THE COMPREHENSIVE GUIDE TO DATA GOVERNANCE

THE CASE FOR DATA GOVERNANCE

Data is the lifeblood of an increasingly digital economy. Emerging technologies have helped streamline and optimize processes with new and innovative uses of data, but they also expose businesses to significant risk across a continually shifting landscape of threats and vulnerabilities. With increased implementation of artificial intelligence, machine learning, the Internet of Things (IoT) devices, robotic process automation and more, there has never been more information to harness—and to insulate from risk.

Whether they like it or not, companies large and small find themselves awash in data from many different sources, with increasingly varied formats and levels of quality and completeness. There is no choice but to confront Big Data, and the broad swath of challenges it creates, with a comprehensive data governance strategy that extends across—and, ideally, beyond—the enterprise.

BDO

SPOTLIGHT:
What Is Data Governance?

Data governance is the overall management of data availability, usability, accuracy, integrity and protection across the enterprise. The fundamental goal is to ensure that enterprise data maintains a certain level of quality to make informed decisions while ensuring that companies remain in compliance—not only for the business, but also for partners, customers, regulators and other key stakeholders.

VISION	Powering actionable insights via the optimal use of information assets
PURPOSE	Understand and govern information, its accuracy and reliability while adhering to policies and procedures and regulations.
OBJECTIVES	Ensure the data is available, catalogued and protected to be utilized for business intelligence and operations while following regulations and legal requirements.
REQUIREMENTS	Develop and adopt an enterprise-wide program that holds data custodians accountable for managing data and information to ensure that knowledge workers understand their responsibilities in protecting and leveraging data and information throughout the organization.

PRIVACY AND SECURITY IN THE FACE OF INCREASED THREATS AND REGULATIONS

Because of the potentially grave consequences of a security incident, concerns about data protection are often top of mind. Escalating cyber-attacks, including sophisticated nation-state attacks and insider threats, have shown time and again that threat actors are adept at exploiting vulnerabilities, costing businesses trillions of dollars each year. Notable privacy breaches affecting hundreds of millions of people have occurred at a number of major companies.

From a compliance standpoint, sophisticated data governance can protect the privacy of personal data and increase security to reduce the likelihood of a data breach, as well as reduce the possibility of regulatory fines associated with the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and pending legislation at the state, national and international levels.

However, avoiding a breach is only one aspect of data governance. Big Data also raises a litany of ethical concerns that demand a data ethics program to protect the rights and freedoms of data subjects. The ethical concerns include the need to reduce bias; provide notice; limit collection to adequate, relevant and proportional information; increase processing transparency and understandability; and prevent misuse or abuse of data.

Beyond the ethical considerations, if organizations don't know what relevant data they have or can't find the data they need, then it can't be used for its intended purpose or even properly protected.

IMPROVING ENTERPRISE VALUE AND BUSINESS INTELLIGENCE

Effective governance is the key to unlocking the value of data. Everyone understands that data can be an asset when exploited. It can have a direct impact on company profitability and top-line revenue growth, yield a competitive advantage and foster market differentiation. Proper governance is equally essential to increasing revenues, mitigating risk and reducing costs.

According to research from Forrester, "insight-driven" organizations are sustaining an average of more than 30% growth annually, eight times faster than global GDP. But converting data to actionable insights is easier said than done. The challenge comes with managing the sheer amount of information as Big Data gets bigger.

Businesses can acquire data easily, but determining how to wrangle it into some semblance of order presents a significant hurdle. In an era of smartphones and IoT, data not only proliferates at exponential rates, it's increasingly unstructured—meaning the information format doesn't fit within conventional databases.

A significant portion of enterprise data collected is either trivial, irrelevant with no business value or cannot be read by the systems in place. Extracting insight from data is also constrained by inconsistent naming conventions, duplicate data and incomplete records—problems that adoption of standard information models and schemas through Master Data Management can address.

According to a 2019 IDC infobrief, data workers waste 44% of their time each week on data preparation alone—time that could be better spent on analysis to yield insights. Streamlining the insight discovery process starts with getting your data house in order. Harnessing analytics more effectively can also help bring dark data into the light, yielding significant insights from information that otherwise might grow stale or remain unanalyzed.

So, data governance programs must be designed to both leverage data as an asset and fortify its protection. To accomplish this, each organization must assess its unique governance needs to determine which policies, procedures and practices are required to ensure harmonization with regulatory frameworks, while also providing the ability to build a holistic governance program to address those obligations and business needs.

SPOTLIGHT:
The Benefits of Sound Data Governance

Time to Market:

- Increased throughput due to data minimization
- Reduced time needed to design, test and implement new data-driven solutions
- Greater value derived from solutions due to enterprise-wide data integration

Business Value:

- Decreased complexity of business solutions
- Efficient use of capital as investments are coordinated
- Ability to leverage leading practices and solutions between teams

Cost and Efficiency:

- Lower risk of project failure/ cost overruns
- Increased resource flexibility across projects
- Lower support and maintenance costs due to standardization and consolidation of redundancies

BUILDING A HOLISTIC PROGRAM WITH BDO'S DATA GOVERNANCE FRAMEWORK® (DGF)

How do you build a world-class data governance program to increase agility and insight, while bolstering data privacy, cybersecurity, compliance and litigation readiness? The solutions will vary, depending on the level of sophistication of your current program, the complexity of systems throughout the organization, the nature of how you consume and use data, and the applicable rules and regulations. For some organizations, it's the Wild West, where harnessing disparate data assets could take significant time and financial investment. For others, data governance has long been a priority, and it's just a matter of updating and refining.

