



Data Governance – Managing Information As An Enterprise Asset Part I – An Introduction

Introduction

In a *knowledge economy*, information is one of the most valued enterprise assets. In a *transformation economy*, proper governance of information becomes a *critical success factor*. Data and information will outlast applications¹ requiring the management of data and knowledge assets through time as applications, and even business processes change. Data governance is essential to ensuring that data is accurate, appropriately shared, and protected. Data is rationalized to create information. Information is rationalized to create knowledge. And knowledge is the basis for wisdom, supplemented by intuition, in decision making. The quality of data and information will certainly impact the quality of the decisions that consume it. However, it can't be assumed that decision making rationale will necessarily make the best use of such information or the best or most appropriate decisions or choose the best course of action. The subject of decision making and decision theory is outside the scope of this report. Nevertheless, positive citizen outcomes are the ultimate objective and this requires government to properly manage data, information and knowledge assets, and to use and manage these assets with the utmost wisdom.

This issue brief will focus on data governance which can and should be broadened into the subject of information or knowledge management governance.

Data Governance refers to the operating discipline for managing data and information as a key enterprise asset. This operating discipline includes organization, processes and tools for establishing and exercising decision rights regarding valuation and management of data. Key aspects of data governance include decision making authority, compliance monitoring, policies and standards, data inventories, full lifecycle management, content management, records management, preservation, data quality, data classification, data security and access, data risk management, and data valuation.

Capabilities for enabling data governance are described in the Federal Data Reference Model as follows²:

- Data Discovery
- Data Reuse
- Data Sharing
- Data Entity Harmonization
- Semantic Interoperability

Data context is the basis for data governance. Understanding data context provides the means for informed government decision making with regard to

April 2008

NASCIO Staff Contact:
Eric Sweden
Enterprise Architect
esweden@amrms.com



NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

Copyright © 2008 NASCIO
All rights reserved

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
Email: NASCIO@AMRms.com

information holdings. Data context is provided by the remaining federal enterprise architecture reference models.

Data Context can be defined as:

Any information that provides additional meaning to data. Data Context typically specifies a designation or description of the application environment or discipline in which data is applied or from which it originates. It provides perspective, significance, and connotation to data, and is vital to the discovery, use, and comprehension of data.³

There are various definitions for Data Governance depending on the specific focus required. The following demonstrate the universe of data governance is indeed broad and deep.

Data Governance (DG) – The formal orchestration of people, process, and technology to enable an organization to leverage data as an enterprise asset.⁴

The MDM Institute

Data governance is defined as the processes, policies, standards, organization, and technologies required to manage and ensure the availability, accessibility, quality, consistency, auditability, and security of data in a company or institution.⁵

Informatica

Data governance encompasses the people, processes and technology required to create a consistent, enterprise view of an organization’s data in order to:

- **Increase consistency & confidence in decision making**
- **Decrease the risk of regulatory fines**
- **Improve data security**
- **Achieve consistent information quality across the organization**
- **Maximize the income [value] generation potential of data**
- **Designate accountability for information quality**⁶

Wikipedia

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 an [organization’s] data by fostering cross-organizational collaboration and structured policy-making.⁷

IBM

Data governance is 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.⁸

The Data Governance Institute

Why is Data Governance important?

Most states are working their way toward a mature enterprise architecture program, effective program and project management, and starting to use discipline for service management such as Information Technology Service Management (ITSM). However, data governance is possibly the least mature capability across the states. Even across industry, data governance is a significant issue.

*Over the next two years, more than 25 percent of critical data in Fortune 1000 companies will continue to be flawed, that is, the information will be inaccurate, incomplete or [unnecessarily] duplicated...*⁹

The demand for trusted information continues to spiral upward. States currently own significant data resources, but turning that data resource into an information asset that can be managed for effective decision making is simply not happening at an *enterprise* level. There are effective point solutions within specific agencies but managing information as an enterprise asset will require effective data governance.

Government performance depends on

accurate and timely information. Historically, performance improvement was delegated to either the program level or the task level. With proper data governance, performance improvement will be available at all levels of a government organization. The real value creation comes from cross organizational performance improvements based on cross organizational information sharing. In one state, health information was distributed across five state agencies. Implementing proper data governance principles allowed the sharing of single sourced information and the implementation of integrated and more meaningful health program measures.

