Data Governance

An Executive Guide

prodago
UNIFIED DATA GOVERNANCE

THIS GUIDE IS PROVIDED COURTESY OF **PRODAGO**

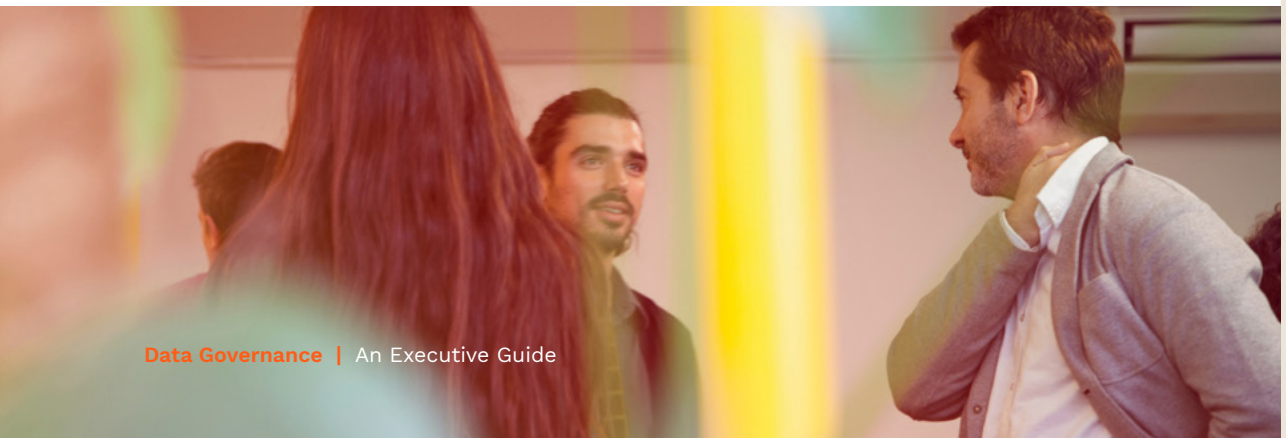
Who is Prodago?

Prodago is the company that business leaders come to when they want to operationalize Data Governance.

The proliferation and enforcement of data privacy laws everywhere, not to mention the explosive growth of data and its modern applications such as advanced analytics, has become more critical than ever for organizations to have reliable Data Governance programs. Yet organizations have long struggled with operationalizing these initiatives; most Data Governance work happens in silos, is duplicated, and is missing or ineffective. This problem endures to this day.

Prodago elevates data assets' value by offering a Data Governance Management Platform that unifies and operationalizes what otherwise amounts to fragmented and sometimes too stringent governance attempts.

Unlike other companies in this space that offer technologies built to manipulate the Data itself, Prodago focuses on the operating practices required to satisfy Data Governance demands, like policies, principles, regulatory compliance, or standards.



> **Data Governance** is the exercise of decision making and authority for data-related matters. It's a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."
>
> **David Plotkin, 2013**

What makes Prodago different?

Prodago's Data Governance Platform enhances data assets' value by facilitating a process-based management framework that unifies what has otherwise been fragmented data governance efforts.

By tying all the various data requirements under one common framework, the Platform enables the measurement and monitoring of progress for all data governance applications. The solution further allows organizations to manage their data risks proactively, clarify roles and responsibilities, increase agility and alignment when facing new data challenges, raise successful data project delivery, and create the capability to be aligned with multiple data regulations.

Prodago has also created curated content in the form of operating practices, each mapped to various laws, regulations, standards, and shared best practices typically found as part of traditional Data Governance (e.g., Data Quality). This curated content, called Accelerators, can reduce time-to-value significantly in implementing Data Governance in three areas: Data Privacy, Data Risk Management, and AI Governance.

PRODAGO IS A

Gartner COOL VENDOR

CRTA | ACTR
CANADIAN REGULATORY TECHNOLOGY ASSOCIATION
ASSOCIATION CANADIENNE DE LA TECHNOLOGIE RÉGLEMENTAIRE

Prodago offers software, professional services, and curated content to help organizations speed up time-to-value in implementing comprehensive, practical, adaptable, and operational **Data Governance**.

Please visit **www.prodago.com** for more information.

DATA PRIVACY | DATA RISK MANAGEMENT | AI GOVERNANCE | UNIFIED DATA GOVERNANCE

Table of contents

Introduction to Data Governance

Most organizations have caught on to the fact that speed is pivotal in their operations. Move leisurely, and you are yesterday's news. To stay relevant, you need to move faster than your competitors can. Your clients also expect near-instant gratification in service delivery. Satiate their appetite or lose them.

Agility helps organizations develop and achieve near exponential growth, building a fast track culture. The core component of agile service delivery is a successful digital transformation. Digital transformation is an element that makes processes more efficient through technology use.

Data technologists believe that the success of your Organization's digital transformation hinges on four main pillars; technology, data, process, and organizational change. Your Organization's digital revolution requires an in-depth understanding of novel forms of unstructured data.

Did you know...

...that close to 80% of your enterprise data is unstructured? You will also need to leverage proprietary data. On top of this, integrate all data forms and shed off bulk data that has not or will not come into use.

Data Governance in the digital transformation era

Data is the fuel for digital transformation. Its absence spells doom for revenue-generating analytics. A shortage of data robs organizations of a competitive edge. That's a plight that grounds even the most basic of business processes.

For data to act as fuel, it has to be relevant, high-quality, and readily available. That said, safety and efficiency in data usage require method and care. At every turn, there is a danger for organizations that cannot observe regulations and rules of data handling.

Your Organization's digital transformation process will only succeed if you can govern your data. As an illustration, there has to be data privacy compliance. Ensure compliance before a security breach for safety.

Mismanagement of customer data is bound to break their trust in your organization. This vice can destroy their willingness to do business with you. Sharing personal customer data with third parties could pose certain data privacy risks. It could expose your organization to non-compliance risk with Data Privacy Laws.

Businesses and governments need good Data Governance to ensure that their data creates value. Unfortunately, according to a Gartner study, **over 87% of organizations** have shallow analytics and business intelligence processes.

A majority of establishments that have common business intelligence frameworks also have no Data Governance programs. They might have heard of Data Governance and are keen on it, but do not know how to build its processes.

What is Data Governance?

The Data Management Association (DAMA) International describes Data Governance as the **control, design, and oversight** of data and its usage. Data Governance also involves the planning and management of related data sources.

The Data Governance Institute's definition of Data Governance is:

> "A framework of accountabilities and decision rights for information linked processes. This structure runs according to predetermined models, outlining the metrics of data usage."

According to David Plotkin (2013): *Data Governance is an exercise in decision-making and authority for data-related matters. It is a system of decision rights and accountabilities for information-related processes.*

Organizations should execute Data Governance according to agreed-upon models. These should outline details such as who can take specific actions, with what information, when, under what circumstances, and using what methods.

Data Governance manages the usability, availability, integrity, and security of data in an organization. It is how you handle data collected by your business. According to Hitachi Vantara, successful Data Governance requires knowing where data is located, how it originated, who has access to it, and its contents.

Effective Data Governance is a prerequisite to maintaining business compliance, regardless of whether it is self-imposed or required by industry or government mandate.

Data Governance is the mechanism by which we ensure that: the right corporate data is available to the right people, at the suited time, in the correct format, with the proper context, through the right channels. Information governance is about ensuring the same for the knowledge gathered from this data.

An outfit's Data Governance prowess is vital to its success. Organizations that manage data with high integrity enjoy benefits such as:

- **An ability to make up-to-speed decisions**
- **Profitable relationships with customers**
- **More innovations**
- **A competitive advantage in their respective industries**

Therefore, it is imperative to apply a well-managed Data Governance framework suitable for your organization's objectives and business models.

Data Governance in the wild—a scenario

Organizations can indeed get more done faster if they do not have to follow protocol. Your employees will enjoy comfortable and uninhibited data access in the absence of regulations and data handling rules.

They can quickly share client information amongst teams to enhance problem-solving. The tech team could zone in the most critical projects and leave menial tasks such as data backup for less demanding workdays.

