privacera

Data Security Maturity Model in 5 Steps

WHITEPAPER

privacera

WHITEPAPER

Data Security Maturity Model in 5 Steps

privacera

contents

Security risks are everywhere in today's connected world, impacting businesses, governments, critical public services and infrastructure as well as individuals. As the frequency, complexity, and severity continues to escalate, strengthening your organization's security posture has become an imperative. In this environment, organizations that are responsible for data security governance must strive to assess and achieve security maturity.

The term **"security maturity"** refers to an organization's security position relative to its risk environment. The risk scenarios will vary, as each organization has its own security risk culture and tolerances. Thus, the maturity level of an organization is determined by how efficiently it assesses risk, implements controls, provides reporting, and manages processes. This white paper provides an overview of what data security maturity means to your organization and why it's critically important, provides guidance to help you assess your level of maturity, and offers recommendations on how to achieve the desired technical and business outcome.

Definition of Data Security

While there may be different interpretations of what Data Security is, the definition that we use for this paper aligns closely to the Gartner and Forrester definitions. Data Security is an element of the broader Data Governance category and focuses on data residing in data stores and used for analytical workloads.

Data security comprises the processes and associated tools that protect sensitive data, either in transit or at rest. Data security methods include:

- Identification and classifying of sensitive data
- Protecting sensitive data which includes:
  - **Encryption** (applying a keyed cryptographic algorithm so that data is not easily read and/or altered by unauthorized parties)
  - **Masking** (substituting all or part of a high-value data item with a low-value representative token)
  - **Enterprise Data Access Control**s at both a global and local level
  - **Holistic audit and reporting of sensitive data and data access** (who is access what data and when)

The Evolution of Security Maturity Models

A security maturity model is a set of characteristics or indicators that represent capability and progression within an organization's security program. What we know today as security maturity models trace their history back several decades. To fully appreciate the value of a security maturity model applied specifically to data security, it helps to understand how other security maturity models have developed over the years.

As organizations adopted computerized systems through the 1960s and '70s, the demand for software development exploded. Developers raced to meet demand without reliable frameworks or best practices as guard-rails, and failures became common. Several strategic U.S. military programming projects failed to meet their objectives, prompting the Department of Defense to create the Capability Maturity Model (CMM), intended to formalize and improve business processes around software development. This model was updated in 2006 with the Capability Maturity Model Integration (CMMI) roadmap.

Since 2012, new maturity models have been developed and updated specifically to address cybersecurity best practices. These include the Cybersecurity Capabilities Maturity Model (C2M2),

the National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF) and the Department of Defense Cybersecurity Maturity Model Certification (CMMC).

While organizations across all industries have relied on these maturity models to measure their business processes and cybersecurity capabilities, until now there was no model that addressed the requirement for measuring data security maturity.

A Data Security Maturity Model: Why Now?

In its most recent hype cycle report, Gartner introduced the concept of the Data Security Platform (DSP), recognizing Privacera as a sample vendor. Traditionally, data security has been delivered by disparate products, resulting in operational inefficiencies, inconsistent application of data security, and an inability to support internal innovations and collaborations involving data. A DSP simplifies your data governance framework and enables the modern approach you need to holistically manage data security and access across your data estate.

DSPs aggregate data protection requirements across data types, storage silos and ecosystems, starting with data discovery and classification. They protect data by using late binding access controls such as data masking, format-preserving encryption (FPE) or tokenization. They also incorporate integrated data access policy creation and enforcement. Especially in cloud-based data stores, a DSP reduces integration cost, manual processes and friction by connecting previously disparate data security controls and capabilities. A DSP significantly increases the visibility of, and control over, data and its broad usage and puts organizations in a position to truly secure their data.

A DSP simplifies your data governance framework and enables the modern approach you need to holistically manage data security and access across your data estate.

DSP adoption is being driven by two trends relating to data security, privacy and advanced analytics. (1) Enterprises are being forced to strengthen data security and privacy to meet the challenges associated with DevSecOps, open data regulations and advanced analytics, and (2) Organizational data is increasingly distributed and data is likely to be processed and stored in public cloud services, requiring organizations to manage their data access and security far more effectively.

A Maturity Model for Data Security

While not prescriptive like the existing cyber-security maturity models highlighted earlier, we have created a data security maturity model to serve as a guide to understanding the current state of your data environment versus the desired future state, and provide you with a framework to measure and achieve that desired state.

In our experience at Privacera with data-driven organizations in many different verticals, when it comes to unified data security and access we have observed five security maturity stages. To provide some guidance for organizations that are relatively new to data security, we have categorized each stage in order from the least mature to the most highly mature, as follows: Fragmented, Siloed, Integrated, Comprehensive, and Transformational.

1. **Fragmented:** The organization has no enterprise data security or access strategy, or if one exists it is limited in scope. Data security is managed by each source system, and sometimes even account by account. Information security processes are unstructured and policies may be documented, but are not consistently applied with no systematic method to verify enforcement. Some coarse grained access likely has been applied probably using IAM. This provides some broad level of data security, but lacks agility and granularity, since it is generally an all or nothing type approach to security for each data silo. In this scenario, controls are not automated or reported to the business and are often limited to foundational controls, leaving many functional gaps that expose sensitive data.

