The IBM Data Governance Council Maturity Model: Building a roadmap for effective data governance

Introduction

It's been said that IT is the engine for growth and business innovation in the 21st century, and data is the gasoline that fuels it. And while data is undeniably one of the greatest assets an organization has, it is increasingly difficult to manage and control.

From structured to unstructured data – including customer and employee data, metadata, trade secrets, e-mail, video and audio – organizations must find a way to govern data in alignment with business requirements without obstructing the free flow of information and innovation.

For many organizations today, data is spread across multiple, complex silos that are isolated from each other. There are scores of redundant copies of data, and the business processes that use the data are just as redundant and tangled. There is little cross-organizational collaboration, with few defined governance and stewardship structures, roles and responsibilities.

Businesses want to leverage information for maximum performance and profit. They want to assess the value of data as a balance sheet asset, and they want to calculate risk in all aspects of their operations as a competitive advantage in decision-making.

It is for these reasons that data governance has emerged as a strategic priority for companies of all sizes.

Data governance is a quality control discipline for adding new rigor and discipline to the process of managing, using, improving and protecting organizational information. Effective data governance can enhance the quality, availability and integrity of a company's data by fostering cross-organizational collaboration and structured policy-making. It balances factional silos with organizational interest, directly impacting the four factors any organization cares about most:

- *Increasing revenue*
- *Lowering costs*
- *Reducing risks*
- *Increasing data confidence*

Many companies are just learning to examine their data governance practices, and searching for industry benchmarks and common frameworks to ground their approach. The IBM Data Governance Council Maturity Model is a breakthrough initiative designed with input from a council of 55 organizations to build consistency and quality control in governance through proven business technologies, collaborative methods and best practices. This white paper will describe the Data Governance Council Maturity Model and explain how organizations can leverage it to help them govern the use of data more effectively.

Data Governance Council Members	
Organizations	
Abbott	Key Bank
ABN Amro	Lumigent
AirMagnet	MasterCard
Alltel	Merrill Lynch
American Express	Monaris
Application Security	Novartis
Axentis	Nordea Bank
Bank of America	Northwestern Mutual
Bank of Montreal	OpenPages
Bank of Tokyo/ Mitsubishi	Organizational Policy Inst.
Bell Canada	Paisley
BITS Financial Services Roundtable	Principal Financial Group
Cadence Design	Regions Financial Corp.
Citigroup	RiskWatch
City of New York, FISA	SecNap
Continuity Software	Semantic Arts
Danske Bank	SPS Security
Deutsche Bank	TIAA-CREF
Discover Financial	Tizor
Equifax	TeliaSonera
Fannie Mae	Valid Technologies
Freddie Mac	VP Securities Services
Guardium	Washington Mutual
Huntington Bank	Wachovia
IBM CIO Office	The World Bank
Intellinx	ZANTAZ
Academia	
North Carolina State University	
Nova Southeastern University	
Bucerius Law School	

A forum for data governance

With high-profile data breaches and incidents skyrocketing, the challenge to protect and manage data has become a universal concern for organizations. To help better understand the emerging space, IBM created a leadership forum in November 2004 for chief data, security, risk, compliance and privacy officers concerned with data governance issues. Since then the IBM Data Governance Council has steadily grown to comprise nearly 55 leading companies, universities and Business Partners, including large financial institutions, telecommunications organizations, retailers and even public sector governments.

With a common forum for data governance practitioners to explore challenges and solutions, the Council has been instrumental in developing benchmarks, best practices and guides to successful data governance. Working together, the members of the Council have identified the top governance challenges facing organizations, including:

- *A lack of cross-organizational data governance structures, policy-making, risk calculation or data asset appreciation, causing a disconnect between business goals and IT programs.*
- *Governance policies are not linked to structured requirements gathering, forecasting and reporting.*
- *Risks are not addressed from a lifecycle perspective with common data repositories, policies, standards and calculation processes.*
- *Metadata and business glossaries are not used to track data quality, bridge semantic differences and demonstrate the business value of data.*
- *Few technologies exist today to assess data values, calculate risk and support the human process of governing data usage in an enterprise.*
- *Controls, compliance and architecture are deployed before long-term consequences are modeled.*

In addition, the Council members collaborated to define a common benchmark of observable and desired behaviors that every organization can use to evaluate and design their own data governance programs. What emerged was the Data Governance Council Maturity Model. Based on insights and benchmarks from their own practices, the Data Governance Council Maturity Model helps define the scope of who needs to be involved in governing and measure the way businesses govern data uses, such as sensitive customer information or financial details. It enables organizations to:

