

Governance Is an Essential Building Block for Enterprise Information Management

David Newman, Debra Logan

Organizations are seeking new ways to exploit information assets to fuel their growth. At the same time, they want to ensure that appropriate safeguards and measures are in place to protect sensitive information, provide transparency and minimize risk. This requires new attitudes, management practices and accountabilities for overcoming information silos, satisfying compliance issues and solving operational inefficiencies. Such objectives require a coordinated, organized program Gartner refers to as enterprise information management (EIM). One of the key building blocks for EIM is governance: the mechanisms through which EIM objectives are set, achieved and enforced.

Key Findings

- Everyone from the boardroom to the mailroom has a role in the governance of information assets. All are accountable for ensuring that information remains protected, consistent, accurate, transparent and accessible.
- Governance includes a formalized process known as stewardship. The roles and responsibilities for stewardship are commensurate with the levels of authority and accountability in the organization. The board (including the CEO and CFO) has stewardship responsibilities that are different from business-unit managers and staff functions.
- The scope of governance spans the life cycle of information assets from creation and capture through deletion, as well as quality, security, accessibility and disclosure. Governance is operationalized in the system development methodology.

Predictions

- By 2008, the need for governance mechanisms on information assets will span multiple groups, forcing business units to develop coordinated processes to solve information quality, security and accessibility issues; however, less than 10 percent will succeed in their first attempts because of cultural barriers and lack of senior-level sponsorship (0.7 probability).
- Through 2009, the demands for consistent and transparent information across the organization to support business performance and enterprise agility will force EIM to mature as a discipline in 60 percent of Global 100 companies (0.8 probability).

Recommendations

- Manage EIM governance as an integral part of corporate and IT governance processes, not as an isolated discipline.
- Develop a decision rights framework using a checks and balances approach (including executive, judicial, legislative and administrative functions) to identify the required information governance roles, authorities and stewardship responsibilities.
- Conduct an information governance review to assess the state of controls and risk factors across the enterprise, including "shadow IT" systems. Identify the extent of sensitive, proprietary or mission-critical information found in unsecured spreadsheets and desktop databases, and take remedial actions to minimize exposure to compliance issues.
- Initiate a day-to-day stewardship program by identifying individuals who are accountable for the production, definition, security and integrity of information assets. These individuals are part of a virtual team that spans the business and IT communities and will assume frontline functions in the implementation of EIM governance.

STRATEGIC PLANNING ASSUMPTION(S)

By 2008, the need for governance mechanisms on information assets will span multiple groups, forcing business units to develop coordinated processes to solve information quality, security and accessibility issues; however, less than 10 percent will succeed in their first attempts because of cultural barriers and lack of senior-level sponsorship (0.7 probability).

Through 2009, the demands for consistent and transparent information across the organization to support business performance and enterprise agility will force EIM to mature as a discipline in 60 percent of Global 100 companies (0.8 probability).

ANALYSIS

What You Need to Know

The proper governance of information as an enterprise asset starts with recognizing and defining the need, determining the scope and objectives, identifying who's involved and describing how it is exercised. Here, we outline a vision for the governance of information assets. Organizations are advised to include governance as a component of their EIM programs.

Why Govern Information?

Information is a vital enterprise resource and is critical to business success. Consistent and accurate information is fundamental to ERP systems, indispensable to CRM applications, foundational to business intelligence and crucial for certain classes of corporate documents. Information also takes on new dimensions and importance in emerging IT strategies, such as service-oriented architecture.

Historically, information has not been governed with the same rigor given to other vital assets, as evidenced by a lack of quality, timeliness, transparency and reuse. Such neglect affects the bottom line. For example, documented studies have shown more than \$600 billion in lost revenue attributed to data quality among North American companies. Some organizations are seeing tangible benefits from following proper information governance (see "Strategic Focus on Data Quality Yields Big Benefits for BT"). By 2008, the need for governance mechanisms on information assets will span multiple groups, forcing business units to develop coordinated processes to solve information quality, security and accessibility issues; however, less than 10 percent will succeed in their first attempts because of cultural barriers and lack of senior-level sponsorship (0.7 probability).

Defining Information Governance

Information governance is the collection of decision rights, processes, standards, policies and technologies required to manage, maintain and exploit information as an enterprise resource.

The purpose of governance is to implement mechanisms that ensure the accuracy, integrity, accessibility and security of information across the enterprise. Successful governance requires accountability. Accountability starts with the CEO, CFO and the board, which are liable for the information appearing on the balance sheet. From there, accountability cascades to levels in the organization commensurate with job function, skill and overall responsibilities. Although there are different roles and individuals involved, all must share the common vision for information as a valued enterprise asset.