2. **Siloed:** Key stakeholders in data, analytics, tech operations, and security teams are collaborating led by an executive owner from one of these teams with the focus on rolling out a unified data security and access strategy. In this stage, simplified and automated data security is only deployed for a single data/business category, with a goal of eventually covering the entire data estate.

> The approach to data security functionality is still fragmented, but functional gaps are gradually being filled.

These may include a unified approach to create siloed security guard rails, integration of an IAM, incorporation of sensitive data tagging and classification, as well as integrated data masking and encryption. Information security processes are established, but policy is informally defined and only partially applied. In this stage, some automation may exist with limited business reporting capabilities.

3. **Integrated:** An enterprise-wide data security strategy involving all key stakeholders led by a dedicated executive sponsor has been established. With the success of the initial business area or data silo, the data security project has been expanded to include multiple business areas and data silos, and fragmented data security functionality has been rationalized.

The organization has integrated Data Security Governance products for greater automation to include a tag/classification-based approach to access control.

Classification and data naming taxonomies are well-defined. A standard approach to sensitive data identification and tagging is being rolled out using common taxonomies that are aligned with user attributes. Data masking and encryption are being consistently applied at a relative granular level to targeted business areas or data silos, thus systematically removing the silos. Enterprise data security guardrails are starting to be rolled out. There is more attention to policy documentation and implementation, with greater levels of reporting.

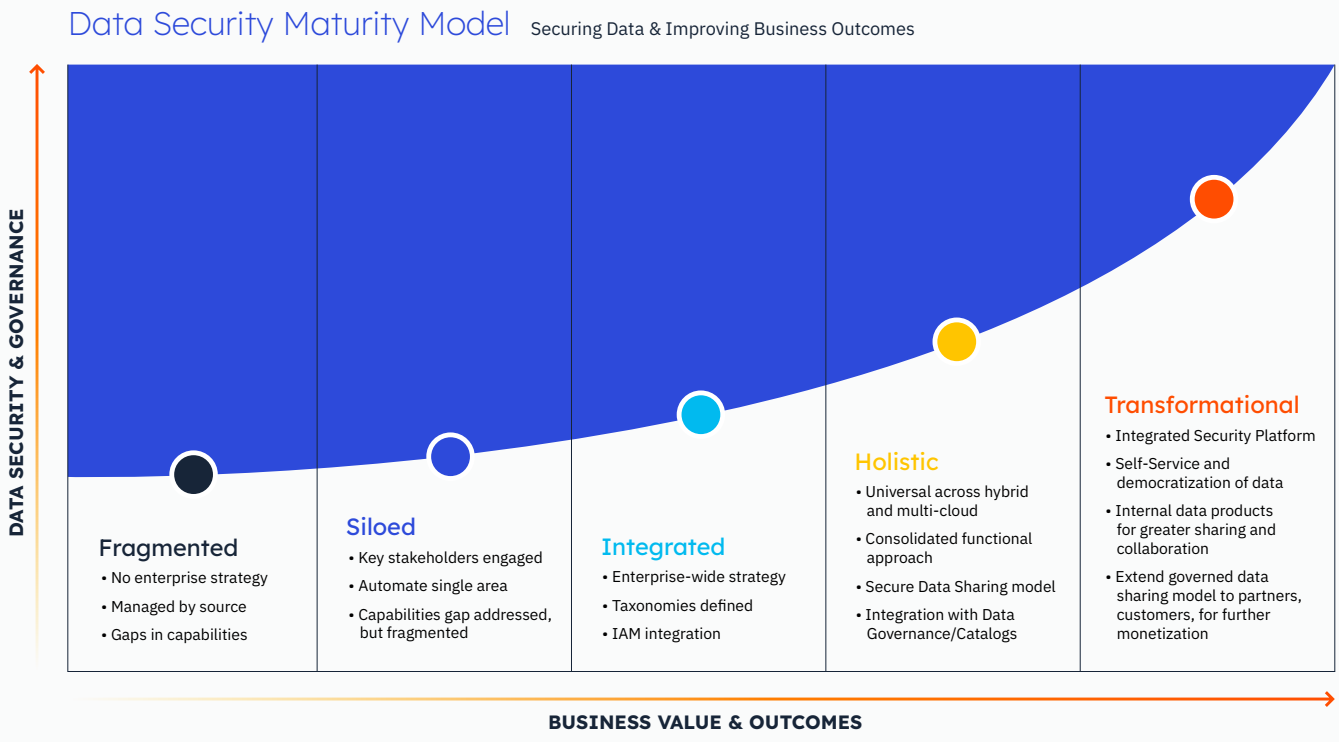
4. **Comprehensive:** The organization's data security strategy has been further refined, with data security being applied across the entire data/business domains including hybrid and multi-cloud. A consolidated standardized approach into a unified data security platform is systematically incorporated across the enterprise to ensure that consistent rules are being applied to sensitive data discovery, tagging, classification, masking and encryption and that is integrated with universal data access controls.