The current challenges in data management can be traced to how applications and systems have evolved over the past many decades. Enterprise information assets are stored and maintained to various levels of quality throughout state government. There is a diversity in data modeling approaches, naming standards, formats, and meta data standards.¹⁰ Applications and systems were developed outside of an enterprise wide portfolio management discipline which has led to the existing or “as-is” environment of “siloed” information resources characterized by unnecessary redundancy, inconsistency and even contradictory data, and inconsistent methods for rendering or modeling data. There are also conflicts between speed of performance and maintenance of data resources. Proper data management takes a longer view at managing information assets. This can create challenges with project timetables and speed of delivery that didn’t fully account for data governance. This problem is becoming worse due to the continuing growth in data volumes. An IDC study recently reported that the size of the *digital record* will grow by a compound annual growth rate of 60%. By 2011 there will be more than 10 times the amount of electronic data that existed in 2006.¹¹ This includes structured data and unstructured data such as web sites, geospatial data, graphics, and visual analytics.

Another factor that is leading to the new heightened concern regarding data governance is the advent of much increased collaborative information sharing across government lines of business and jurisdictions. As information content, or “payload,” is transferred and redistributed multiple times, there is the requirement that the rules for governing that information accompany the information “payload.” These rules constitute the “meta data” or data about the data. An initial challenge is collecting meta data and ensuring that meta data content is accurate and at the appropriate level to reliably inform subsequent information consumers. A second challenge is ensuring that meta data stays with the payload. This will require both administrative and technological controls, and awareness training.

The CDI Institute conducted an extensive survey of Fortune 5000 companies to learn how these corporations are investing in data governance and what barriers they had encountered. Many states could easily compare with Fortune 500 corporations in terms of budget, personnel, locations and complexity. Therefore, many of the conclusions from the CDI study are certainly applicable to state government. The study presents the following reasons for establishing data governance discipline.¹² These have been adapted to state government.

- Given the importance of data as the “currency” of the [state government] enterprise, data [information] must be treated as a highly valuable enterprise asset.
- The value and associated risks of the enterprise’s data [information] assets must be ascertained if it is to be properly managed and protected. [Ascertaining the criticality, value or relative value will help to determine the level of investment in security, access, quality assurance, and recoverability.]
- Data must be maintained to some level of quality if it is to be trusted [or relied upon for decision making]. Data must be managed as an enterprise asset

The digital record is growing at compound annual growth rate of 60%.

similar to finance and physical assets. Data governance provides the means for properly managing this asset.¹³

- Information must be integrated across the enterprise. [The citizen should see “one state government” independent of agency. Further more government decisions require more types of data from multiple and diverse government lines of business.]
- Decision making relies on business intelligence that is derived from enterprise data. Data resources must be properly managed within a data governance operating discipline to enable [effective] decision making.

Finally, data governance will not only bring new capabilities for saving and better applying limited resources, but with the advent of standards comes the ability for the enterprise to act as a single enterprise, and the ability to respond to environmental threats and opportunities faster and more effectively. What drives that new capability is readily available data and information to make effective decisions in line with the urgency of environmental circumstances. Environmental circumstances are a spectrum of continually changing domains that include homeland security, public safety, natural disasters, environmental events, public health events, and economic changes locally and globally. Environmental circumstances also include business and technology innovation. Additionally, these circumstances must be anticipated as being *interrelated* which creates even further necessity for effective *cross line of business* and *cross enterprise decision making* capabilities founded on accurate, timely, reliable, integrated, and available information.

Determining The Value and Sensitivity of Information

Valuation of information is a necessary component of asset management. There are documented approaches to valuation of information assets based on characteristics or *components of value (COV)* such as: the cost to acquire information; shareability;

the audience(s) that use the information; the context within which the information will be used; the value produced by the processes that use the information.^{14 15}

Not all data or information has the same associated value. Nor is all information subject to the same risks. Some information is so vital or sensitive to state government that it requires a high level of assurance of security and extremely granular access rights. For example, if information content is highly sensitive, then access to that information will require careful validation of the access rights, the identity, and the role of the requester. Further, there is increased demand for high data quality. Risk can be described as having two major components: the *probability* of an undesirable event and the *impact* of that event. The worst case is where there is a high probability coupled with a high impact.

*Quantified Risk = Probability X Impact
(e.g., measured in terms of \$, morbidity,
mortality, environmental outcomes)*

In certain circumstance there is a zero tolerance for loss of data, or loss of access to information. This circumstance could be exemplified by health information related to an interview with a patient that subsequently dies. If that last record of information is lost, it cannot be recreated, or replicated. In essence any event that involves the perishing of the source presents a circumstance that requires the highest level of data protection because the data cannot be recreated. This is one end of the *quantified risk spectrum*.