A casual approach to Data Governance, however, has extreme consequences. An organization focusing on longevity and growth should have ground rules that man data access and use. In its Data Governance Trends Report, **Egnyte** states that the demand for a robust data management process is intensifying by the day.

Enterprises are going for self-service models that need quick file access in diverse locations. There are GDPR like laws setting in as novel opportunities in data use sprout all over the business landscape.

Organizations that lack proper data oversight processes have to create or reimagine their information control programs on this day. Do this or face emerging security threats that accompany the dynamic business environment. Egnyte says that an organization with insufficient data handling processes is at the risk of challenges such as:

- **Unstructured data sprawl as remote work takes center stage in this age of Coronavirus.**
- **The risk from unsecured WiFi networks as more employees access corporate files on their devices. 47% of these files hold sensitive management or client data.**
- **Exposure to reckless acts by employees that do not follow procedures or policies of document security.**

This eBook explains Data Governance. You will learn how to leverage **value-based data** and analytics to grow your business while minimizing your exposure to compliance, quality, and ethics risks.

One of the critical benefits of Data Governance...

...is that it helps organizations use data based on a unified understanding.

CHAPTER 1

Why Data Governance is important for your organization

Running an enterprise online exposes it to perennial cybersecurity risks. **Norton states** that the current top cybersecurity threats include **deepfakes** because of inaccurate in-depth learning data and synthetic identities.

There are also novel threats through AI-powered cyber-attacks, social media disinformation, and cloud jacking. Governments have laws that guide organizations in upholding secure systems to prevent data breaches.

Since your organization stores and runs data on its operations, clients, and employees, it has to be data security compliant.

If you are exploring ways of using Data Governance, know that security systems focus more on mitigation than preventing security breaches. Governance is as much about fixing data issues as it is about preventing them. Besides controlling and protecting data, Data Governance gives your business an edge in various ways.

Data Governance is as much about creating value from data as it is about data risk management and protection.

Reasons Data Governance is vital for your organization

Safety of data

Data by Varonis states that most companies only have **5% of their folders** under protection. The data security and analytics pioneer adds that, on average, **53% of companies have over 1000 sensitive records** open to all their employees.

Exploring ways to protect your enterprise from hackers has never been as critical as it is today. Close to 68% of executives recognize that cybersecurity threats are on the rise as per Accenture's **Cost of Cybercrime study**.

Worse is that in 2019, the global average cost of a data breach was **$3.92 million**. Additionally, upholding your business's integrity as a secure data establishment requires holding acceptable data and ethical data use.

As an illustration, the **General Data Protection Regulation (GDPR)** stipulates that organizations can only legally obtain personal data under stringent conditions. The EU information access law also oversees data management, prohibiting data exploitation, and misuse.

Failure to observe GDPR could amount to hefty penalties. Currently, the law carries a €20 million or 4% of an organization's annual global turnover maximum fine. Because of this factor, you might have to delete data from your website in line with personally identifiable information (PII).

While you may not be subject to GDPR (yet), a Privacy-by-design approach could give you excellent design and operating practices for privacy objectives. Information that can locate or identify an individual is sensitive. If your business handles such data, you must put measures governing its accessibility if only to protect the organization's reputation.

PII ensures data does not harm individuals through unethical or malicious intent or by giving false information about an individual. Such behaviors contrast from data security, which involves practices and laws that protect unauthorized access to company data and focus on protecting an organization.

68%
of executives recognize that cybersecurity threats are on the rise as per Accenture's **Cost of Cybercrime study**.

Access to reliable data

Organizations now have access to data-driven strategies and tools like never before. To leverage these technological advancements, an organization needs quality data. Excellent business intelligence can help translate insights into profits by aiding better decision making.

The **Analytics Advantage by Deloitte** shows that 49% of executives from various American, UK, and Asia enterprises use data analytics for superior decision-making. 16% of these leaders agree that business intelligence supports strategic initiatives, while 10% say it enhances business relationships. Two-thirds of these senior executives say that quality data is a critical business strategy driver.

The ideal database should have comprehensive data on the subject. For this to happen, your team should plan effective research methods to collect and index data then ensure it is relevant for your company's needs.

The integrity of data concerns its validity, that is, its intended use. The validity of the Data also concerns the need for its updating to maintain accuracy. However, collecting the correct data and failing to implement data pattern metrics can render it useless to your business. Mitigation for such requires metrics on authorized access and use, and measures to ensure its security and recoverability.

Compliance with regulations

Meeting internal and external regulations such as those set by the government or by legally instituted organizations certifies your company as an ethically established entity. Without necessary compliance certification, your business could face litigation for unlawful business practices.

To illustrate this point, over half of all small organizations have failed GDPR compliance in data processing and lawful personal data use. The **2019 GDPR Small Business Survey** shows that most business owners do not understand basic digital data security concepts such as VPNs or end-to-end encryption.

It is very easy for your organization to lose its status as a secure data organization. This scenario could lead to losses, as potential customers shun you in fear of data insecurity implications.

Over half of all small organizations have **failed GDPR compliance** in data processing and lawful personal data use.

Improves data use and accountability

Data Governance laws such as the CCPA and the GDPR are big motivators for excellent data handling behavior. These regulations, however, require more in-depth insights into the origin and form of data and its protections.

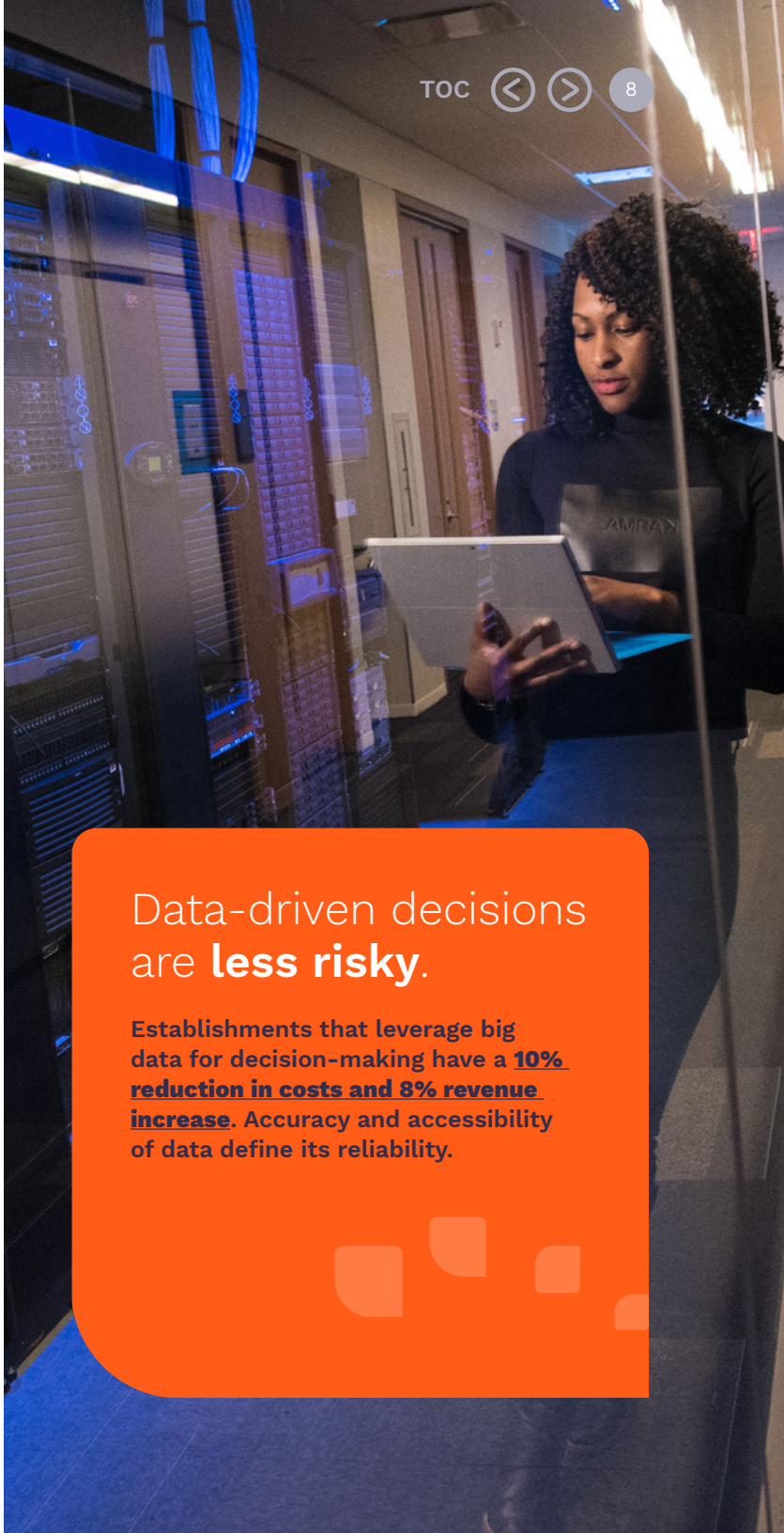
There is a need for inventory, reporting, and mitigation for data assets. Traceable Data equals trusted data and will minimize internal risk.

