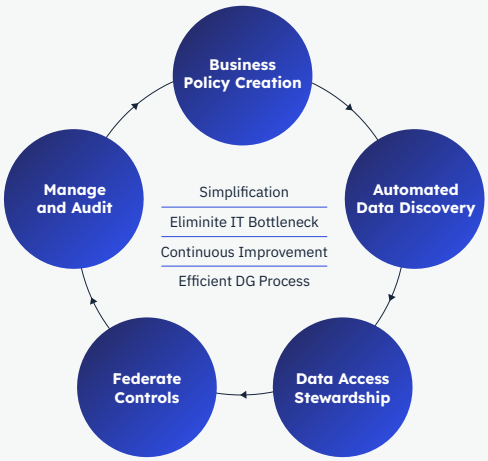
How Privacera Delivers

End-to-end solution for managing data security governance processes.



Modern, Simplified Data Security Governance

Holistic data visibility, secure access, and compliant collaboration across the entire data estate.



Business Policy Creation	Automated Data Discovery	Data Access Stewardship	Federate Controls	Manage and Audit
Data access governance mission	Scan data sources	Develop business access policy definition—business attribute, function, title, location	Implement global controls	Comprehensive auditing and reporting
Business policies and standards	Discover sensitive and PII data	Business-area-specific workflows and access request approval	User-attribute-based rules with IAM integration	Drive process improvement
Define data classification levels	Implement and refine tag and classification rules	Domain or business-specific policies and rules	Control and protect data at rest and in motion	Sensitive data mapping and tracking across data estate
Define types of sensitive data		Define business-oriented data domains (logical), ownership and federated stewardship	Implement logical/ functional data domain-specific rules and controls	Integrate into SIEM and other infrastructure-wide monitoring platforms
Define classification levels sensitive data falls into				
Define protections based upon the classification levels				
Evaluate and create additional tag and classification rules				

Previous table in a RACI matrix

Data Security Governance Task	CDO/ CIO/ CISO	Business Data Owner	Data Gover-nance Leader	Data Steward	Data Engineer	Data Ana-lyst/Data Scientist
Business Policy Creation						
Data Access Governance Mission	A	I	R	C	C	C/I
Business Policies and Standards	A	C	R	R	I	C/ I
Define Data Classification Levels	I	C	R	C	I	C
Define Types of Sensitive Data	A	I	R	C	I	I
Define Classification Levels Sensitive Data Falls Into	A	I	R	C	I	I
Define Protections Based Upon the Classification Levels	A	I	R	C	C	I
Evaluate and Create Additional Tag and Classification Rules	I	C	A	C	R	I
Automated Data Discovery						
Scan Data Sources, Discover Sensitive/PII Data			A	R	I	
Implement and Refine Tag and Classification Rules			A	A	R	I
Develop Business Access Policy Definition—Business Attribute, Function, Title, Location	I	I	R	A	C	C

Data Access Stewardship						
Develop business access policy definition—business attribute, function, title, location	I	C	A	R	I	I
Business Area Specific Workflows and Approval Requests	I	Ç	A	A	R	I
Domain or business-specific policies and rules	I	C	A	R	I	I
Define business oriented data domains (logical), ownership and federated stewardship	I	C	A	R	I	I
Federate controls						
Implement Global Controls	R/A		A	R	C	I
Implement Localized Controls Single System or Stakeholder Group	I	I	A	R	C	I
User-Attribute Based Rules	R/A	I	A	R	C	I
Implement logical/ functional data-domain specific rules and controls	I	I	A	R	C	I
Manage and audit						
Comprehensive Auditing and Reporting	A		R	I	I	I
Drive Process Improvement	A		R	C	`C	I
Sensitive data mapping and tracking across data estate	I	I	A/R	R/C	C	C
Integrate into SIEM and other infrastructure-wide monitoring platforms	R		A	I	C	

RACI role	Definition
Responsible	Executes the work to complete the task.
Accountable	Delegates work and is the last one to review the task or deliverable before it is deemed complete.
Consulted	Provides input based on how it will impact their project work or their domain of expertise on the deliverable itself.
Consulted	Provides input based on how it will impact their project work or their domain of expertise on the deliverable itself.

Privacera's end-to-end data security governance solution eliminates complexity by providing a unified platform for managing data security versus a patchwork of governance and controls per data product, service, or account.

Without Privacera, today's solution architects try their best to consider data security and data privacy in their application and then implement policies into each system; in some cases using scripting against data elements that need protection. This approach increases the workload of data stewards, data engineers, and others involved in managing the data ecosystem.