At the other end of this spectrum is data that is public knowledge and easily replicated from multiple sources. Examples include environmental temperature, job description, organizational charts, etc. This end of the spectrum would have a low risk due to its ubiquity or public status. This information would require minimal or possibly no security. This type of information may be intended for broad undefined access, duplication and sharing.

The point is that data must be managed within a *risk portfolio*. Such a portfolio will present a context for profiling data; for deriving information value (i.e., aggregated data); its value to state government; its potential value to criminals; the potential for unauthorized change and the secondary effects of such change; and the associated necessary security measures to properly protect it. Associated security measures are also derived from legal requirements mandated by local, state or federal government.

What has been described here constitutes components of the *meta data* for data and information which must reside within the state's knowledgebase. State data management practices must ensure that this meta data remains coupled with the information payload. Meta data includes many others aspects related to the management of data and information. This can include data security classification, and data retention schedules. Human roles, software and system processes, as in an SOA environment, that have the appropriate level of authority, can then execute the policy presented in the meta data.

Before data and information can be properly secured, it must be properly classified. Classification is contextual. Therefore the first reference point for classification of data must be state regulations.

Some information can be assumed as highly targeted for cyber attack. This includes certain information highly critical to operations, such as vital records required for continuity of operations; or information that has resale value such as personnel information including social security numbers, credit card numbers, etc. A higher security investment is justified for this type of information as compared with certain information that is inconsequential, temporal and has an associated probability of attack close to zero. The latter information would not justify the same investment in security. Further, sometimes when data is aggregated, data

that would be less valuable on an individual basis becomes *more* valuable when it is part of a larger data set. For example, 10 individual information resources may be worth \$100,000 individually. However, if that data is aggregated into a central information resource, that resource is now worth \$1,000,000 or more and may justify a higher level of security.

Potential Barriers to Progress in Implementing Data Governance

Exeros conducted survey of 130 IT executives from Fortune 1,000 companies to learn what barriers impede progress related to data governance. These are the barriers that must be taken into account and managed proactively to ensure data governance efforts are moving forward.¹⁶

Most commonly cited barriers organizations must overcome to implement data governance policies and procedures:

1. determining the rules and requirements; interpreting and understanding the rules concerning data sources
2. gaining agreement of all parties regarding policies
3. developing new tools and software to enable data governance
4. the cost of implementing policies
5. incompatible systems
6. competing priorities within the organization
7. getting management to understand what is necessary
8. building the project process

Additional barriers within state government parallel those that inhibit information sharing. These include legislative issues, the lack of incentives and unique grant related requirements that effectively create *information stovepipes*.¹⁷

Gaining commitment from executive management is critical to a data governance initiative. In presenting the need for data governance, the message and justification have to be kept at the right level. Statistics and costs associated

with poor quality of data, unnecessary redundancies, and cyber attack success rates and impact will assist in promoting the value of data governance. The message to executive management must also include a description of the magnitude of current investments in data assets, data bases, data base management systems, content management systems, electronic records and archiving.

Key ingredients for successfully initiating and implementing data governance include the full understanding and support of the state CIO, endorsement and participation by agency executives, and the backing of the current state administration and general assemblies. This support must then be leveraged to gain commitment for establishing an inter-agency task force to build a program that is founded on joint consensus across state agencies. Establishing this level of support, commitment and participation require a well planned and executed *marketing and communication plan*. Such a plan must include initiatives to retain commitment once the data governance program is up and running. Participants and executive management must have ongoing affirmation and confirmation that the program is necessary and is effectively delivering results. This requires appropriate metrics that demonstrate progress in achieving the targets related to data quality, reliability, integrity, accessibility, etc. Those results must be effectively presented and communicated. *Communication* is the most often overlooked dimension of data governance.¹⁸

Implementing Data Governance – The Organization

First and foremost, an operating discipline in data governance will not be successful without ownership from the business side of government. Information and data must be viewed at the enterprise level as state government assets that are owned by the business. Data governance is a

business concern that can be supported by information technology. It must be viewed as an *enterprise asset management program*. The best data architecture team and data governance technology will not have the full and necessary impact unless the business side of state government is convinced that data governance is essential to their success.¹⁹ According to a Gartner study (*quoted in the referenced blog*) “less than 10% of organizations will succeed in their first attempts at data governance.”