Accountability is executed through a formalized top-down, bottom-up process known as stewardship. Stewardship is the act of taking care of a resource that is entrusted to an individual

or a group. People don't "own" assets, such as information, but they can be held formally accountable for them.

By applying information governance across the enterprise, the following tangible business benefits can be achieved:

- Transparency, trust, reputation and risk mitigation
- Faster time to market and faster cycle times as the result of improving information flows (such as during product development)
- Levels of mutual understanding and commitment to information as an enterprise enabler
- Consistency across the organization, particularly when operating in a shared service or distributed organizational model.

Relating Governance to EIM

Governance is one of the essential building blocks of EIM (see "The Essential Building Blocks for Enterprise Information Management"). In the EIM framework model, governance appears next to the organization building block for a reason. Governance processes are executed, enforced and implemented at various levels in the organization.

The governance building block integrates with the vision and strategy building blocks by providing the mechanisms for achieving EIM objectives. Governance enacts policies and procedures that guide application development and technology infrastructures. It also provides mechanisms to monitor and enforce metrics, such as accuracy, consistency and quality.

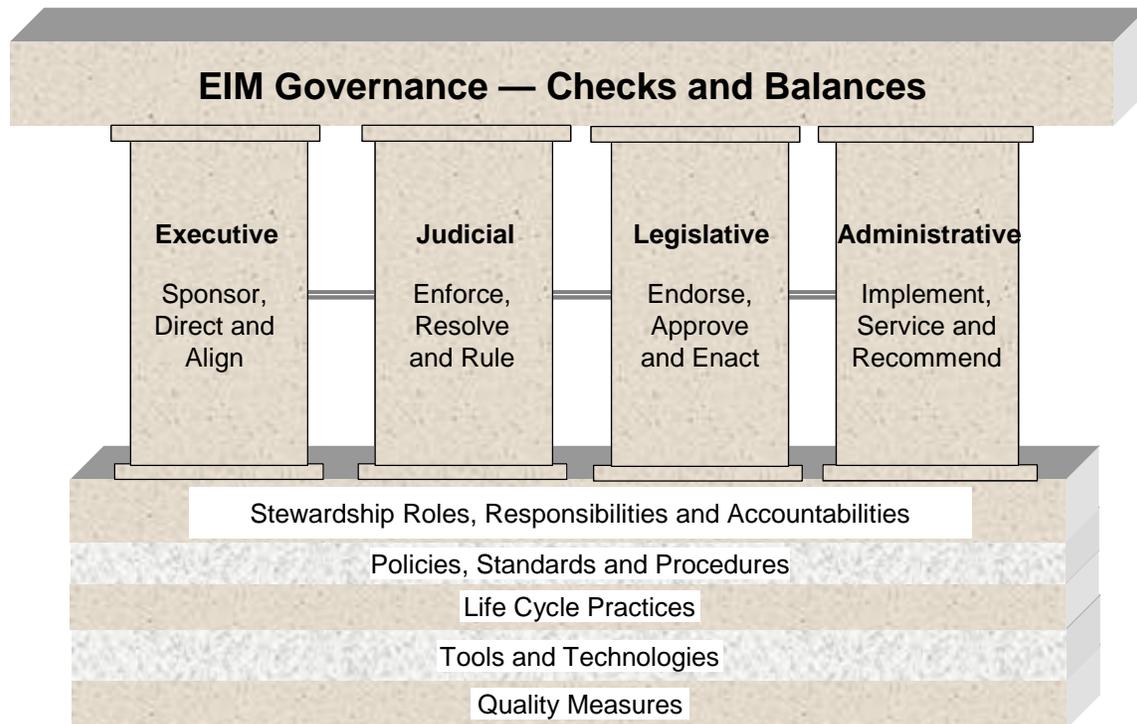
Scope and Objectives of EIM Governance

EIM governance is an integral part of corporate and IT governance processes. It is not an isolated discipline or activity. The scope spans the life cycle of information from capture and creation through deletion, as well as archiving, security, accessibility and disclosure. Moreover, specific governance policies are developed and administered to ensure that adequate controls and approvals are in place to safeguard the security and privacy of key information assets. These "duty of care" responsibilities are required to fulfill compliance or regulatory mandates. Governance must include escalation procedures to ensure that a process is triggered by noncompliance to governance standards, or when relevant issues arise.

Who's Involved?