- *Assess where they currently are in terms of governance, where they want to be and the steps they need to take to get there.*
- *Gain an informed, objective, documented assessment of the maturity of their organization.*
- *Objectively identify, uncover, highlight and detail the strengths and weaknesses of their data management capabilities.*
- *Gain knowledge of existing capabilities and levels of understanding around these elements.*
- *Challenge internal assumptions and normalize methods for continuously examining business processes and IT practices.*
- *Benchmark future levels of organizational performance and develop a roadmap to get there.*
- *Document and centralize reference information that should reside across the organization to govern more effectively.*

Maturity models: An overview

Developed by the Software Engineering Institute (SEI) in 1984, the Capability Maturity Model (CMM) is a methodology used to develop and refine an organization's software development process. The CMM describes a five-level graduated path that provides a framework for prioritizing actions, a starting point, a common language and a method to measure progress. Ultimately, this structured collection of elements offers a steady, measurable progression to the final desired state of fully mature processes.

At Maturity level 1 (initial), processes are usually ad hoc, and the environment is not stable. Success reflects the competence of individuals within the organization, rather than the use of proven processes. While Maturity level 1 organizations often produce products and services that work, they frequently exceed the budget and schedule of their projects.

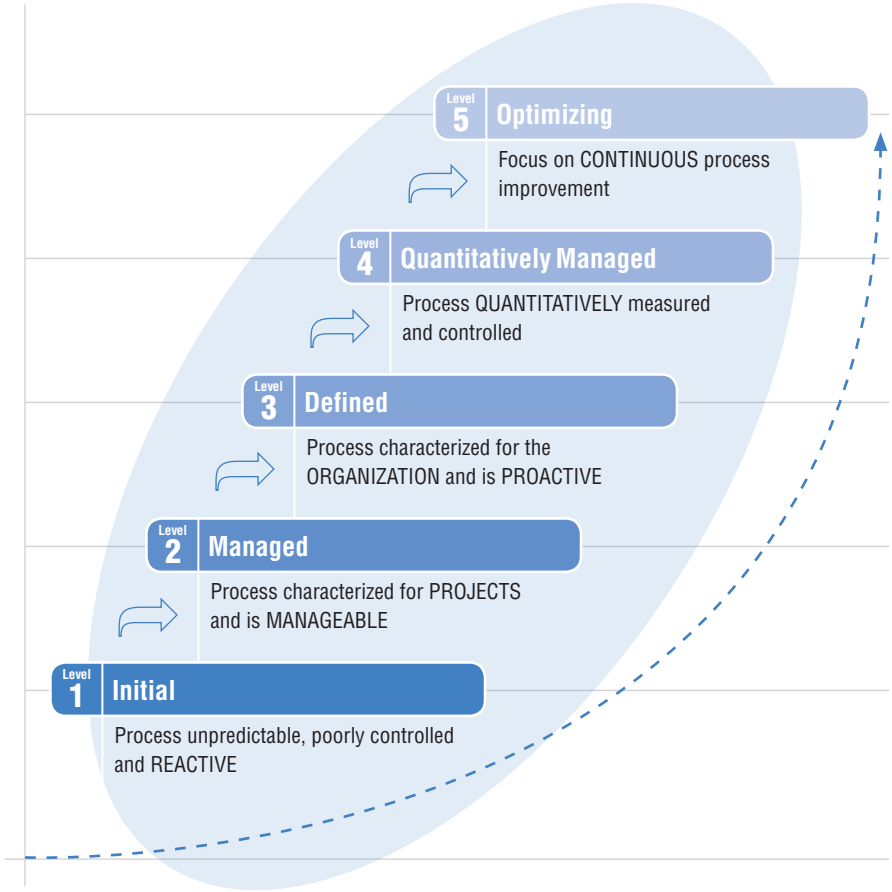
At Maturity level 2 (managed), successes are repeatable, but the processes may not repeat for all the projects in the organization. Basic project management helps track costs and schedules, while process discipline helps ensure that existing practices are retained. When these practices are in place, projects are performed and managed according to their documented plans, yet there is still a risk for exceeding cost and time estimates.

At Maturity level 3 (defined), the organization's set of standard processes are used to establish consistency across the organization. The standards, process descriptions and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit.

At Maturity level 4 (quantitatively managed), organizations set quantitative quality goals for both process and maintenance. Selected subprocesses significantly contribute to overall process performance and are controlled using statistical and other quantitative techniques.

And finally, at Maturity Level 5 (optimizing), quantitative process-improvement objectives for the organization are firmly established and continually revised to reflect changing business objectives, and used as criteria in managing process improvement.