The biggest challenge is commitment to keep the program alive and moving forward. State CIOs have attempted to establish governance of information technology investments and have had successful first meetings of the stakeholders – i.e., agency directors. What too frequently happens is the agency executive director delegates participation to the agency IT operations director. As presented by Rick Sherman of *Athena IT Solutions*, gaining executive involvement is oversimplified in most presentations on data governance. *Sustained* executive involvement is hard to achieve. This challenge must be anticipated and planned for. As stated above, a communication strategy and plan must be established. That strategy and plan must also take into account the *culture of the organization*.

Executive involvement is more than funding. What is required is enterprise commitment implemented so that every job / role includes a data governance performance dimension.²⁰ The following list was presented in SearchDataManagement.com as the key reasons that data governance projects fail.²¹

- **Cultural barriers**
- **Lack of senior-level sponsorship**
- **Underestimating the amount of work involved**
- **Long on structure and policies, short on action**
- **Lack of business commitment**
- **Lack of understanding that business definitions vary**
- **Trying to move too fast from no-data-governance to enterprise-wide-data-governance**

Organizational Levels and Roles for Implementing Data Governance

Executive Level

- Sponsorship
- Strategic Direction
- Funding
- Advocacy
- Oversight

Judicial Level – business and technology leaders

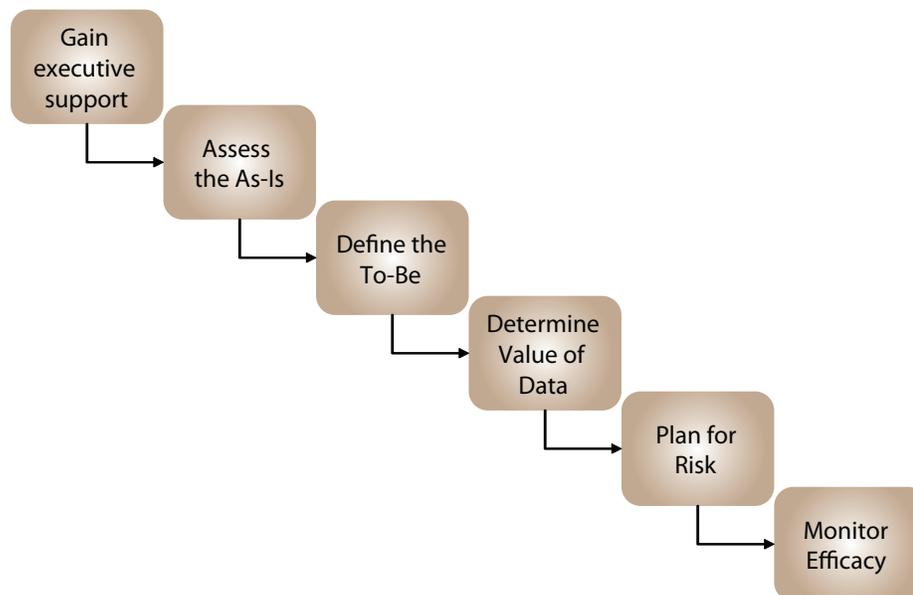
- Strategic planning activities
- Enforce governance activities and policies
- Mediate disagreements about governance

Legislative Level – chaired by a senior business leader designated by executive leadership – members from business and technology leadership

- Establish data governance policy traceable to enterprise business strategies
- Establish policies for managing structured and unstructured data
- Commit resources to data governance
- Establish data stewardship programs
- Identify gaps in policies
- Escalate unresolved issues to the Judicial Level

Administrative Level – implementers of data governance

- Carry out data governance policies
- Clearly articulate business drivers
- Overcome inhibitors to progress
- Clarify steps to make progress at the organization, system, project and program levels
- Manage specific subject areas
- Develop data models and vocabularies
- Implement master data management best practices
- Organize content and records management
- Preservation, digital archives and long term access to data and information
- Implement data security and access policies
- Institute and monitor data quality processes
- Tracking governance related metrics
- Recommend standards and policies to the Legislative Level
- Oversee subject level data stewards who implement governance policies and standards and maintain data quality metrics



Data Governance Process

Gartner recommends establishing organizational checks and balances *similar* to a government structure in implementing data governance.²²

Finally, the greatest challenge for any strategy, plan or operation is *effective execution*. Once the delivery process is established, it must be carried out. This requires sustained energy of effort, maintaining commitments, communication and delivering results. This may require an evangelist to keep things moving forward.²³