To this end, organizations that adhere to regulatory compliance build systems with databases whose storage can be accessed at any time. You can allow and monitor data usage, know who uses it, when, and for what purpose. With such systems, your organization is ready, open to regulatory audits, and can protect itself against data breaches and corruption.

Supports decision making

Most organizations go with strategies that have sound theories. However, organizations that excel make data-driven decisions. Information-based decision-making does away with experience, opinions, or gut feelings, basing decisions on what has worked in the past.

Appropriate Data Governance ensures data integrity, which in turn builds confidence in it by its users. With such data, your company can make concrete decisions in real-time based on facts and align them with the objectives of your business or campaigns.



Data-driven decisions are **less risky**.

Establishments that leverage big data for decision-making have a 10% reduction in costs and 8% revenue increase. Accuracy and accessibility of data define its reliability.

Instill a data-centric culture

When your company invests in intelligent Data Governance, it builds a culture that encourages the useful **collection and ethical handling of data**. However, culture (and change management) is probably one of the most challenging aspects of Data Governance.

It is a fact that the success of an organization's digital transformation initiatives rests on senior management reception of the dynamic. If your thought leaders have a data-centric mindset, this will give your Organization's Data Governance processes a **61% chance of success**.

A digital transformation culture that starts from the top enhances the sharing of information and the proper structure of its storage. It enables your company to coordinate its activities, from marketing, front office, technology, data office, compliance, risk management, and any other departments unique to your company's operations.

These practices enhance teamwork and accountability within your organization. It fosters the sharing and implementation of insights, which exponentially boosts business growth. In such an environment, everyone feels obliged to manage and share data responsibly. With such loyalty, your business can thrive and survive the murky waters of industrial espionage.

Development of training programs

For your company to benefit from Data Governance and a data-centric culture, you must invest in empowering your human resource through training and onboarding programs.

Training will build awareness within the company. At another level, it will empower your staff in their roles in implementing the company's Data Governance framework. With such skills, all players can participate in Data Governance, perform their functions efficiently, and collaborate with others.

You should not perceive data Governance as a preserve for the technical department. It should span all operations in the business from front office engagements to management activities by company directors.

With the careful and **efficient use of data**, your company can gather insights and gain an edge over the competition by using Data Governance to identify new opportunities and expedite them.

A business should view data as an asset and protect its integrity and usage.

CHAPTER 2

Critical data aspects for successful information governance

Now that we understand what Data Governance is, let us explore the aspects of data that organizations should govern. This analysis will bring to light areas that need prioritization in Data Governance. There are nine **key components** of Data Governance. They, however, fall into three major categories.

The three main categories are:

1. **Data protection**—Your Data has to be safe from loss, compromise, or corruption. You need reliable and credible data. Data protection covers Privacy or Person Identifiable Information (PII), security, and compliance.

2. **Utility**—Data has to be useful to the organization. While the quantity and quality matter, it is what you can do with it that counts. Utility covers integration, data quality, and metadata.

3. **Value**—Use the data in the right context and help manage potentially harmful implications. Value covers retention, data risks, and impact (ROI).

Aspects of data protection

Do you want to succeed in information governance? Here are some key things that you must keep in mind.

Privacy

Data privacy is not merely a compliance requirement. It is a competitive advantage and a potential time bomb to a company's reputation that lacks proper Data Governance. Customers are also more aware of data privacy risks.

Innovations for collecting big data are born every day. As a result, there is mounting pressure from customers and regulators for organizations to improve how they **manage Data privacy** and collect, store, use, and share personal information.

Sharing personal data without consent violates the General Data Protection Regulation (GDPR) law. It can cause a penalty as high as 4% of annual revenue. For example, Bounty, a UK based company, was fined **half a million pounds** for selling customer information to a third-party data broker.

In the US, you now must give consumers a "Do Not Sell My Personal Information" option, according to the California Consumer Privacy Act (CCPA). Violation of this could lead to a fine of up to $7,500 per case. In Nevada, consumers may withdraw their information from being sold.

Personal Identifiable Information (PII) of privacy protection

Today, everything is running on a system or digital program of sorts. Our lives are digitized. While this improves the ease of doing things, it also exposes our privacy to external parties.

Although data collected may not directly provide a risk, there is a need to consider the possibility of deducing personal information from it and subsequently compromising the person's privacy.

So, how do you safely share data and comply with privacy laws?

Adopting the following practices can help you avoid the risk of violating privacy laws:

- **Increasing data privacy awareness within your organization**
- **Establishing third party vetting programs**
- **Always review if sharing personal information is necessary**
- **Have a Data Sharing Agreement (DSA) with every third party**
- **Adopt procedures for the secure transmission of data**

Security

There are two aspects to consider in data security; data privacy protection and data security. Data security is about preventing unauthorized access to company information. It is an important aspect that includes prohibiting unauthorized access while maintaining direct and indirect data and privacy protection.

Sometimes, there is even the removal of data to ensure compliance. Privacy or PII protection protects individuals, for example, customers. The two aspects are similar and mostly addressed in the same privacy and security laws (GDPR, CCPA, and **PIPEDA**), but they are entirely different in scope and focus.

Compliance

Even though data protection laws have been passed in over **120 countries worldwide**, implementation is lagging. Many organizations are not yet compliant with the EU's GDPR, which is the most comprehensive data protection act so far. In January 2020, only **30% of companies** had complied with CCPA, the California privacy law.

Authorities are already enforcing the laws and imposing hefty fines for non-compliance. Many companies are still struggling to fully comply with data protection legislation because besides the cost implication, meeting every single requirement is a process. Unfortunately, if you meet 99% of the requirements and do not comply with 1%, you still fall on the wrong side of the law.

Data Governance varies per Organization. However, it is necessary to ensure compliance with the relevant regulations, policies, set of rules, or a simple request from a stakeholder. Additionally, there should be room for demonstrating, proving, or reporting compliance when required.

While Data Governance is part of the compliance solution, there are other reasons companies are non-compliant, including:

- Companies do not know which laws apply to them
- Lack of knowledge on what Data they collected
- Failure to categorize collected Data
- Lack of a precise aim for collecting and processing data
- Failure to know where the collected Data is stored
- Companies do not track how their user data is shared
- They do not know for how long they should keep data
- Failure to provide sufficient notification to users

Aspects under utility

Integration

Arguably one of the most challenging areas in Data Governance, integration, is how data sets are connected. The world is very interconnected. Datasets can also not exist in isolation, which presents a significant challenge of proper integration. Data integration, while a simple term, is quite the opposite; complex and multi-layered.

No set of data gives maximum value if it is independent. As complex and multi-layered as integration is, it determines if data is usable—if it will provide the value it should.

The good news is that the work guarantees results. The integration allows for data usability and its timeliness.

Data quality

The quality of data is one of the most common drivers of information governance. It carries a lot of weight. Understandably, everyone wants quality. However, the desired level of quality should be based on the Data's ability to serve its intended purpose.

For an organization to derive actionable insights from data, the data must be accurate (quality). Many organizations have well-documented **data quality**. However, some do not have a single source of truth or a central repository where data can be reconciled and aggregated.

The lack of structure often makes it hard to make strategic data-driven decisions because it is questioned. Failing to centralize, cleanse, augment, manage, and govern data makes it hard to interpret, control, and manage information. It also leads to an organization losing critical business data.