Global enterprise guard rails have been established and data access and security can be delegated across the enterprise to data owners and stewards, with the guard rails ensuring that consistent application of data security policies are universally followed. Exception workflows can be established where data consumers require access beyond their classification level and time-based and/or project based access can be provided to provide timely data access while minimizing security risks.

This unified approach to data security functionality supports secure data sharing and facilitates integration with data governance products such as data catalogs thus creating a fully data governance life cycle approach. The organization controls its information security processes with comprehensive policies, widespread implementation, a high degree of automation, and business reporting.

5. **Transformational:** At this stage, the organization has achieved a high level of data security maturity and has a data security-first culture. The highly automated data security platform has a thorough understanding of all data and what is sensitive, serves contextual or business insights about the data and its use, provides insight about risks and threats to the data, and is able to control and protect the data. Information security processes are constantly optimized through monitoring. The data security platform extends the governed data sharing model to partners and customers, and enables monetization models, self-service and democratization of data.

At Privacera we see prospects and customers at each stage and in some cases with elements of multiple stages, while missing other components in those same stages. This is normal, and our maturity model is intended to be a guide that can help you to identify where you are in the continuum, discover existing gaps that you may have, enable you to prioritize your approach, and help you to determine and achieve your ultimate goal: the transformational stage.



Do You Need a Security Maturity Assessment?

While not every organization will benefit from an assessment, **if you check any of the boxes below, a security maturity assessment should be a priority.**

☐ You acknowledge the need for improved data security. You have a basic level of security controls and policies but haven't invested in automation or consistent policy management across multiple accounts or data environments. You'll benefit from an independent audit to understand your cyber-strengths and weaknesses and determine what aspects of security you should focus on to increase your security maturity.

☐ Your organization is regularly audited for compliance. Most large organizations, especially those in highly regulated industries, are subject to regular audits and certifications such as PCI-DSS, SOX 2, HIPAA, GDPR, and ISO27001. Meeting compliance requirements and conducting a regular security maturity assessment provides auditors with evidence of your organization's security posture.

☐ Your organization's software and infrastructure are deployed in hybrid or multi-cloud environments. While the responsibility for security in a public cloud is shared between the provider and the customer, it's important to understand how the responsibilities are distributed depending on the provider and the specific cloud model. Assessing your security maturity across these environments where the most effective controls are being provided enables you to level-up across your integrated environment.

☐ Your organization is undergoing a digital transformation or data driven initiative. You'll need to create a baseline to ensure your security posture is at least maintained, and preferably enhanced, through the cloud modernization or data driven initiative. Then you'll need regular reassessments throughout the transformation to evaluate your security level.

Recommendations for Improving Your Data Security Maturity

Achieving the highest level of data security maturity - Transformational - isn't easy, but it's certainly not impossible if you approach it as a journey involving multiple stages that build on one another. The toughest challenge is probably just getting started.

We recommend that you begin by creating a comprehensive unified enterprise data security strategy, and adopting a Data Security Platform that can enable you to effectively execute on that strategy. The Privacera DSP automates data access, security and policy management across multiple cloud services from a single, unified interface, balancing the need for data accessibility in an efficient, consistent and transparent manner while maintaining data protection.

Embrace a risk management strategy. Identifying, assessing and mitigating security risks is critical to developing and maintaining a robust data security program (and to also address many compliance requirements). Identify your data security risks, analyzing and measuring them in relation to how your IT systems currently process, store and allow access to sensitive and business-critical information. Instead of trying to create a risk management strategy from scratch, consider building from a recognized framework like the NIST Guide for Conducting Risk Assessments.

To protect your critical data, you need to know where it is located. Use data discovery and classification technology to scan your data stores, both in the cloud and on premises, and label sensitive or regulated data by type, purpose, and classification level. Then you can prioritize your data security efforts appropriately to improve data security and ensure regulatory compliance.

Adopt a shared data security and access model, where data owners and stewards, who have a thorough understanding of their data are empowered to control who and how their data is used, while deploying enterprise data security guard rails to ensure data security and privacy rules are consistently and automatically being adhered to. This is also a requirement if you are implementing a data security Zero Trust model that includes least-privilege access control, which means limiting user access to only the data they need to perform their jobs. This provides a consistent, policy-based balance between data accessibility and data protection. Gartner predicts that 60% of organizations will adopt Zero Trust as a starting point for security by 2025.

Continuously audit activity in your IT ecosystem, including all attempts to read, modify or delete sensitive data. You need to be able to identify and assess what, where, when and how users are accessing data, including administrators and users with elevated privileges.

The Privacera Data Security Platform supports the entire lifecycle of data access and security governance with an automated, unified solution that provides enterprises with sensitive data discovery, fine-grained access control, distributed native policy enforcement, and extensive auditing and reporting... all delivered through a single pane of glass.

Want to learn how Privacera can help you achieve the highest level of data security maturity for your organization? **Contact Privacera for your Data Security Platform demo today.**

REQUEST A DEMO

CONTACT US

privacera