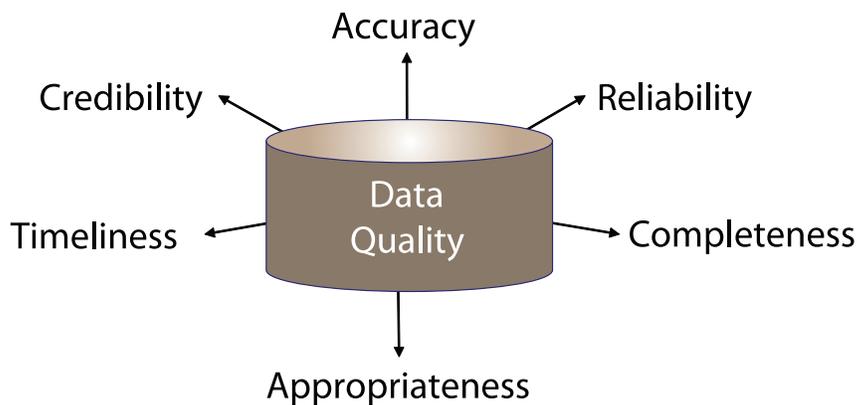
Implementing Data Governance – The Process

A data governance program starts with an understanding of the “As-Is” environment. In most cases, the As-Is situational analysis must be created because there is no central or consistent record to answer what data exists, who uses it, and how it is used. The As-Is may uncover that the organization is at the initial stage of maturity in data governance where the organization thinks and acts “locally.” Good data governance characteristics may be highly isolated because individual agencies and departments only manage

their data within a limited sphere of influence. The target scenario, or “To-Be”; is then articulated from an *enterprise perspective*. Mature data governance requires the enterprise to think and act “globally.”

Strategies are developed to bridge the gap. This basic approach of *understanding the As-Is, envisioning the To-Be, gap analysis, and strategy development for bridging the gap* is consistent with the general approach presented in the NASCIO Enterprise Architecture Toolkit²⁴ within enterprise architecture and various expertise centers on data governance.

There are a number of maturity models available that can assist in the assessment process throughout the journey from the As-Is to the To-Be and which can be used for taking the pulse of the organization at each stage and presenting recommendations for moving to the next level of maturity – *one step at a time* - allowing for proper management of a very complex initiative. Associated risks are identified and the necessary mitigation plans are planned and implemented. Finally, ongoing monitoring of the data governance discipline is required to evaluate effectiveness and ensure proactive change management.



Characteristics of Data Quality

Establishing a data governance program must be seen as a journey. It doesn't happen all at once. Each phase of the journey can be evaluated against a maturity model to measure progress. Fair warning to those just starting – its easy to fall backward in data governance maturity. Management turnover and enterprise priorities can cause a loss of focus. A robust data governance program is required that will allow continued progress even as the enterprise moves through changes such as changes in administration.

The Behavioral Dimension

The quality of data determines the quality of decision outcomes which impact citizen outcomes in state government. Data quality methods and procedures are essential to ensuring accurate data is available in a timely manner to decision makers. What happens too frequently is data values are dependent on where data was retrieved. There may not be a single authoritative source – or authoritative data source (ADS). Every process and transaction outcome depends on the quality of the data used. Poor data quality exposes state government to ineffectiveness, the risk of poor decisions, and unintended outcomes. In addition there is

financial and publicity risk. *High data quality* can contribute to achieving the opposite – i.e., desired outcomes in government services due to effective decision making based on reliable, timely information.

Many people attribute the quality of data to the system from which it was retrieved. However, data must be initially *entered* into a system. Even derived data was calculated from base data that was, in most cases, entered into a system by a person. Thus, any governance discipline must take into account *human factors*.²⁵ Many elements contribute toward poor data quality including lack of authority or the required time to correct data problems. There may be other motivational factors such as lack of interest, concerns regarding exposing errors on the part of others, or a lack of data ownership.

Effective data governance must address the *human factors* aspect in order to ensure the quality of the data being collected and maintained is consistent and reliable. To meet these *behavioral challenges* it is important to effectively communicate how data quality impacts the effectiveness of state government, provide training on data quality, the roles and responsibilities for data quality, and how to prevent and correct data quality problems. Maintaining data quality must

Accuracy: Data is correct and precisely reflects the object or transaction it describes.