Metadata

Metadata is data about data. Meta means underlying definition or description. It is the necessary information about the data you want or have that makes finding and using it much more manageable. Therefore, metadata means summarizing other underlying details on data.

For example, an image's metadata would include the date it is taken, date modified, file size, etc. The ability to locate and filter confidential information makes data management easier. Metadata management is crucial in understanding the context and journey of data in Data Governance.

It helps to access crucial information that would otherwise be hidden, to enable powerful business insights from accurate analytics. However, metadata management does not operate independently; you must embed it within the Data Governance framework from the beginning.

A successful metadata management strategy increases data value for organizations. The following are the steps to creating one:

- **Adopt a metadata model that suits your business**
- **Have a metadata specialist to manage the model**
- **Gain different metadata**
- **Having a good background in your data is essential, particularly during consumption.** You can easily judge any biases and identify errors and hence, be well-informed in its use.

Metadata management does not operate independently—you must **embed** it within the Data Governance framework from the beginning.

Aspects under value

Retention

One of the critical questions in data storage is, how long should you keep data? Should you let go according to age or keep it indefinitely? Knowing how crucial data is, we hoard it even as we collect more.

Many organizations have files from ages ago that are kept for 'just in case.' As an organization, your information governance needs to be clear on what data to keep. Additionally, you should indicate how long you will keep the data, where you will store it, and how often you will access it.

Some storage spaces may contribute to lowered integrity of data, while others may increase costs. Some old data may be of value, but there is the question of cost and storage space. These are considerations why you need a data **retention** policy.

A **Data Retention Policy** is a set of rules on holding, storing, and deleting data within the organization. It helps to differentiate what is necessary or not, and how to dispose or delete data diligently.

A well-designed Data Retention Policy should:

- **Give guidelines on how different long types of data should be stored, including encryption.**
- **Show the information the organization handles**
- **Show clear authorization protocols for accessing kept Data**
- **Have clear protocols on the digital sanitization of data and physical destruction of paper**

Even though many organizations have heavily invested in data, data problems continue to grow. There are significant challenges associated with collecting, organizing, and activating high volumes of data. One cause of such challenges is that organizations are not managing data as an asset. Some have not admitted that corporate Data needs a comprehensive strategy, just like a strategic plan and roadmap.

Data risks

Data brings with it its distinct list of risks. And its use within an organization comes with accompanying threats. Currently, risks are from data breaches and emerging concerns like ethics that can tarnish the organization's reputation.

Impact or Return on Investment (ROI)

Data should provide value to the business. No, ideally, organizations should find value within data. By its nature, data is inherently valuable. Therefore, it is up to you to exhaustively explore its value and how best to harness it.

Sharing of data may work in some instances, but not in others. You can measure data's ROI by how it affects revenue, costs, and competition. Besides, its speed-to-value and impact on team-efficiency are good indicators.

Taking care of these aspects brings you a step closer to effective information governance. Additionally, ensure that your governance program is business-led but also strongly supported by Information Technology.

Stable information governance is a vital contributor to business growth through improved competitiveness and efficiency of operations.

Because Data Governance enhances collaboration, it has the potential of increasing the value of data assets.

A data strategy helps guide what Data Governance must focus on

A **data strategy** is a tool that helps to mitigate many data challenges. It is a plan to collect, store, manage, share, and use data. It is a roadmap that explains how data will support and even drive business strategy.

- Up-to-date knowledge of customer and market trends
- Informed decision-making
- Improved and better internal operations
- Better products and services
- Accurate information to help mitigate risks
- More revenue

Six elements of data strategy

A data strategy aligns data, its governance, and the people involved. This process also involves the platforms and infrastructure, and communication with the relevant sections as per the diagram.

Technology and Data Governance

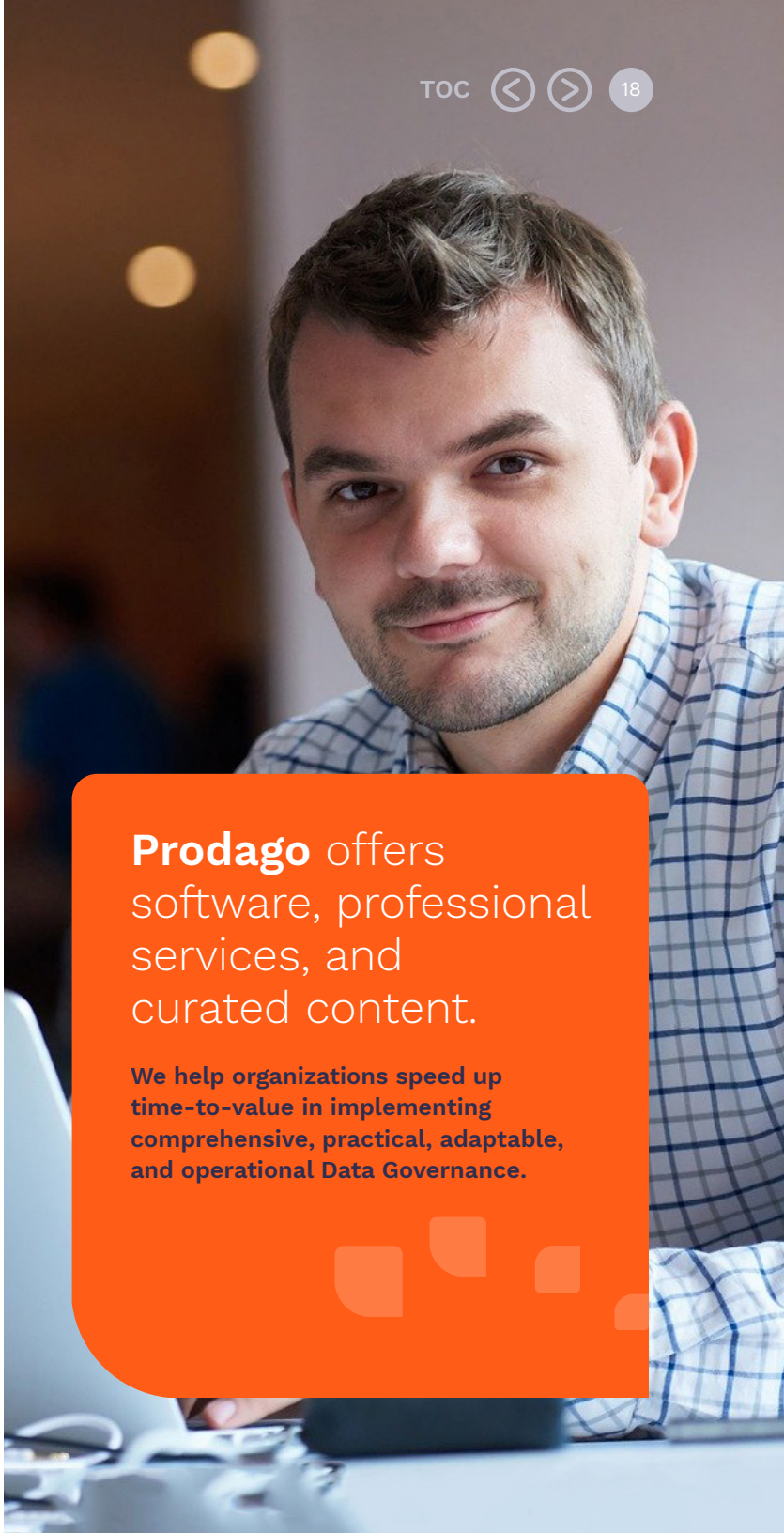
Using the right technology for Data Governance can help businesses derive significant value and drive digital transformation.

Technology helps because Data Governance streamlines processes for accessing data in an organization. Business users should be able to access data for various projects—when and how they need it.

However, the Data Governance technology used can affect the efficiency of data access processes. Out-of-date technologies can prevent an organization from leveraging data for better decision making. Businesses must adopt modern technologies in Data Governance to stay competitive and meet data users' developing demands.

One way to meet such demands is to adopt all-inclusive **data intelligent platforms**. These platforms integrate Data Governance, data quality, and data analytics, enhancing the user's control over data. Business users need to have control over data; this empowers them to serve their data needs without relying on the IT department.