While there is no one-size-fits-all approach, you can generally follow four basic steps to build and maintain strong data governance: Assess, Design, Implement, and Monitor & Govern.

Assess

- Assess business priorities, data opportunities and risks
- Build prioritized data governance roadmap and compliance path

Design

- Design data governance blueprint and foundational elements such as people, process, technology, and controls

Implement

- Roll out quick wins
- Build and roll out new technologies, and business and governance processes
- Train resources

Monitor & Govern

- Establish metrics
- Assess and audit compliance to govern and continuously improve

BREAKING DOWN THE DATA GOVERNANCE FRAMEWORK TO DEVELOP A CULTURE OF ENTERPRISE INFORMATION GOVERNANCE (EIG)

All organizations want strong and effective data governance, but building this requires following specific steps to ensure success. Technically speaking, the term data governance typically refers to an IT responsibility, whereas the ability to extract business insights from your organization's data falls under the larger term of enterprise information governance (EIG). The 12-step framework detailed here lays out the requirements for building an EIG program that encompasses data governance as a key aspect.

MASTER DATA MANAGEMENT

BUSINESS INTELLIGENCE DATA WAREHOUSE

ENTERPRISE CONTENT MANAGEMENT

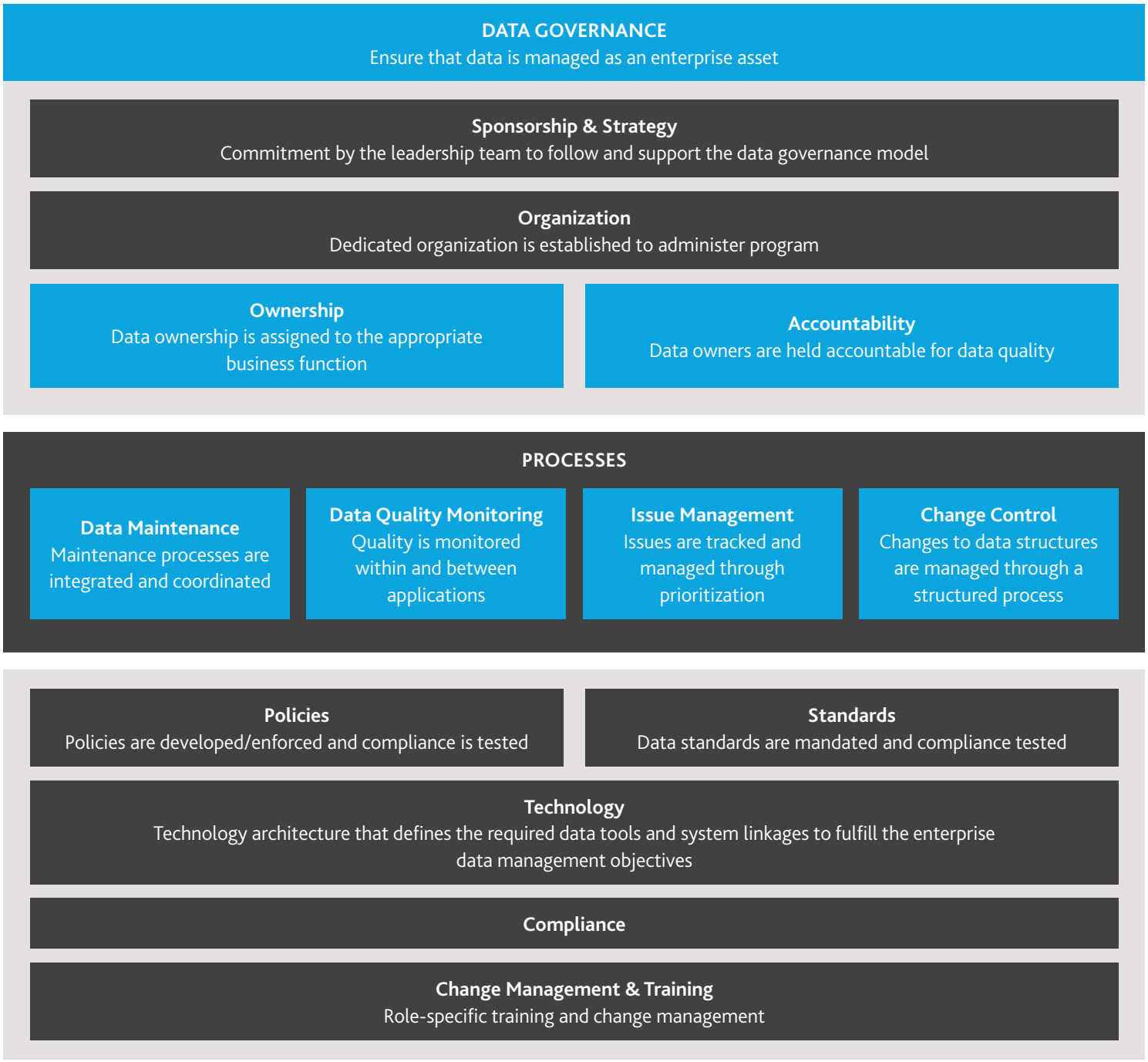
1. Organization (authority, structure, accountability)
2. Policies and standards
3. Data architecture (data models, information architecture, data quality)
4. Data privacy and protection (by design and default)
5. Data classification, retention and disposition
6. Technology and security architecture, tools and controls
7. Risk monitoring and control
8. Intracompany and third-party accountability
9. Incident management, legal holds and discovery readiness
10. Communications, training and change management
11. Legal/regulatory obligations and compliance
12. Business continuity and resilience