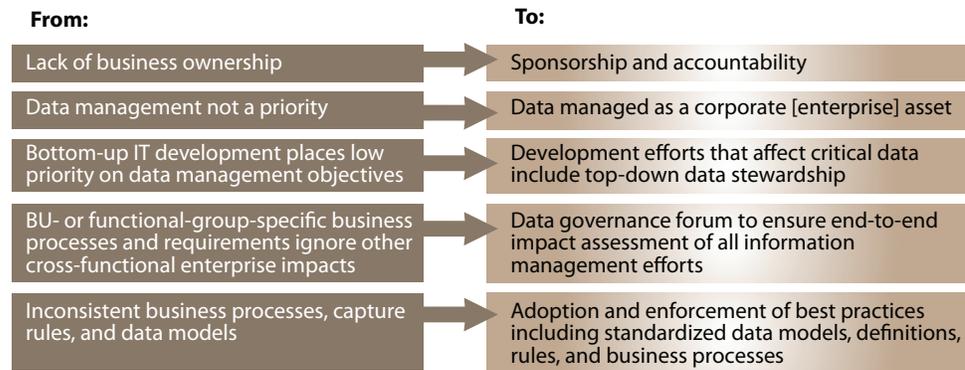
Reliability: Data is consistent across multiple transactions.

Credibility: The degree to which decision makers trust both the accuracy and reliability of data. Data must be credible in order for it to be used for analysis or decision making.

Timeliness: Data is available to the information consumer when it is needed. Data that is not available when needed is of no value.

Appropriateness: The degree to which the data itself is relevant to the needs of an organization. Slanderous, derogatory, offensive, irrelevant or otherwise inappropriate data that does not add value to the organization degrades the data quality.

Completeness: All of the relevant or required data is readily available for use when required.



Source: Forrester Research, Inc.

Data Governance Evolution²⁷

problems. Maintaining data quality must be understood as everyone’s job and should be a job performance dimension for every job. Data ownership and stewardship must be established through appropriate job roles. The *data owner* is typically the creator of the data. A broad definition of *data stewardship* would be the ongoing management of maintenance, quality, and access. Specific roles are defined by David Loshin.²⁶ The point presented is that *it is people that will finally implement a data governance program*. People need to understand the importance of data quality, and be motivated and empowered to implement data governance. Proper data governance will require involvement from everyone in the organization.

Many of the barriers to information sharing are presented in the NASCIO series, “Perspectives on Information Sharing.” There are many organizational pathologies that lead to the organizational hurdles that get in the way of creating effective data governance. These include fear of losing control or a “turfdom”, or fear of exposure to internal criticism or the press. These issues are real and reflect to some extent the organizational health, level of trust, and ability of the enterprise to work together in a collegial manner. A data governance initiative will quickly uncover the level of trust within the organization. And it is executive management alone that can create the necessary trust organi-

zation required to ensure proper management of enterprise information assets.

Conclusion

In this introductory brief data governance has been presented as a necessary enterprise initiative that must be adopted within the culture of the organization, and most importantly by the individual. Data governance is really about properly managing data, information and knowledge as a state asset and resource. Such an asset requires careful handling because it forms the basis upon which decision making is founded. That decision making touches every aspect of state government and impacts the lives and well being of our state citizens.

Calls to Action

1. **Place data governance as a priority agenda item to be investigated and addressed as part of an overall IT governance initiative.**
2. **Understand data governance as part of the larger scope of knowledge asset management. Governance must ultimately encompass that scope.**

3. ***Understand data governance must be properly planned and chartered (policy, organization, process, commitment, communications, frameworks, methods and procedures, valuation, and tools). Start with a limited scope initiative.***
4. ***Leverage a maturity model for planning manageable phases in data governance.***
5. ***Engage the business side of government in data governance. Make communication of the benefits and intended outcomes a high priority in order to gain and sustain involvement from stakeholders.***

Appendix A: Acknowledgements

Mike Byrne, GIS Coordinator, The State of California

Dr. Brian Cullis, Vice President and Global Lead Enterprise Information Strategies, CH2M HILL

Pat Cummins, Government Strategist, Environmental Systems Research Institute Inc. (ESRI)

Paul Warren Douglas, Acting Director of Enterprise Architecture, State of Washington

Neil Downing, Director of Enterprise Information Management, Keane, Inc.

Mike Dunham, Senior Principle Consultant, Keane Federal Systems

Lauren Farese, Director, Public Sector Solution Architects, Oracle Corporation

Dan Feinberg, Solutions Architect, Enterprise Management Solutions, CH2M HILL

Michael Fenton, Director of Enterprise Architecture, The State of North Carolina

Graeme Finley, Director, Grant Thornton LLP

Stephen Fletcher, Chief Information Officer, State of Utah, Co-Chair of the NASCIO Enterprise Architecture Committee

John Gillispie, Chief Information Officer, State of Iowa, President of NASCIO

Dennis Goreham, GIS Coordinator, The State of Utah

Christopher Ipsen, Chief Enterprise Architect and Acting Chief Security Officer, State of Nevada