The Privacera solution automates manual data governance security tasks and processes. It enables continuous improvement of data governance security. The daily lives of data stewards are improved by automating sensitive data discovery, which simplifies the process of creating security protection policies and controls for all relevant source systems.

How does Privacera deliver on this promise?

Automated Data Discovery

You cannot govern or secure data if you do not know it exists. It is critical to identify and classify sensitive data as it is ingested and before it is accessed by users. Privacera provides comprehensive visibility into all sensitive data across source systems. Data stewards can make the right decisions about what should be protected and who should or should not have access across source systems. Privacera automatically detects across multiple cloud databases and analytics platforms, allowing rules to be written once for all sources. Specifically, Privacera uses pattern recognition and machine learning to power the discovery and tagging of unprotected data and PII. These technologies automatically scan, identify, and tag sensitive data on-premises and in the cloud—across the entire data estate.

Data Access Stewardship

Data access stewardship as a goal should be non-invasive and utilize organic data stewards where possible. However, because data access is ultimately about who can access data, this function needs to be done in tight coordination with data owners. The process should start by the data governance leader with data owners defining business data domains and appropriate data access stewards for those business domains. Where possible, it is ideal for these to be the same people that manage domain metadata and data quality.

With data stewards identified, they should be focused on domain-specific access policies and controls. In the form of a data stewardship council or steering committee, data stewards together tackle global access policies and controls working closely with data governance, security, and infrastructure teams. This is so global rules can be defined and consistently and globally applied to support regulation and compliance requirements.

Regardless of whether they're formulating localized or business-area policies and controls, data stewards need one place in which to define business data domain standards, data access policies, and data access controls. They need to be able to define policies and controls easily. Defined policies and controls then need direct approval processes. Built-in approval workflows allow for business-specific data requests by data consumers to be approved by data stewards.

Federate Controls

With sensitive data, data infrastructure, governance, and security teams need to be able to formulate data access controls for global management. This starts by defining global data rules, how data should be classified and tagged based on the sensitivity of the data and the business damage that would result from unauthorized internal or external exposure, how that data needs to be protected, and which users can access that data based on their user attributes, such as access level, certifications, and function.

At the same time, the implementers of the data stewardship council may need to be part of the defining and implementation process.

The above is done by using a combination of control mechanisms including; role and resource-based access control (RBAC), attribute-based access control (ABAC) and tag-based access control (TBAC). These controls simplify and automate data protection and can eliminate much of the manual work implementing and managing data security and access controls.

To enable this, Privacera has native integrations with the broadest range of data sources and data governance and security tools. This creates an end-to-end integrated and comprehensive data access, governance, and security ecosystem. Additionally, Privacera supports a federated access and security data stewardship model with global guardrails.

To enable this, Privacera has native integrations with the broadest range of data sources and data governance and security tools. This creates an end-to-end integrated and comprehensive data access, governance, and security ecosystem.

Manage and Audit

Privacera allows you to manage the end-to-end data security governance process, including monitoring and auditing your data security and access policies. In particular, Privacera allows you to evaluate the performance of your data security governance program, including all data security and access policies implemented, and view all sensitive data and where it resides. Privacera does this by providing comprehensive dashboards, and reports, as well as a detailed audit trail. Detailed audit trails help data stewards and auditors understand what data was accessed, by whom, and when. This detailed audit data can be integrated with your security analytics tool of choice, such as Splunk to perform advanced analytics and to apply analytical and machine learning models to detect and alert when any anomalous access or behavior occurs.

Fortune 500 enterprises trust Privacera for their universal data security, access control, and governance. Discover how to streamline data security governance with Privacera.

Take a unified approach to data access, privacy, and security with Privacera.

REQUEST A DEMO CONTACT US

Privacera, based in Fremont, CA, was founded in 2016 by the creators of Apache Ranger™ and Apache Atlas. Built on the principle of delivering trusted data access to data consumers, the company provides data privacy, security, and governance on its SaaS-based data security and access governance platform. It serves numerous Fortune 500 clients in the finance, insurance, life sciences, retail, media, consumer industries, and government agencies and entities. Privacera has been recognized as a leader in the 2023 GigaOM Radar for Data Governance and has achieved AWS Data and Analytics Competency Status. The company was also named a 2022 CISO Choice Awards Finalist and received the 2022 Digital Innovator Award. Recently, it was named a "Sample Vendor" for data security platforms in the Gartner Hype Cycle for Data Security, 2022. Learn more about Privacera at privacera.com.

privacera