Maturity model

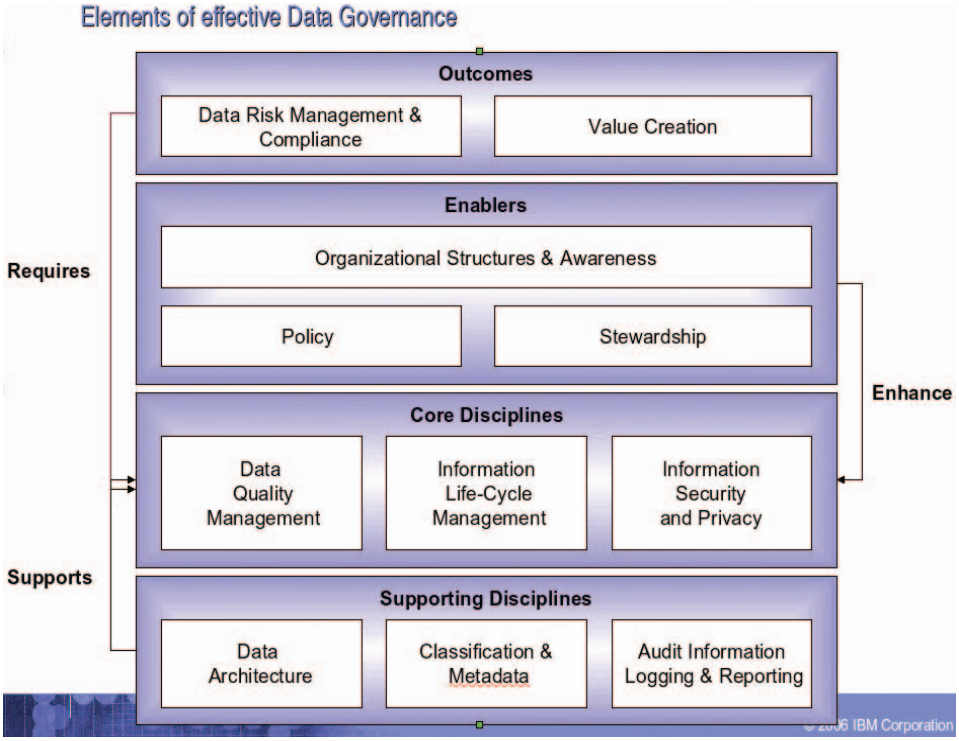


The elements of data governance

The Data Governance Council Maturity Model measures data governance competencies of organizations based on the 11 crucial domains of data governance maturity, such as organizational awareness and risk lifecycle management (see Table 1).

An initial high-level grouping of DG domains demonstrates primary relationships between these groupings.

- *Outcomes*
- *Enablers*
- *Core Disciplines*
- *Supporting Disciplines*



As an example, consider that quality and security/privacy requirements for data need to be assessed and managed throughout the information lifecycle. Executive-level endorsement and sponsorship is an enabler for stewardship of information that requires standardization across processes and functional boundaries. Consistency in practice can be enabled through stewardship when there are enterprise-level policies and standards in place for data governance disciplines.

The 11 categories of the Maturity Model are described below. Each category contains many subcategories grouped into five levels of maturity, with transition layers between maturity levels to denote concrete steps and milestones organizations can track as they advance. Through these multiple levels, organizations can not only assess where they currently are, but can set concrete goals about where they want to be.

Table 1: IBM Data Governance Council Maturity Model

Category	Description
1 **Organizational Structures & Awareness**	Describes the level of mutual responsibility between business and IT, and recognition of the fiduciary responsibility to govern data at different levels of management.
2 **Stewardship**	Stewardship is a quality control discipline designed to ensure custodial care of data for asset enhancement, risk mitigation, and organizational control.
3 **Policy**	Policy is the written articulation of desired organizational behavior.
4 **Value Creation**	The process by which data assets are qualified and quantified to enable the business to maximize the value created by data assets.
5 **Data Risk Management & Compliance**	The methodology by which risks are identified, qualified, quantified, avoided, accepted, mitigated, or transferred out.
6 **Information Security & Privacy**	Describes the policies, practices and controls used by an organization to mitigate risk and protect data assets.
7 **Data Architecture**	The architectural design of structured and unstructured data systems and applications that enable data availability and distribution to appropriate users.
8 **Data Quality Management**	Methods to measure, improve, and certify the quality and integrity of production, test, and archival data.
9 **Classification & Metadata**	The methods and tools used to create common semantic definitions for business and IT terms, data models, types, and repositories. Metadata that bridge human and computer understanding.
10 **Information Lifecycle Management**	A systematic policy-based approach to information collection, use, retention, and deletion.
11 **Audit Information, Logging & Reporting**	The organizational processes for monitoring and measuring the data value, risks, and efficacy of governance.