Platforms like Collibra offer data intelligence, digital transformation, and self-service analytics for organizations. Even better, are unified Data Governance platforms like **Prodago**. Prodago is not just an organization that manages data. It's a solution that builds data policy alignment for organizations. Prodago will guide your C-level executives in designing, planning, and deploying effective Data Governance processes.



Prodago offers software, professional services, and curated content.

We help organizations speed up time-to-value in implementing comprehensive, practical, adaptable, and operational Data Governance.

CHAPTER 3

How to enhance data privacy in your organization

Embedding a data privacy framework into IT systems, services, products, and technologies during the inception stage defines the data privacy by the design process.

Experts advise on this as the best way of **enhancing data privacy for businesses**.

GDPR makes data privacy by design mandatory for organizations under Article 25. Failure to do this may attract a fine of up to 4% of their gross income. They also suffer damage to their reputation and lose credibility, while the aggrieved may sue the organization for damages.

Even without the legal implications of adopting data privacy by design, integrating data privacy in the design stage helps avoid the burden of adding it at later stages of the use of modern technologies as a crisis management measure.

The steps on the following pages form a guide in ways by which businesses can enhance data privacy.

GDPR makes data privacy by design **mandatory** for organizations under Article 25.

Creating a design and implementation framework

Establishments should design processes that handle all privacy related requests by clients. These can be achieved by reducing third parties and controls that do not align with the organization's perspectives. Such a process should provide opt-out options and erasure of nonviable requests.

This ensures we don't compromise the clients' privacy at any point during and after interactions and transactions with an entity, or that their personal identification information exists in dubious establishments.

Penalties for this contravention are grave, as seen in the **flagging of a German real estate firm** in October 2019 for storing tenant's data for longer than necessary; this attracted a fine of 14.5 million euros for failure to provide data privacy by design and default.

To avoid a similar occurrence, corporations should invest in services that allow users to manage their consent and individual's rights. For instance, this could enable individuals to request personal information to be deleted from a company's database and invoke their rights to access their data.

Breach management and reporting

An organization should invest in a security system that monitors and identifies external threats. It should report any vulnerabilities and data leakages in real-time. Better still, such a system should mitigate such risks.

Training of data handlers

Using technology in business requires frequent updates of procedure and policy. Their practical implementation requires relevant **capacity building to create a data-centric culture**. Therefore, all stakeholders should be trained in maintaining data privacy to not infringe on consumer rights. This training should involve all those who handle customer data and requests in the organization.

Investing in appropriate technology

Organizations should invest in applications, servers, and workstations that support anonymization, deletion, and other expectations as per regulatory data standards.

Many companies have invested heavily in this. Statistics show that many companies in the US keep investing millions of dollars annually in technology upgrades. The data supply chain should leverage such technology for an effective strategy of privacy protection.

Launching Mobile Device Management (MDM) processes

Mobile Device Management (MDM) is the management and monitoring of handheld electronic devices. It is also the security oversight of an organization's tablets, laptops, and smartphones, and is now a standard fixture in organizations. Note: this is different than Master Data Management (MDM), which we also cover in this document.

Most employees have one or more of these gadgets opening up a new area for Data Governance systems. Most organizations today have a mobile-first workforce policy and require device manager platforms to run them.

Acquiring a privacy program officer

Data privacy is significant for all organizations. Therefore, most companies have opted to appoint an officer in charge of the privacy program governance. A **report by Capgemini Research Institute** shows that two-thirds of organizations in California have hired full-time staff to implement GDPR compliance requirements.

The officer is accountable for data privacy and consumer rights matters. Such an appointment communicates the integrity of data privacy for all the members of the organization. The officer also guides the management in decision making to avoid exposure to risky situations.

The officer requires bringing other employees on the board to ensure the entire company staff adheres to this framework. We recommend training and refreshing employees' skills to handle emerging issues in their privacy protection policy framework. Such activity should create awareness in employees of the significance of privacy protection and best practices to achieve it.

A company must conduct due diligence on its third-party providers to ensure audits find them GDPR compliant in the same light. It should also regularly review the third party's compliance level to avoid compromising data privacy by such links.

Data collection and structuring for storage

Prioritize collection and indexing of personal information in implementing a privacy program. The automation of the process should utilize appropriate tools to use existing technologies, access uncategorized data, or supplement those available with other options on the market.

The organization should then invest in data discovery to create a path from data creation to consumption. This guides in the formulation of privacy regulation compliance practices.

In conclusion, businesses that **embrace data protection and privacy as a prospect** and not as a burden of compliance have more to reap when they stand out as certified for data privacy compliance. Compliant companies outperformed the non-compliant ones by about 20%, which confirms that compliance gives a business a competitive edge.

How to share data safely in compliance with US laws

Data sharing with third parties put companies and organizations at risk of contravening Data Privacy Laws. Violation of laws that regulate the sharing of personal information attracts hefty penalties as prescribed in legislation like the California CCPA and the Senate Bill of 2020 of Nevada.

Note, though, that some wrong data sharing activities arise because of oversights in conducting due diligence on third parties involved and the inability to identify phishing scams. Exposure to deceit, however, does not absolve any company of retribution for the outcome. Avoiding such implications consists of adopting **best practices in data sharing**, as outlined in this guide.

Monitoring third-party data processors

The law finds you liable if you share personal data with third-party processors who use it for nefarious intents. Considering the difficulty of confirming third parties' integrity who ask for data from your organization, the solution partly lies in signing a Data Sharing Agreement (DSA).

The DSA is a contract that complies with GDPR and states the obligations of each party. Such an agreement captures details of the nature of data involved, and the reason and method of its processing. It also states the duties and obligations of the controller.

Contracts alone, however, do not provide the security you seek. It is upon you to **conduct due diligence on third-party data processors** for integrity. And to update any existing contracts and drawing up new ones with appropriate terms. You must also monitor the activities of the third party to ensure it adheres to the DSA.

The evaluation of the data receiver should include reviewing their security systems and servers to confirm their safety. If they use a cloud, you must investigate the cloud provider's practices. Ensure it encrypts and limits the accessibility of the data. **61% of firms that audited data sub-contractors for compliance were also GDPR compliant**, which shows that they follow through with legal requirements to remain compliant.

Explore alternatives to sharing personal data

Before committing your company to an arrangement involving personal data transmission, confirm that it is the only option. However, it would also depend on the circumstances.

If you must share personal data, you can anonymize it. GDPR regards this as Data stating that it is not permitted to reveal an individual's identity or infringe on their rights. In such a situation, you do not need consent from anyone to share the data. You also avoid penalties set by GDPR on data privacy non-compliance.

Integrate data privacy awareness into organizational culture

Upholding data privacy requires accountability and a well-documented list of principles to guide its members on compliance. Documentation alone is inadequate unless the company creates awareness among its employees about data protection.

Mishandling of data by employees is a leading cause of data breach incidents because of a lack of understanding of the importance of data and its security.

Organizations need to develop a data protection curriculum to train employees and create awareness to ensure they engage in ethical data sharing practices. The training should also entail recognizing phishing data requests to enhance risk management.

Formulate procedures for secure data sharing

Secure data sharing processes require the use of encryption technology such as TLS and SSL. Some methods of data transmission, such as email, expose personal data to risks.

The organization should identify the circumstances that make sharing personal Data permissible and whether this requires consultation with a legal office, a data handling officer, or IT. Streamlining this process and training your team to adopt it will minimize the possibility of data sharing breaches.

Identify circumstances for lawful data sharing

Data privacy law outlines the circumstances identifiable as fair data sharing processes. These bases include a contractual obligation to facilitate engagement in a contract. There should be consent from an individual to access their data unless there arises a legal obligation that forces the organization to surrender such data according to the law of the land.

Personal data sharing also happens when upholding public interest or if the individual's life is in danger.

Organizations that process data should also invest in technology to identify and mitigate data breaches to avoid liability in hacking or phishing cases. They can achieve all this by observing US Privacy Laws.

Data inventory

An organization must index its data to know the nature of data it holds and the diverse levels of privacy or sensitivity of the data.

It must also draw up a comprehensive data sharing policy in maintaining the integrity of the data register.

Effective data protection—how to avoid a data breach

Data breaches continue to stalk organizations with severe legal and financial implications.