1. ORGANIZATION

Authority & Structure

Establishing effective enterprise information governance begins with a holistic program mandate that addresses data integration and compliance, and articulates the purpose, scope and goals of the program. It should detail the impact on productivity, operational efficiency and risk mitigation, and how these efforts align with IT practices. Specifying problems that impact your organization, how EIG will address these problems and what actions need to be taken to accomplish this will make the efforts concrete and measurable.

Forming an executive committee to lead this process helps set a vision from the top down, which encourages buy-in from all levels. This integrated initiative draws on numerous departments, and it should outline costs and expectations for the program that will require internal resources and technology expenditures. The executive committee should empower a working group with representatives from applicable business functions, and have a primary executive advocate to champion the effort in order to create and maintain momentum across the organization.

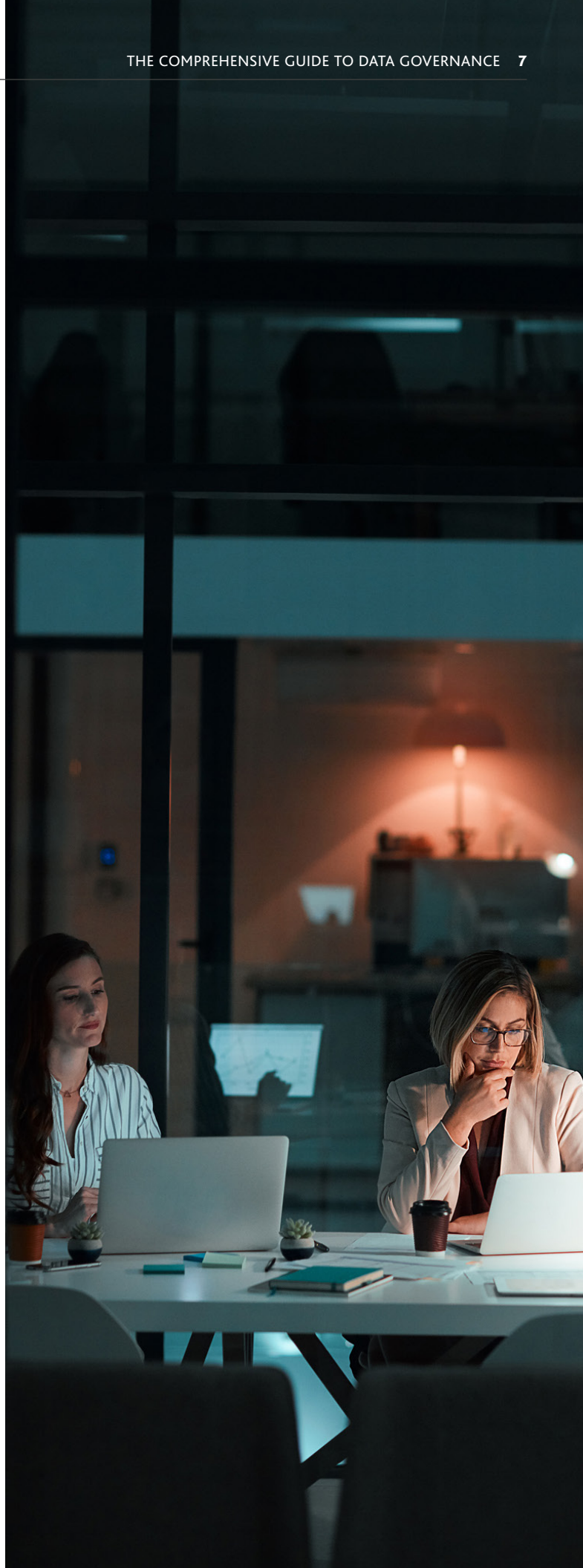


Accountability

Accountability throughout the process also helps keep the efforts on track to succeed. The structure of the governance program should assign responsibilities to different roles in your organization for completing various tasks in the process.