Shawn Karrick, Communications Coordinator, NASCIO

Zsolt Nagy, GIS Program Manager, State of North Carolina

Sharon Poulalion, Enterprise Portfolio Management, South Carolina Division of the State Chief Information Office

Doug Robinson, Executive Director, NASCIO

Bill Roth, Chief Enterprise Architect, State of Kansas

Russ Saito, Comptroller, Chief Information Officer, The State of Hawaii

Glenn Thomas, Director of Data Architecture, Commonwealth of Kentucky

Chuck Tyger, Associate Director Enterprise Architecture, The Commonwealth of Virginia

Chris Walls, Senior Website & Publications Coordinator, AMR Management Services

Tom Walters, Division of Data Architecture, Commonwealth of Kentucky

Appendix B: Resources

NASCIO www.nascio.org

IT Governance and Business Outcomes – A Shared Responsibility between IT and Business Leadership
<http://www.nascio.org/committees/EA/download.cfm?id=98>

Enterprise Architecture: The Path to Government Transformation
<http://www.nascio.org/nascioCommittees/EA/>

Call for Action, A Blueprint for Better Government: The Information Sharing Imperative
http://www.nascio.org/washwatch/NASCIOWw/calls_for_action.cfm

PERSPECTIVES: Government Information Sharing Calls to Action
<http://www.nascio.org/publications/index.cfm#perspectives>

In Hot Pursuit: Achieving Interoperability Through XML
<http://www.nascio.org/publications/index.cfm#xml>

We Need to Talk: Governance Models to Advance Communications Interoperability
<http://www.nascio.org/nascioCommittees/interoperability/Interop.%20Gov.%20Research%20Brief%20Final.pdf>

A National Framework for Collaborative Information Exchange: What is NIEM?
<http://www.nascio.org/nascioCommittees/EA/#niem>

List of NASCIO Corporate Partners
<http://www.nascio.org/aboutNascio/corpProfiles/>

List of NASCIO Publications
<http://www.nascio.org/publications/index.cfm>

List of NASCIO Committees
<http://www.nascio.org/nascioCommittees/index.cfm>

The Center for Information Systems Research (CISR)

<http://mitsloan.mit.edu/cisr/>

The Data Administration Newsletter

<http://www.tdan.com/index.php>
 Presents 8 chapters that describe how to implement data governance

The Data Governance Institute

<http://datagovernance.com/>

The Data Management Association International – DAMA

www.dama.org
 The Data Management Body of Knowledge (DMBOK) -
<http://www.dama.org/i4a/pages/index.cfm?pageid=3364>

The Federal Enterprise Architecture Reference Models

<http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html>

The IT Governance Institute (ITGI)

<http://www.itgi.org/>

Information Systems Audit and Control Association (ISACA)

<http://www.isaca.org/>

Certification in Governance of Enterprise IT (CGEIT) from ISACA

<http://www.isaca.org/Template.cfm?Section=Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=36129>

The National Information Exchange Model (NIEM)

www.niem.gov

Global Justice Reference Architecture for SOA

http://www.it.ojp.gov/topic.jsp?topic_id=242

[The Global Justice Reference Architecture \(JRA\) Specification, Working Draft Version 1.4](#)

[The Global Justice Reference Architecture \(JRA\) Web Services Service Interaction Profile Version 1.1](#)

[The Global Justice Reference Architecture \(JRA\) ebXML Messaging Service Interaction Profile Version 1.0](#)

Appendix C: Endnotes

¹ “Oracle Master Data Management: An Executive Overview”, An Oracle White Paper, November 2007.

² The Federal Data Reference Model, available at <http://www.whitehouse.gov/omb/egov/a-5-drm.html>.

³ The Federal Data Reference Model – see glossary of terms.

⁴ See <http://www.tcdii.com/whatsDataGovernance.html>.

⁵ “How to Launch a Data Governance Program: Practical Guidelines for Technology Implementers”, Informatica. Retrieved on March 5, 2008, from www.informatica.com/solutions/data_governance.

⁶ Retrieved on February 14, 2008, from en.wikipedia.org/wiki/Data_governance.

⁷ “The IBM Data Governance Council Maturity Model: Building a roadmap for effective data governance”, October 2007, retrieved on March 10, 2008, from <http://www-306.ibm.com/software/tivoli/governance/servicemanagement/data-governance.html>.

⁸ The Data Governance Institute, retrieved on April 2, 2008 from http://www.datagovernance.com/adg_data_governance_definition.html.