Nevertheless, many organizations have not attained data protection compliance. For example, by January 2020, only a third of California's companies had complied with the California Privacy Law (CCPA).

Give adequate notification to data users

CCPA regulations require users of data to receive a notice before the collection or sale of their data. Similarly, they should receive an updated notification on the financial benefits accrued from the transaction. The law terms it a violation if you cannot give timely notifications to users. That remains true even if you have a button to opt for the sale of personal information on your website's privacy policy.

Do not treat data sharing agreements casually

Entering a data-sharing agreement does not imply that instances will not arise when your recipient of shared data exposes you to risk. After sharing or selling users' data, follow up and ensure, for example, that the processor does not change the data or use it for other unauthorized purposes.

You could find yourself liable if the third party misuses the data. The law requires you to remain keen on not selling data when the law explicitly forbids it or without the owner's consent. When bound by such a contract, you must seek auditing of third parties involved to ensure they observe acceptable practices. You must also conduct due diligence to protect yourself against data breaches arising from phishing or hacking.

GDPR **compliance** is an exercise in totality.

An organization must meet all the audit requirements to attain compliance certification. Although organizations remain persistent in their compliance endeavors, total compliance remains elusive, as seen in the factors discussed in this chapter.

Prodago believes that organizations must operationalize data governance.

Avoid unacceptable structuring of collected data

When collecting data, regulations require that you categorize it appropriately. The structuring guidelines include classifying data depending on whether you need the authorization to manage it, and who can access that data once collected.

Categorization aids in compliance because you follow the guidelines given by different auditors on data handling. The wrong categorization also means that you cannot notify users because you lack a concrete privacy policy to guide you. Ensure you maintain a data register to monitor mapping during collection and **classify data following prevailing legal requirements**.

Do not use wrong data collection practices

Sometimes penalties arise because organizations collect excess data in the expectation that it might come in handy later. Such seemingly proactive actions are another way of breaking private data sharing laws. Good practice requires you to inform your users why you are collecting their data.

In the same way, you may unknowingly collect more data than intended through plugins or Google Analytics, which collects user IP addresses. You should be wary of adding social media plugins on your websites. You will find yourself charged in violation of the law and facing legal disputes if they collect extra data from users without their consent.

To maintain compliance and avoid breaking the law, an organization should refrain from collecting data for unspecified reasons. It should wait until it establishes the basis for collecting the data and clarify how long they will store it after use.

Ensure legal responsibility for data handling

Many people and organizations that collect data don't know the laws that govern it. Consequently, violation of the laws occurs unwittingly. The same applies to the event where users come from other countries.

Different regions have unique legislation on personal data handling requirements. For example, the US does not prohibit data sales. Still, some states like California and Nevada prohibit private information sales except where the owner allows it.

You could unknowingly violate laws from another country while transacting with users from that country. For this reason, consult legal personnel to avoid any penalties from the oversight. Remember, too, that countries keep amending their laws, so ensure you keep your team updated on any emerging issues.

Besides **knowledge of the law and implementing it on data privacy frameworks**, the organization must maintain compliance. It also calls for the team to balance information accessibility and protection to ensure it continues to serve its functions but within the law.

It becomes mandatory to invest in a data privacy strategy, including technology, to efficiently manage user data preferences. In all these, there must be a framework on Data Governance as regards its collection, storage, and dissemination.

Does your team use automation for the data handling process?

If so, you must keep reviewing the system to keep it compliant with **legal amendments and your customers' growing needs**.

Prodago will allow you to assess gaps if laws or regulations change.

CHAPTER 4

Ways to manage data utility and value to strengthen your organization

Data are the wheels that companies run on. Without adequate, concise, and factual information, companies cannot review their progress conclusively nor have reliable information to guide their goals and daily activities.

In this light, data strategy remains vital in giving your company an edge, as seen in this guide.

Understanding your data management strategy

Data strategy is a framework intended to harness data's power in an organization's growth and transformation. Have a document detailing policy on data management from the planning stage of data mapping. It starts from collecting, structuring for storage, dissemination, and all the human and technological resources involved in data handling.

The strategy should also outline the objectives of the exercise and evaluation, such as auditing for compliance. It should also have a framework to assess company revenue growth, given the **company data management and compliance measures**.

The strategy formulation process

For an organization to attain quality data frameworks for its operations and campaigns, it should break down the process into the following components, which will inform the strategy formulation process:

Data as the asset

Treating data as an asset will guide practices involving collection, quality reviews, and data management. It will dictate the life-cycle of that information within the company and its strategies for guidance. Data Governance relates to this by providing guidelines on security and privacy policies and measurement of achievements accrued from the strategy.

Transmission of data

In this component, the company creates channels of data access, sharing, and enhancing collaboration. It achieves this through an awareness program focused on encouraging all team members to use the data at their levels to improve their output.

Culture and resources

These describe the people involved not just in the company but the customers too. It entails leadership styles, the roles, skills, responsibilities of each member, and a data-centric culture to guide the team.

This component also involves the platforms used for data management and the technologies used for Data Governance. In an ideal scenario, although there must be a procedure of authorization for data access, it should not be a preserve for the IT department only. That hampers operations when staff lack access to data to complete their tasks.

Cost-benefit implications of data quality

Use data to mitigate business risk and increase profitability.

Data quality is not absolute. It should be analyzed through a cost-benefit perspective. Quality is about meeting business objectives. So, data quality is about making the data fit-for-purpose. No more, no less.

Fit-for-purpose, therefore, requires a thorough understanding of this purpose. What will the data be used for? How? What will other data will we connect to it? Every single use-case will require its list of data quality requirements. This is important.

Every new use case will require new data quality requirements, which in turn will need to be monitored and governed. Each data initiative or project must include an integral part of its requirements and the definition of what it means for the data to be of adequate quality. What is expected? If we are lucky, all the rules and monitoring mechanisms are already in place, but that is rarely the case.

Data quality is, therefore, not some elusive yes or no, you-have-it-or-you-don't thing. It is continually evolving. New use cases add new requirements, and the data itself may change. There is no such thing as implicitly assuming that a Data Management group should know how to make the information high-quality. The simply execute and implement the quality rules. Data Governance (and to some extent, the data-related projects) must define what should be done and how far to go.

Data quality should be profitable—the cost to make the data usable.

Myth: Data Quality is good or bad. We need good data.

Reality: Data Quality depends on the use case or the purpose you will use it for. What is good for one use case may be inadequate for another.

Data Quality Management is intimately linked to analytics requirements.

Outcomes of Data Quality Management

It strengthens teamwork since all the organization members must collaborate to implement data quality management practices. Through the expected transformation, everyone attains a role to play, which enhances accountability.

With concrete data at hand, the members feel confident to give insights that guide in effective decision-making. Because of the importance of data to manage personal and corporate responsibilities, the members will be keen to keep the data accurate and relevant to the organization's goals. Doing this eliminates confusion and enhances clarity from data.

Data Quality Management can propel the company towards attaining regulatory compliance. If your data follow quality guidelines, then you will have an easier time complying with regulations. As an illustration, with GDPR, ascertaining the amount of personal data within your databases is half the battle.

Since all the members are aware of acceptable data management practices and observe them, it becomes easy for the company to meet audit requirements. This compliance certificate enhances the reputation of the company as a data secure establishment and attracts more clients.

In conclusion, despite the budgetary implications reflected in human and technological resource requirements, organizations that view this as an opportunity by growth gain more in the long run. It motivates employees and encourages accountability. It also improves the quality of output through capacity building practices that enhance skills and collaboration. All these aligned into a data strategy transform the company into consistently profitable policies.

CHAPTER 5

A no-nonsense guide to creating a data strategy

Everywhere you look, there is data. The world today is suffering from an overabundance of information and the challenge of identifying credible data.

Over 80% of this content is unstructured. To this end, there are over 40 zettabytes of data out there, up from a low of 1.2 zettabytes in 2010. On this account, gone are days when the IT department would be in charge of data stored in files, databases, and servers somewhere. IT people now manage infrastructure and offer services.

The role of product management and guiding the IT department to manage data assets now belongs to non-tech people. The role of the Chief Data Officer has become crucial as organizations find it harder to manage their data torrents.