The RASCI (Responsible, Accountable, Support, Consulted and Informed) responsibility assignment matrix helps to specify these duties and details the relationship between the executive committee, working group and coordinator network. This sets a common vision to align data with current and future business objectives, which maximizes enterprise value in terms of operations and outcomes. The four parts of the RACI matrix are:

- **Responsible:** Assigned to those who do the work to achieve a task.
- **Accountable:** Assigned to the person in charge of ensuring the proper completion of a task or deliverable. They may delegate work to those at the "Responsible" level but need to confirm and approve that the task has been completed correctly.
- **Support:** Provides support during the implementation of the activity, process or service.
- **Consulted:** Assigned to those who provide input about a task or review completed work, often a subject matter expert in the applicable area.
- **Informed:** Assigned to those who do not have specific duties to complete a task but who should be updated as the work progresses or is completed.



2. POLICIES & STANDARDS

After outlining a clear EIG program mandate and designating teams to drive and implement it, policies and standards must be developed that incorporate business requirements, best practices and regulatory obligations into the strategy. These will help to ensure data protection, as well as standardize the use of data and technology by aligning controls and guiding processes that optimize data.

Several industry frameworks enumerate security and compliance requirements for business controls, which vary to some degree based on industry sector. These are managed by independent groups, including the American Institute of Certified Public Accountants (AICPA), Data Management Association (DAMA) and National Institute of Standards and Technology (NIST), the last of which falls under the U.S. Department of Commerce.

When evaluating the appropriate policies that your organization should implement, consider whether the policies consistently meet these primary standards:

- **Framework:** Ensure that there is a policy about the policies. Develop a policy about how policies should be organized, managed and governed, an acceptable format and when new policies should be developed and updated.
- **Governance Structure:** The policies clearly address the governance, compliance and regulatory requirements of the organization, are not created in a vacuum. Once policies are created, they need to be socialized across appropriate teams.
- **Uniqueness:** Ensure that policies do not overlap and that they are unique to one another. Reference other policies when they complement one another but ensure that policies are not redundant in nature.
- **Clear and Consistent Language:** When developing your policies, terms should be well defined. Clear and plain language should be used to make the policy easy to understand for the user.
- **Exceptions:** Whenever necessary, include an exception in the policy for circumstances when the policy might not apply or when an escalation process is required to bypass the policy.

Some key policies that are essential for an EGI program include:

- **Privacy:** The entity provides notice about its privacy policies and procedures, and identifies the types of personal information and the purposes for which personal information is collected, used, retained and disclosed.
- **Records Management:** The entity must maintain accurate, complete and relevant personal data, and it should ensure that the policy outlines specific uses for personal data along with retention, destruction and change control requirements.
- **Acceptable Use:** The organization maintains certain standards as it relates to how its employees, contractors or others are required to handle, manage and use data and information assets.
- **Mobile Device Use:** The entity implements a policy that mandates the use of mobile devices (either corporate or personal devices), establishes reimbursement policies and ensures that it references the Acceptable Use Policy.
- **Data Classification:** The entity should establish practices around how data is to be classified and apply those classifications to all types of data across the organization (either new or existing).
- **Records Retention:** The organization should require that all data types are assigned a records retention period to ensure that data is managed accordingly throughout its lifecycle and destroyed appropriately at the end of its life.

Other policies and plans that should be considered include business continuity, disaster recovery, incident response, and asset management. Taken as a whole, a set of policies and procedures that complement regulatory and industry frameworks will help establish clear processes that enable management and governance while eliminating any potential blind spots for your business.

3. DATA ARCHITECTURE

Data architecture encompasses all aspects of how data assets are collected, stored and managed throughout the organization, as well as the policies and standards governing this. The data architect, typically a designated IT professional, oversees the architectural rules, policies, standards and models to have a complete understanding of how the systems in place are linked and managed, and how these systems are constructed on the technology infrastructure.

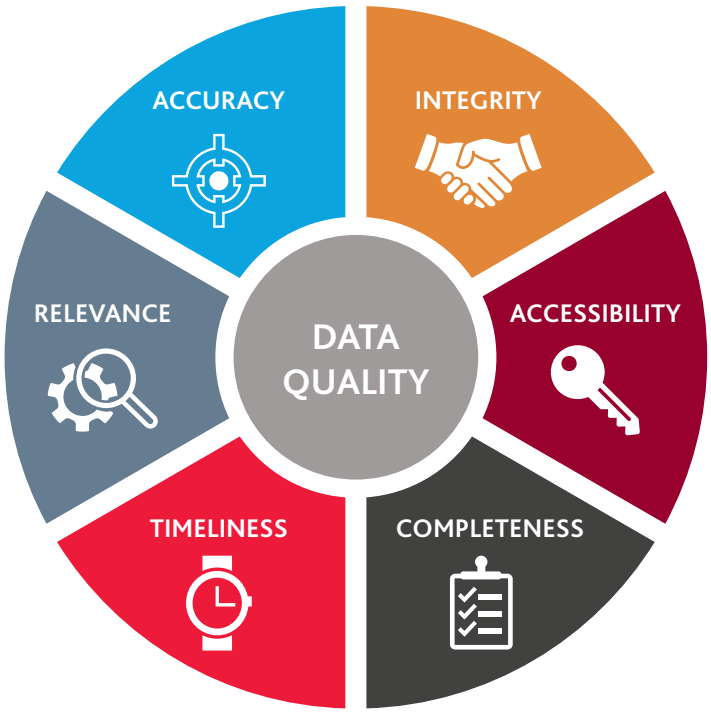
The architect can advise about the benefits, drawbacks and limitations of using different technologies, such as Cloud storage. They should also stay up to date about new advances in the field to control how any changes to the architecture—such as those prompted by organic growth or restructuring—could introduce potential problems and vulnerabilities or other downstream effects.