Each category is both a starting place for change and a component in a larger plan. Grouping the 11 domains of data governance can help organizations gain insight into how to establish the larger plan. Each of the 11 categories has five levels of maturity, which include:

- *Level 1 – Initial*
- *Level 2 – Managing*
- *Level 3 – Defined*
- *Level 4 – Quantitatively Managed*
- *Level 5 – Optimizing*

In turn, each category has subcategories that further break down the path to maturity. Organizations can start with any of the 11 domains, based on their own business needs.

For example, an organization could assess the level of governance maturity within its organizational structures by identifying the following milestones and benchmarks:

- **Level 1:** *Policies around regulatory and legal controls are put into place. Data considered "critical" to those policies is identified. Risk assessments may also be done around the protection of critical data.*

- ***Level 2:*** *More data-related regulatory controls are documented and published to the whole organization. There is a more proactive approach to problem resolution with team-based approach and repeatable processes. Metadata becomes an important part of documenting critical data elements.*

- ***Level 3:*** *Data-related policies become more unambiguous and clear and reflect the organization's data principles. Data integration opportunities are better recognized and leveraged. Risk assessment for data integrity, quality and a single version of the truth becomes part of the organizations project methodology.*

- ***Level 4:*** *The organization further defines the "value" of data for more and more data elements and sets value-based policies around those decisions. Data governance structures are enterprise-wide. Data Governance methodology is introduced during the planning stages of new projects. Enterprise data models are documented and published.*

- ***Level 5:*** *Data Governance is second nature. ROI for data-related projects is consistently tracked. Innovations are encouraged. Business value of data management is recognized and cost of data management is easier to manage. Costs are reduced as processes become more automated and streamlined.*

Similarly, an organization could assess its Data Risk Management Framework maturity through the following benchmarks:

- ***Level 1:*** *There is no formal high-level risk assessment process in place. Risk assessments are done on an as-needed basis, but not yet systematically integrated into strategic planning.*

- ***Level 2:*** *Some lines of business have processes and standards for performing risk assessments. Risk assessment criteria are defined and documented for specific items (such as credit risk) and the process is repeatable. There is limited context to validate that the risks identified are significant to the organization as a whole.*

- ***Level 3:*** *Enterprise-wide adoption of risk assessments for specific items. Example: The privacy risk of a third-party vendor relationship uses a common scoring methodology. Risk assessment criteria are defined and documented for specific items and the process is repeatable. Data on risk assessments is aggregated for senior management. Risk assessments "outside of norm" are reviewed.*

- ***Level 4:*** *Enterprise-wide adoption of high-level risk assessments for all components of the organization such as new projects, products, technologies, vendor relationships and/or applications and systems exist. Risk assessment criteria are defined and documented for all items and processes are repeatable. Data on risk assessments is aggregated.*

- *Level 5: A consistent controls framework exists and is customized to the specific profile of the firm. Output of the controls assessment process is integrated into incident, reporting, and customer notification processes. A formal, ongoing high-level risk assessment process exists.*

The Data Governance Maturity Model is a tool to assess your organization's current state of Data Governance awareness and effectiveness. Through this concrete and objective set of benchmarks, organizations can evaluate current gaps in their data governance practices and define new opportunities quickly for improving the governance based upon the observable behaviors and insights of the Data Governance Council. However, it is important to recognize that the Maturity Model acts as a framework for addressing data governance rather than a prescription.

The Model is presented both as a Maturity Framework and as a set of assessment questions with answers constructed to indicate maturity levels. But how an organization chooses to use this tool will depend on many factors. Just as every organization is unique, each organization will set its own goals and methods based on individual business scenarios, plans and needs. In addition, the Maturity Model is not intended to be static and continues to evolve along with the data governance space. The IBM Data Governance Council welcomes new members who would like to contribute and provide feedback.

Summary

In the past decade, data governance has emerged as one of the top strategic priorities for organizations everywhere. As a result, there is a growing industry-wide need for services to help companies become more proactive to gain insight on where important information resides within the organization, governing its use appropriately.

Based on collaborative methods and practices from Council members, the IBM Data Governance Council Maturity Model provides a set of benchmarks and milestones to help organizations of all sizes measure their data governance maturity. Beyond maturity levels, business practices and organizational behavior, IBM provides a number of tools and solutions to help organizations take advantage of the Maturity Model to reach new levels of maturity. By leveraging the Maturity Model, organizations can take the first step to determine where they are today—and where they want to go tomorrow.

For more information

To learn how the IBM Data Governance Council Maturity Model can help you get started on the path to data governance, visit **ibm.com/** software/data/information/trust-governance.html or call a representative at 1 877-426-3774.

IBM Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
10-07

LO11960-USEN-00