Not surprisingly, most organizations are behind the curve in data management. As per an **HBR study**, most of them use less than 1% of their unstructured data in decision-making. Over 70% of employees have unnecessary access to sensitive data.

Some corporations have hired data analysts. However, cumbered with so much content and a lack of a data strategy, 80% of them spend their time at work preparing and discovering data. Because of inefficient data strategies, the average tenure of a CDO is 2.4 years, as per a Gartner study.

Every organization needs a data strategy—a plan to use data to help them achieve their goals. You can equate a data strategy to a contract between the people who need data, like you, and those who provide you with high quality and relevant data that meets your needs.

Every organization needs a data strategy—a plan to use data to help them achieve their goals.

You can equate a data strategy to a contract between the people who need data, like you, and those who provide you with high quality and relevant data that meets your needs.

What is a data strategy?

A data strategy is a roadmap that shows how an organization comes together to gather, store, manage, and optimize its use of data. The process involves identifying how the data helps in meeting an organization's goals. And how it can give a competitive advantage.

There are seven significant aspects of a data strategy. You should define exactly how each should be delivered. These aspects are:

- **The data asset itself**
- **How we assign value and set priorities**
- **Communication**
- **The platforms and digital infrastructure**
- **Data Governance**
- **The organization, the people, and the culture**
- **Data strategy influence on Data Governance**

An efficient data strategy is key to a robust Data Governance program

Most organizations do not have Data Governance best practices because they lack a data strategy. Technology is not a limiting factor for Data Governance. Organizations that excel at Data Governance focus on the administrative processes and roles that build top-notch data catalogs.

They also zero in the practical execution of data management and quality monitoring. An all-encompassing holistic data strategy that does away with siloed data access systems will lead to the success of Data Governance processes cost-effectively.

> "A data strategy is a roadmap that shows how an organization comes together to gather, store, manage, and optimize its use of data."

The benefits of an excellent data strategy

There is a likelihood of better data transformation by having a program that can serve as guidance for more than a fiscal year to deliver better value and create the underlying sub-components efficiently.

Having a solid data strategy can help you to:

- Make evidence-based decisions
- Understand customer trends
- Know industry trends
- Mitigate risks
- Develop smarter services and products
- Have better internal operations
- Make more revenue
- Comply with regulations on data protection

Before the actual plan

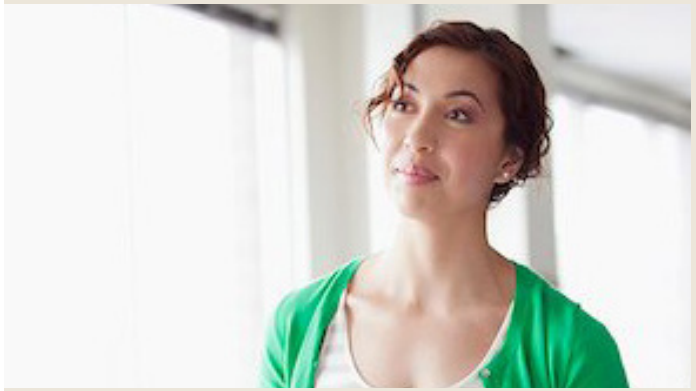
Like all good things, a sound data strategy requires adequate planning and getting all pre-conditions in place. Some things to take into consideration include:

1. **The proper buy-in.** Have everyone on board.
2. **Put together a data management team.** You need someone to shoulder the responsibility and put in the work.
3. **Involve all essential functions.** Everyone can contribute and benefit. Do not leave anyone out.
4. **Ensure data quality.** You don't need mountains of data; you need quality. Find the correct Data for the purpose at hand.

The actual plan

With the prerequisites done, here is how to build your data strategy.

- **Assess the current state** of affairs. Look at where you are now.
- **Define what you want the future to look like** considering the six components earlier discussed.
- **Identify the necessary changes** necessary to optimize the value of data activities. What stands between where you are and where you want to be?
- **Prioritize what is of most importance** to the organization if the gaps are more than you can now, refine your target to focus on crucial.
- **Create a timeline** for completing the plan.
- **Decide on a transition approach** that combines organizational constraints and priorities. Outline and communicate the plan.
- **Develop a program** that continually transitions to the future you envision. The key is to build up rather than make drastic decisions.
- **Make use of the Data Governance function** to guide the program and adapt.



The fundamental question at the core of a data strategy is this:

What problem am I trying to solve?

The data strategy should be part of the entire organizational strategy and draw on people.

Ensure that the data strategy is specific, detailed, and actionable while allowing for change when required. Data Governance, becomes the driver of the evolution of your data strategy.

How to ensure your data strategy is successful

1

The data strategy should be executive-sponsored.

A strategy with the top management's support will benefit from proper attention, assignment of the right staff, and follow-ups that ensure tangible results.

2

There should be unity and inclusivity.

The data strategy should unify since it involves the entire organization rather than one department. It also binds good collaboration and working together to improve team performance.

3

Allocate adequate resources to the plan.

For the data strategy to be successful, you must allocate enough time for the exercise and assign the right people. The focus remains on ensuring quality rather than rushing to finish developing and implementing the strategy.

4

Ensure it is holistically developed.

All the parts of the strategy need to be considered building a healthy and interconnected system.

5

Create awareness that organizational culture must be data-driven.

The success of the data strategy in the long term depends on how entrenched it is within the organization. You must invest in forums, systems, and activities that foster data incorporation into everyday tasks and ultimately make it the culture.

Developing a successful data strategy should be part of the overall organizational strategy.

You should accord it adequate resources and subject to review by a professional third party who can point out any biases and mistakes. With the business needs in mind, build towards the future you want, and ensure that your Data Governance is business-driven.

Remember...

Document the process to keep your vision within sight and help others to understand the journey you took.

While your current team may be fully on board, you will need future ones to understand its importance. They should know what informed their decisions along the way and the compromises they had to accept.

CHAPTER 6

Integrated AI governance to reduce data risk

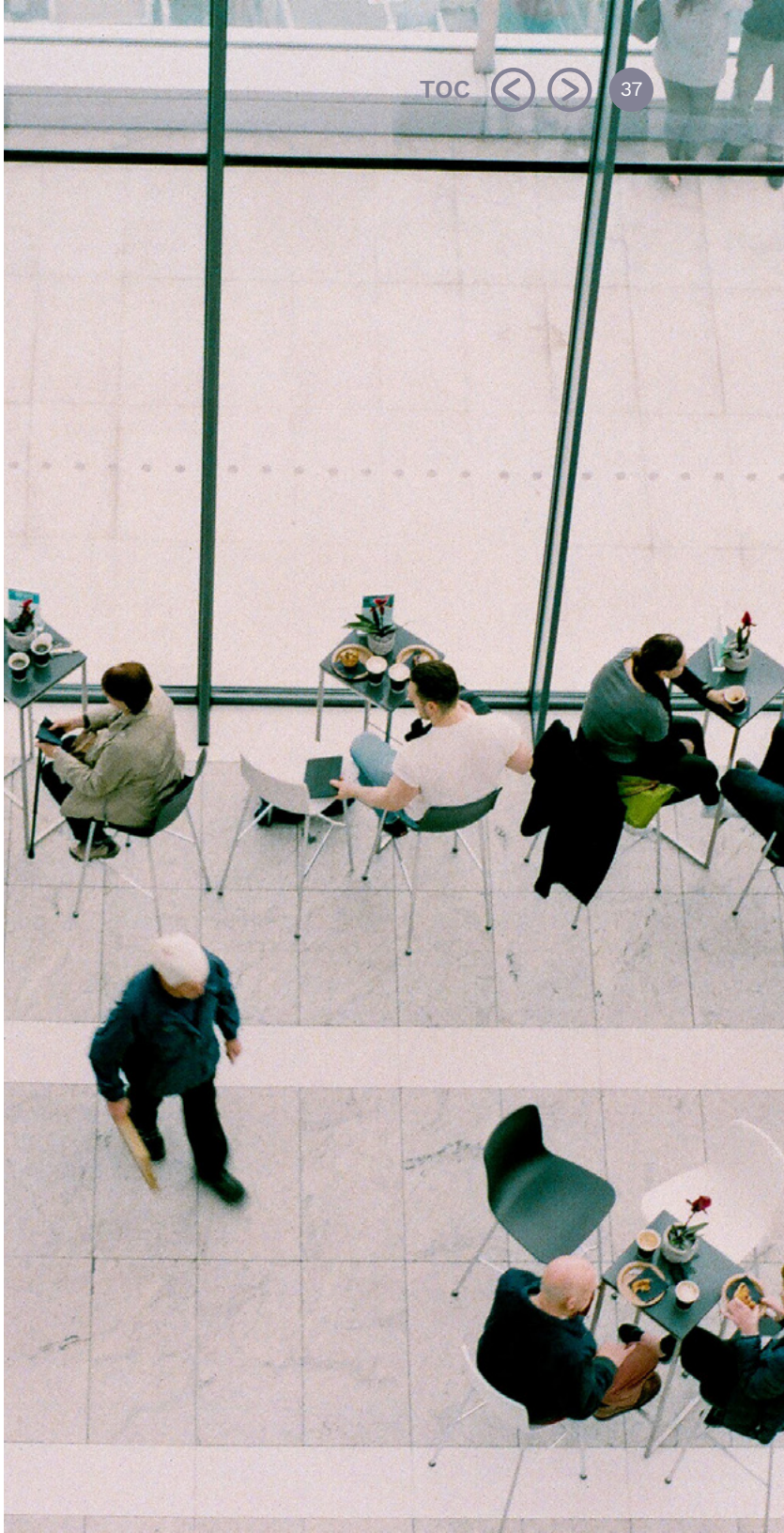
We now live in a world of working smart rather than working hard. Creating artificially intelligent machines is one way of improving efficiency.