Data Model

An enterprise data model provides the foundation for key practices like master data management, and it can inform initiatives such as data integration. Developing the enterprise data model requires making an integrated visual representation of the creation and use of information in all databases, as well as the rules governing them. This model shows concepts and definitions for applications to provide an understanding of how data is distributed across systems.

The goal is to create a resource that facilitates communication between stakeholders on business teams and the IT staff, who are responsible for the technical and physical implementation of the model. Creating this requires a level of abstraction from application models, which are more complete, such that the data model illustrates key concepts without obscuring these with too much detail.

So, the model will show what data the architecture contains at the conceptual level of data entities, their attributes and their relationship with other entities. Through this, the enterprise data model helps identify and minimize redundancy and errors, while also enabling effective analytics and lifecycle management.



Information Architecture

Information architecture helps maintain consistency of data in both storage and retrieval. To manage enterprise data effectively requires developing models for associated metadata, search and taxonomy. This enables business teams to find and access relevant data when and where they need it. Informed by the data model, information architecture helps align the use of data for business systems across the enterprise.

A metadata model promotes consistent and complete values for associated data to systematically label accurate attributes and relationships for all entities, which will produce better search results for business teams. An effective taxonomy model allows for easy navigation of this information by grouping and classifying it to facilitate business needs. This taxonomy can extend and change as your business grows, but the data architect will need to monitor this to ensure it continues functioning properly.

Data Quality

According to research by Gartner, poor data quality is estimated to cost organizations an average of $15 million in losses per year, and for some businesses that figure is much higher. In order to help safeguard data quality, your organization should designate a data owner for each domain (e.g., sales, marketing, financial reporting). This owner acts as the primary contact who defines and communicates requirements, as well as assigns access rights for data stewards and users within the domain.

Ensuring quality data requires establishing processes and checking them for accuracy (correct and precise for the intended use), integrity (valid and free from collection bias), accessibility (available to those with permission), completeness (comprehensive and without gaps in necessary information), timeliness (informative during the timeframe of use) and relevance (needed for a business purpose).

In addition to these processes, determining the metrics to confirm data quality will help to monitor these critical efforts and see that the data effectively serves its business purpose. The data owner should work with the data manager—who is often an IT professional that oversees the infrastructure and confirms access protections—to check the established metrics for consistency and confirm that quality is maintained.

4. DATA PRIVACY & PROTECTION

The public outcry from big-headline data breaches and scandals has forced regulators' hands around the world. More than a year into the EU's GDPR legislation, and with CCPA looming, the era of indiscriminate collection and manipulation and distribution of personal data is ending. One aspect of GDPR, Privacy by Design, has helped make consumer privacy a priority in systems that collect and store personal data. While industry privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), are well established, stakeholders on every side of GDPR and the upcoming CCPA are still working out the details and nuances.

As companies and regulators continue to determine how personal data can be used, a parallel conversation has emerged about how it should be used. Compliance with industry standards and regulations is arguably the bare minimum. Privacy and cybersecurity initiatives need to go beyond what a company is required to do. Your organization should also adopt a mindset of thoughtfully measuring the business need for consumers' data to support operations. Taking a "how would I feel" approach to this can provide consumers with reasonable expectations as to how their data will be used, processed and shared.

To help safeguard data privacy and install proactive protections, best practices include:

- Records: Develop a Records of Processing (ROP) register and rank associated risks, safeguards, retention and data flows.
- External Notice: Update external notices to include details on collection, use, retention, disclosure and disposal of personal information categories.
- Internal Privacy Policy: Develop internal-facing privacy policies incorporating proportionality, adequacy, minimization, purpose or use limitation, storage limitation, accuracy, completeness, security, confidentiality, integrity and accessibility requirements.
- HR Policy: Develop job applicant and employee policies that include details of the lawful basis, data processing and individual rights.
- Choice & Consent: Establish policies and mechanisms for opting in and opting out of data processing, sale, marketing contact and cookies.

7 PRINCIPLES OF PRIVACY BY DESIGN

1. **Proactive not Reactive; Preventative not Remedial**
   Anticipate and prevent data privacy incidents and address privacy risks before they materialize.
2. **Privacy as the Default**
   Privacy is built into the system by default, requiring no action on the part of the individual to protect their privacy.
3. **Privacy Embedded in Design**
   Embed privacy in the design and architecture of IT systems and business processes as a core functionality.
4. **Full Functionality: Positive-Sum, Not Zero-Sum**
   Privacy protections should not and do not need to come at the expense of security or functionality.
5. **End-to-End Security & Lifecycle Protection**
   Embed strong security measures throughout the information management lifecycle, from cradle to grave.
6. **Visibility and Transparency**
   Provide assurance to all stakeholders—users and providers—that data is being used in accordance with stated principles and objectives, subject to independent verification via a compliance and redress mechanism.
7. **Respect for User Privacy**
   Take a user-centric approach to data privacy, prioritizing individual privacy interests and communicating effectively.