⁹ Gartner, Inc press release. “‘Dirty Data’ is a Business Problem, Not an IT Problem, Says Gartner,” March 2, 2007.

¹⁰ “The Data Governance Maturity Model: Establishing the People, Policies and Technology That Manage Enterprise Data”, DataFlux Corporation, retrieved on March 11, 2008, from www.dataflux.com.

¹¹ Mearian, L., “Study: Digital universe and its impact bigger than we thought”, March 11, 2008, Computerworld, retrieved on March 17, 2008, from <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9067639>.

¹² *Corporate Data Governance Best Practices – 2006-07 Scorecards for Data Governance in the Global 5000*, CDI Institute, April 2006, retrieved on March 10, 2008, from <http://www.tcdii.com/#>.

¹³ Marco, D., Smith, M., “Understanding Data Governance and Stewardship, Part 1”, DMReview.com, September 2006, retrieved from <http://www.dmreview.com/issues/20060901/1062028-1.html> on April 1, 2008.

¹⁴ Engelsman, W., “Information Assets and their Value”, retrieved on April 8, 2008, from <http://referaat.cs.utwente.nl/new/paper.php?paperID=186>.

¹⁵ Glazer, R., “Measuring the value of information: The information-intensive organization”, IBM Systems Journal, Vol 32, No. 1, 1993, retrieved on April 8, 2008, from www.research.ibm.com/journal/sj/321/glazer.pdf.

¹⁶ “Market Survey: The State of Data Governance”, 2007, Exeros, retrieved on March 10, 2008, from www.exeros.com/pdf/State_of_Data_Governance.pdf.

¹⁷ “Perspectives – Government Information Sharing: Calls to Action”, NASCIO, March 2005, <http://www.nascio.org/publications/>.

¹⁸ “The Basics of Data Governance”, The Data Governance Institute, retrieved on April 2, 2008, from http://www.datagovernance.com/adg_data_governance_basics.html.

¹⁹ Sherman, R., "Getting Down To Business with People and Policies"; Enterprise Data Management, posted on June 25, 2007, on blogs.informatica.com, retrieved on March 24, 2008, from http://blogs.informatica.com/enterprise_data_management/2007/06/getting_down_to_business_with.html.

²⁰ Sherman, R., "The Two Titanic Data Governance Mistakes"; Enterprise Data Management, posted on July 7, 2007, on blogs.informatica.com, retrieved on March 24, 2008, from http://blogs.informatica.com/enterprise_data_management/2007/07/the_two_titanic_data_governanc.html.

²¹ Sherman, R., "Why data governance projects fail"; SearchDataManagement.com, March 28, 2007, retrieved on March 24, 2008, from http://searchdatamanagement.techtarget.com/tip/0,289483,sid91_gci1249228,00.html.

²² Newman, D., "Data governance requires checks and balances, Gartner says"; SearchDataManagement.com, November 17, 2006, retrieved on March 24, 2008, from http://searchdatamanagement.techtarget.com/news/article/0,289142,sid91_gci1230521,00.html.

²³ "Three Reasons Why Good Strategies Fail: Execution, Execution, ..." published August 10, 2005 in Knowledge@Wharton, retrieved on April 2, 2008, from <http://knowledge.wharton.upenn.edu/article.cfm?articleid=1252>.

²⁴ Enterprise Architecture Development Tool-Kit v3.0 available at <http://www.nascio.org/publications/>.

²⁵ Whitehead, J.C., "Solving the Data Quality Problem", 2006, retrieved on March 17, 2008, from www.tritunsinnovation.com.

²⁶ Loshin, D., *Enterprise Knowledge Management: The Data Quality Approach*, Kaufmann Series in Data Management Systems, January, 2001, ISBN-13: 9780124558403; Chapter 2 electronically available from SearchDataManagement.com; retrieved on March 17, 2008, from http://searchdatamanagement.techtarget.com/generic/0,295582,sid91_gci1252276,00.html#.

²⁷ Karel, R., "Data Governance: What Works And What Doesn't"; Forrester Research, September 10, 2007.

Disclaimer

NASCIO makes no endorsement, express or implied, of any products, services, or websites contained herein, nor is NASCIO responsible for the content or the activities of any linked websites. Any questions should be directed to the administrators of the specific sites to which this publication provides links. All critical information should be independently verified.

This report and the NASCIO Enterprise Architecture Program are funded by a grant from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

The opinions, findings, conclusions, and recommendations contained in this publication are those of the contributors, and do not necessarily reflect the official positions or policies of the Department of Justice.