Artificial intelligence (AI) is now essential for organizations to innovate and leverage their data assets, compete, and increase productivity. However, there are fears of the links between AI and data risks.

A simple poll by Prodago via LinkedIn in August 2020 showed that 92% of the people surveyed believed that advanced analytics increased an organization's enhanced or new data risks. They have a basis. Hackers are now increasingly targeting AI systems that handle an extensive amount of private data.

AI concerns

Today, the use of AI and advanced analytics has exploded. Organizations are increasingly applying them to all functions and processes. With the world running on data, concerns on security, ethics, privacy, and risk management are only natural. There is a need to address these concerns within a legal framework and universally. That is where data and AI governance comes in.



AI governance

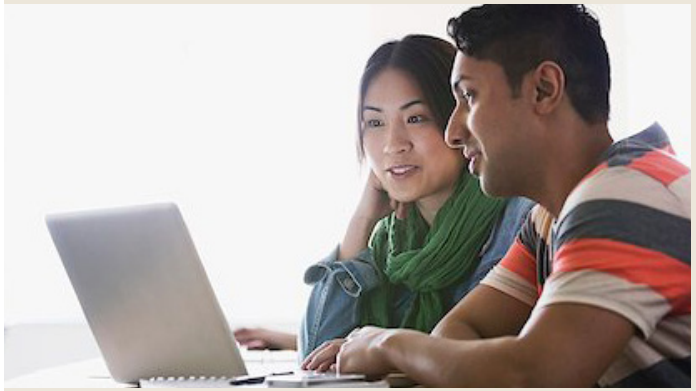
AI governance includes structuring, maintaining, and regulating actions and rules, then assigning responsibility and accountability. Artificial intelligence has to be ethical, transparent, and explainable.

Each organization defines transparency, ethical, and explainable in its unique way. That challenges the universality of AI governance. As the world grapples with addressing this challenge by developing legal frameworks, there should be more cohesion at the organizational level.

Usually, several people in an organization handle parts of Data Governance. For instance, the Chief Risk officer needs to mitigate data risks alongside all other risks. The Privacy Officer sets the legal requirements, including those aspects that touch on data. At the same time, the information officer is technically responsible for securing data.

A majority of the staff handle a certain level of data. Without proper contextual adaptation, addressing data-related concerns can burden the business resources, hence the need for its integration.

Presently, Data Governance in many organizations is mostly unorganized. Suppose each department within the organization undertakes its form of governance. In that case, there are bound to be loopholes that present opportunities for data loss and misuse.



Poll results also showed that **74%** of the respondents highlighted that they had some form of Data Governance, but that much of the data work was still carried out in silos.

Every organization needs to integrate Data Governance in all its systems and processes fully.

How to successfully integrate Data Governance

Each organization has a role to play in safeguarding its data and that of its customers. Effective integration of data is crucial in ensuring data privacy, safety, and ethics. Although many organizations use Data Governance to keep their data strategy relevant, the challenge lies in its effective integration. You can overcome this challenge by:

- **Ensuring inclusion.** For an organization to effectively integrate data, there must be an inclusive design that considers each stakeholder's needs without infringing on their rights. Once everyone is in, it is easier to make organizational changes and introduce systems.
- **Communicating effectively.** All decisions made must be well communicated. Where necessary, they should offer training to ensure that everyone understands what is going on and their responsibility. Leave no room for assumptions and grey areas.
- **Implementing purposefully.** An integrated Data Governance system must be in use throughout the organization and at all times. If well-tailored, it should serve all stakeholders appropriately and seamlessly ensure data security.
- **Accounting tirelessly.** There should be regular monitoring and evaluation of AI Data Governance across all departments. Any errors, security, and privacy breaches and misuse must be swiftly reported and corrective measures instituted.

Artificial Intelligence Data Governance is continually gaining importance in our organizations

Data is a crucial tool in building organizations and presents substantial risks to the same organization. Artificial intelligence can help improve an organizations' performance by sieving through data to present what is relevant for informed decision making.

Integrated Data Governance helps build decision rights, processes, and accountabilities within the organization for consistent data management.

CHAPTER 7

The future of Data Governance

Right now, there is way more data than ever, and it will increase. Properly managing data will be the foundation for building high-quality products.

So, what does the future of Data Governance look like? *Here we go.*

There will be an increased focus on privacy

Many people still think of Data Governance as "data privacy." That is not entirely true. However, quite a chunk of Data Governance has to do with data privacy. We have been governing Data Privacy since the 1970s when the first data privacy laws cropped up. COVID-19 has shown us we are super connected. As everyone gets online, there are even more data being shared. Therefore, there will be an ever-growing need for data privacy.

General Data Protection Regulation (GDPR) is a massive law passed recently, focusing hugely on privacy. Besides, although it has been there for a while, many people still do not understand it. They have not implemented it to the intended extent.

In the future, the cyber infrastructure's best minds will keep focusing more on data privacy to fill this gap.

Data Governance will heavily influence customer experience

There is a lot of growth in the data atmosphere. Customers expect serious companies to build technology that quickly connects with them. That should enable customers to have a tremendous and seamless digital relationship with brands.

Data Governance is critical in such digital relationships. You should know how to connect your products with your customers effectively. Linking can be omnichannel, cross-platform, via AR/VR, or even AI. To properly handle customer concerns at scale, you need to use your Data effectively.

With proper Data Governance, you ensure that you'll track usable and accurate data. Ultimately, your data strategy influences your product strategy. You, therefore, need to implement your data strategy carefully.

Data Governance programs will need to keep adapting

Do you remember how excited you were when you first heard of Snowflake? When did data lakes become a thing? What about when you first heard of a data mesh?

Yes, things are evolving fast. They will need to do so to keep up with the market. Teams will need to adapt to changing organizational structures, customer experience journeys, and product development practices, among other changes.

Every product team will have a dedicated Data Governance role

As we move deep into the 2020s, we should expect to see each product team formally creating a product Data Governance and management role.

As behavioral data gets more complicated, there needs to be more effort on personalization. Ensuring data is well maintained and handled responsibly by the product team will be critical.

The decision-making process will improve and become more seamless

With the growth in Data Governance, the build-measure-loop will accelerate. It will help the staff to ask questions and get timely answers.

It will be easier for them to predict future behavior based on quick access to past data. Over time, this will improve the decision-making process. Companies that master Data Governance will enhance minimal friction. This can give them useful insights that can turn them into industry disruptors.

prodago

To learn more about Data Governance,
contact Prodago at **www.prodago.com**