5. DATA CLASSIFICATION, RETENTION & DISPOSITION

Data Classification

Overall, effective data management can be realized by establishing consistent practices to ensure data quality throughout the lifecycle, while maintaining processes for minimizing data in accordance with privacy and retention requirements. To prepare for this, data should be standardized in a consistent format, to help with classification and collaboration across business lines as needed.

Key elements of data classification include:

- Establish a standard syntax or "data glossary" for cataloging structured and unstructured data (e.g., metadata).
- Establish rules and policies for how data is accessed, stored, retained and disposed.
- Set metrics for measuring the quality and usability of data assets.
- Diagram current data flows and track data lineage.
- Have a clear understanding for current and future data and analytics use cases.
- Develop an adaptable data reference architecture.
- Determine data storage needs to facilitate information sharing and data integration.

To maximize the full value of enterprise information, you need to be able to extract insights from both structured and unstructured data, in combinations that are seldom predefined. More sophisticated analytics and machine learning initiatives will require a cohesive architecture that integrates both data and analytic applications.

Records Retention & Disposition

Every organization has distinct statutory and regulatory requirements relating to records management. Organizations must view their data disposal policies and procedures not just in terms of these requirements, but also in the context of their broader EIG program, with an eye toward increasing efficiencies and data protection.

The journey of data from creation to disposition requires careful handling and monitoring. The data life cycle has numerous steps and varies depending on industry, but it can be summarized generally as: collect, process, store, use, share, archive, destroy. And responsible data management must implement quality control measures across each step of the life cycle.

Key records management principles to consider include:

- Determine who is accountable and responsible for maintaining retention schedules.
- Align records schedules with business and operational practices, as well as legal obligations.
- Ensure that the record keeping program protects personal records and data.
- Identify and articulate potential legal concerns due to non-compliance.
- Document organizational practices and ensure that data is properly categorized, including public, private, confidential and company secrets.
- Determine safeguards when required during the disposition processes—including shredding documents and destroying electronic assets in the proper manner.
- Update and maintain current retention schedules and policies, and ensure that retention is enforced across the organization.
- Ensure that there is transparency about the organization's data retention practices, both internally and externally.

"Data hoarding" of files that provide no business or historical value, duplicative information, and "dead" data that hasn't been used or accessed in years do not just increase data security risks, these also make identifying and accessing relevant information much more time-consuming.

Implementing a data reduction strategy as part of the ordinary course of business is essential to reducing data volumes to manageable levels. Organizations will need to leverage a mixture of data minimization, deduplication, and more sophisticated AI-driven data analysis to limit data collection and retention to only the most pertinent and useful information.

6. TECHNOLOGY & SECURITY ARCHITECTURE, TOOLS & CONTROLS

In monitoring data risks, a threat-based approach to cybersecurity helps identify the vulnerabilities that a cyber-attack would likely try to exploit, and outlines measures to secure those vulnerabilities. This takes a forward-looking view and uses predictive analysis of your organization's unique threat profile to identify at-risk areas and protect against the most likely types of cyber-attacks that could occur.

This threat-based approach requires a multipronged strategy and a range of proactive steps, including independent assessment and penetration testing, software encryption and multi-factor authentication, a security patch management program, and managed detection.

An independent firm can assist with these advanced diagnostics and help patch any vulnerabilities. They can also perform a red-team security test that mimics a threat actor and searches for any holes in an organization's upgraded cybersecurity defenses. Ongoing cybersecurity training for staff helps keep these practices top of mind as well.

TO OUTSOURCE OR NOT TO OUTSOURCE

Outsourcing data governance and privacy responsibilities, whether short-term or long-term, can provide significant savings and value for an organization, while also ensuring security and minimizing risk. But it is crucial to determine if and how such a solution fits your organization's needs. Some key questions to consider include:

- Do you currently have an automated internal system for data analytics and processing that is designed by a data scientist? Optimizing such a system without experience in the area presents significant challenges that can consume time and money unnecessarily.
- Is this system accessible and optimized for business users, or does it require additional processing, training and/or some data management background? It is inefficient if business personnel need to coordinate with IT for access and analysis.
- Do you currently have data management experts on your team, or is the work of maintenance and quality control being executed by untrained personnel? Leveraging outsourced expertise can increase efficiency and quality while making internal resources available for more tasks.
- Are you applying data governance to all facets of your organization (marketing, customer service, et al.)? Leveraging data in a secure and consistent manner can yield significant results across multiple initiatives.
- Is the data management program set up to account for privacy compliance? Online reporting and automated workflow help ensure your organization can fulfill current and upcoming regulatory timing requirements.

For organizations that lack the in-house expertise and resources for robust data governance, outsourcing presents the opportunity to enhance security, mitigate risk, reduce costs and harness the full power of that data across the entire business.

7. RISK MONITORING & CONTROL

Assessing your organization's data protection risk profile involves numerous aspects, including determining which employees have access to which systems and whether tighter restrictions need to be placed on employee access controls. It is estimated that 43% of all data losses occur at the hands of internal actors, so limiting access to data can be a basic but effective method to mitigate risk. Overall, a cybersecurity risk assessment must review all current policies and operations, identify potential issues and then prioritize remediation initiatives.

Some data breaches that affected tens of millions of people continued unnoticed for months or even years, such as with Yahoo! (2013-14) and the U.S. Office of Personnel Management (2012-14). Because valuable data records are stored across numerous systems, organizations must establish effective controls and continuously monitor risk 24/7/365. Otherwise, they leave themselves vulnerable to threats and intrusion on an ongoing basis, and they may not even know when a breach occurs.

As part of your organization's processes, create a mechanism to see a "single view of risk" through consolidating data and establishing key risk indicators (KRIs), which can be just as important as key performance indicators (KPIs). Considering the drastic effects of a breach, these are vital tactics to help strengthen monitoring and mitigate risk. New technology makes monitoring and trend analysis an easier practice to implement as well.

8. INTRACOMPANY & THIRD-PARTY ACCOUNTABILITY

Organizations need to have a clear understanding of all third-party vendor relationships, and then map those relationships against data flows to understand what level of access vendors could have to their data and information systems.

Vendors' data governance policies and procedures should be closely examined, as should their compliance practices. The vendors then must demonstrate a thorough understanding of their direct requirements, as well as your organization's responsibilities—and the consequences of running afoul of those rules. Existing contractual obligations may need to be modified to include all compulsory details and terms.

The vendor management process does not end after the contract is signed. Successful vendor risk mitigation is a continuous process—not something that is simply conducted upfront and then forgotten. Your organization must diligently monitor risk and review internal controls with service providers to ensure they remain compliant and prepared for new threats in an ever-changing environment.

Third-Party Assurance via SOC Attestation

Undertaking System and Organization Controls (SOC) attestation provides numerous benefits. It can help build trust with current customers and prospects, as most large organizations partner with hundreds or even thousands of outside service providers, so auditing each vendor one by one would be time-consuming and inefficient.

SOC attestation also validates the risk management model and proves business value, because company stakeholders and prospective investors look for it as a good measure of corporate health when they contemplate investing or plan an exit strategy. Moreover, it can help to find and close the gaps in controls. In 2017, the AICPA developed description criteria for a new SOC attestation, SOC for Cybersecurity, further enhancing the value and scope of SOC reports.

9. INCIDENT MANAGEMENT, LEGAL HOLDS & DISCOVERY READINESS

In a world where attempted cyber-attacks are not a question of "if" but "when," every organization must be prepared to respond quickly and limit the impact of a breach. The handling of data breaches is now closely monitored by regulators at the state, national and international levels. Failure to contain the threat and notify customers and regulators in a timely manner can result in significant financial penalties.

Critical aspects of developing sound incident response and data breach notification processes include:

- A consistent and current incident response program that includes policies, procedures, roles and responsibilities, as well as communications plans
- Consistent definitions across the organization that includes the definition of an event, an incident or a breach
- Direction to teams that an incident has occurred, and the steps required if they suspect this warrants further investigation
- Contracts with outside counsel, forensic and cyber-investigative experts, as well as PR firms that specialize in this area
- Internal training to identify suspicious activities
- Steps to minimize further threats or exposures, and a process to remediate the current situation
- Notification practices, such as outsourced data breach notification companies or credit monitoring contracts after a breach has occurred
- The ability to recover systems back to their functioning state to minimize impact to the operations of the business and its customers

Beyond sound practices for incident response and breach notification, your business must ensure it is prepared for litigation and discovery before these needs arise. Many organizations mistakenly view information governance and e-discovery as two distinct functions, but in fact they are two sides of the same coin. If data sets are too vast and disorganized, it becomes tedious and costly to process and analyze them—or they could be missed altogether during the discovery process. Implementing a data retention and destruction strategy as part of the ordinary course of business prior to when the duty of preservation kicks in is essential to reducing data volumes to reasonable levels.

10. COMMUNICATIONS, TRAINING & CHANGE MANAGEMENT

Training and change management are critical to performing a successful roll-out of any program, and EIG is no exception. Firm-wide communication detailing key aspects of the governance strategy and program helps ensure understanding and adoption of the necessary practices.

Unfortunately, many EIG initiatives struggle with implementation and are met with resistance, so the initial planning steps are crucial. The strategy should set clear goals supported by consistent communication, which helps convince senior managers across the organization about the value of implementing an EIG program. It should also plan the implementation in stages to avoid change fatigue for staff, and set up processes to support the tools that will be leveraged.

Although implementation plans vary widely, standard steps that can be employed in any organization include:

- **Pilot:** Test the process, policies or procedures with a small group.
- **Roll-out:** Once you conduct the pilot, begin to roll out the program to all employees.
- **Training:** Immediately following your roll-out, ensure employees are trained in a timely manner with ongoing testing and positive reinforcement to instill behavioral change.
- **Governance:** Monitor progress against the program, adjust as needed and update accordingly. This will help to ensure that the program is fluid and can meet the organization's business, regulatory and legal needs.

Ultimately, every employee must understand that they are a steward of organizational data and accountable for its proper handling.

11. LEGAL/REGULATORY OBLIGATIONS & COMPLIANCE

Businesses are in new regulatory territory as U.S. and international lawmakers create a governing framework for emerging digital risks. Today, there are more than 100 federal and international data privacy and protection laws, each with their own set of requirements regarding how data is collected, used, retained and safeguarded.

However, data privacy is just one facet of the current regulatory environment. From financial regulation, such as Dodd-Frank and the Bank Secrecy Act, to environmental health and safety reporting rules, to industry-specific frameworks, organizations face a barrage of disparate compliance requirements regarding records retention and information assurance. So, sound data governance must remain responsive and align with all relevant legislation.

Under the Federal Rules of Civil Procedure (FRCP), once a party "reasonably anticipates litigation," it has a duty to preserve electronically stored information that may be relevant to a discovery request and place it under a litigation hold, requiring the suspension of routine data deletion or destruction procedures. Failure to preserve relevant data may result in claims of intentional destruction of data or allegations of a lack of cooperation that could lead to court-mandated sanctions.

Data Divestitures in CFIUS Mitigation

Data divestitures have become a frequent component of transactions subject to CFIUS mitigation terms. Exactly what is to be divested is unique to each deal, but usually it must be done in a manner that it is irretrievable.

Businesses have many sources of data that may be captured in one system and disseminated within the organization in various ways, including through automated backups, and by employees via email systems, personal network share locations and local computers. This can create a cascading effect in that multiple systems, not just the data input system, need to be considered when divesting protected data. A holistic, top-down approach to data governance is recommended to examine both the source of data origin and an exhaustive trail of every possible location the data could exist, which helps ensure compliance with requirements for all applicable data being irretrievably deleted.

National Security and CFIUS Compliance

From a national security standpoint, U.S. organizations that own, maintain and operate components of U.S.-based "critical infrastructure"—defined as "a system or asset, whether physical or virtual…vital to the United States"—must ensure their assets are protected from ongoing physical and cyber-related threats, in order to meet national security compliance requirements developed by the National Industrial Security Program (NISP). Avoiding a national security letter, or complying with one, requires an intricate knowledge of an alphabet soup of regulations, including FOCI, ITAR, DFARS and more.

The complexity of navigating these regulatory processes will continue to increase in tandem with international investment. A critical element of national security compliance is the involvement of the Committee on Foreign Investment in the United States (CFIUS). Chaired by the U.S. Department of the Treasury, this interagency task force is responsible for the review of foreign direct investment that could result in the control of a U.S. business or U.S. critical infrastructure. CFIUS is also responsible for reviewing the impact these transactions could have on national security.

Companies brokering a deal with a foreign entity must be cognizant of how the transaction may impact the reliability, availability and integrity of their resources, as well as transmissions and underlying protected information, and the potential applications of their technologies by their acquirer.

12. BUSINESS CONTINUITY & RESILIENCE

In order to minimize the potential effects of a data breach or cyber incident, your business must develop and test plans for business continuity and disaster recovery. Establishing a data loss prevention (DLP) program is a key component of this. Comprised of administrative, technical and physical controls to protect an organization's data, a DLP program forms an essential component of EIG and takes an umbrella approach to guarding against data loss.

Beyond just automated backups, an effective DLP program can monitor all systems, apps and databases for data use patterns, threats, vulnerabilities and privacy violations. This becomes much easier to implement if measures have been taken to ensure data quality and records management as part of the EIG program.

LOOKING FORWARD

Eventually, every business process should be data-driven, with analytics and robotic process automation embedded throughout. This includes core processes (e.g., customer service, purchasing), management processes (e.g., budgeting, risk management) and support processes (e.g., HR, accounting). The journey to operationalizing these analytics across the enterprise starts with holistic data governance. After all, insights are only as good as the information they're based on.

As businesses become increasingly data-driven, striking the right balance between data security, data access and data quality is more important than ever. Those who figure out how to get it right will find themselves a step ahead of the competition.

Developing mature data analytics capabilities to supplement data governance initiatives can help your organization by:

- Identifying customer and market trends accurately and more efficiently
- Enhancing internal audit functions and fraud prevention
- Bridging departmental data into cohesive dashboards
- Strengthening the overall enterprise's information governance program with improved data quality
- Allowing for modifications in regulator reporting as requirements change
- Strengthening privacy and data protection through the identification and masking of protected data

CONTACT

KAREN SCHULER
Principal, National Governance, Risk & Compliance Leader
301-354-2581
kschuler@bdo.com

MARK ANTALIK
Managing Director, Information Governance & Privacy Leader
617-378-3653
mantalik@bdo.com

NEBIAT KIDANE
Director, Governance Risk & Compliance
703-336-1522
nkidane@bdo.com