Here, we outline the various responsibilities, roles and levels using a familiar "checks and balances" model to denote the various governance activities, such as setting standards, enforcing policies, resolving cross-team issues and implementing day-to-day procedures (see Figure 1). This model is a logical or conceptual view. It does not imply dedicated teams or a particular organizational structure.

Figure 1. Governance Bodies



Source: Gartner (May 2006)

Executive Level

This group:

- Provides executive sponsorship and strategic direction to the EIM program (usually at a CxO level).
- Communicates support and approves program funding.
- Includes EIM as an agenda topic for update or discussion during its scheduled meetings.
- Designates a lead to oversee EIM activities and provides executive oversight as necessary.

The executive level is responsible for the governance of the EIM program. The board (particularly the CEO and CFO) has strategic and fiscal accountabilities to shareholders for the accuracy and integrity of enterprise information (such as the annual report). Governance tasks at the executive level include:

- Mandate enterprisewide information governance reviews to evaluate risk factors and controls.
- Endorse a consolidated, enterprisewide information governance policy.

The executive level has final decision rights about the EIM governance. It plays an important advocacy role in articulating and endorsing the vision of EIM. As a measure of its support, this group follows a governance policy which states that only reports and information from official,

sanctioned sources are used in strategic decision making or corporate planning functions. This group establishes strategic policies, such as corporate privacy, security and legal directives pertaining to information assets. With the emergence of compliance groups in many organizations, these responsibilities may be delegated to them. The executives, however, are responsible for information quality, especially as it pertains to compliance and regulatory issues.

Judicial Level

Acting as a steering committee, these are next-level individuals (such as line-of-business leaders) who are called into session as needed. This group:

- Is responsible for enforcing cross-team governance policies (such as adherence to master data management objectives, external data transfer security requirements and so forth).
- Ensures adherence to governance standards (such as the adoption of a common business vocabulary for a "single version of truth" of master data assets).
- Resolves cross-team disputes or escalated issues identified by the legislative level (see below).
- Serves an important governance function by ruling on issues affecting distributed environments, such as struggles between local needs and strategic business objectives.

Participants in the judicial level include senior business-unit and IT leaders. Governance tasks at the judicial level include:

- Review information governance policies against compliance requirements, including Sarbanes-Oxley, Basel and other relevant guidance.
- Determine the EIM requirements needed to address government regulations or inquiries.

Legislative Level

This group:

- Mandates governance policies.
- Meets on a regular basis to discuss the status and direction of the EIM program (usually monthly). The meeting is chaired by the senior business leader who is designated by the executive level (see above).
- Includes representatives from business and technology areas.
- Institutes enterprisewide governance policies that align with strategic business objectives (such as designating controls on access to key financial or customer information).
- Escalates to the judiciary level any cross-team issues it cannot resolve.

Example participants in this group include leaders from corporate audit, security, controllers, IT and information resource management areas. This level endorses all aspects of a formalized stewardship process and commits resources from appropriate areas to perform day-to-day stewardship activities (see below).

Initial governance tasks at the legislative level include:

- Identify gaps in policies in terms of the absence of appropriate policies or the lack of proper scope.
- Enforce scope of governance to include structured content (flat files, databases and transaction systems) and unstructured content (electronic content, e-mail and information in paper form).

Administrative Level

This group:

- Implements the EIM governance program.
- Enforces the EIM policies, guidelines, definitions, standards and procedures defined at the legislative level and coordinates their day-to-day execution.

This group is managed by the senior leader designated by the executive level (see above). It may be formed as a competency center or a centralized team. It may exist in an IT or business area and will likely contain dotted-line reporting relationships and various liaison roles.

The administrative level is tasked with implementing a variety of information governance functions, such as:

- Supporting system development methodologies to ensure standards are followed
- Conducting data and process model reviews as part of the project life cycle approval process
- Implementing model management procedures (for standardization and reuse)
- Developing naming conventions, definitions, controlled vocabularies, data models and master data standards
- Organizing content and records management functions, including taxonomies to classify proprietary and sensitive information assets
- Instituting metadata management policies (for storing, cataloging and reusing information assets)
- Recommending standards to consolidate information management tools across the organization
- Centrally administering data security and data access policies to ensure proper governance from improper use inside and outside the enterprise
- Implementing data quality processes and administering data quality scorecards

Day-to-Day Stewardship

At the administrative level, stewardship activities are coordinated on a day-to-day basis between the IT and business units that work together on virtual teams to achieve common information governance objectives.

In business units, individuals are assigned stewardship responsibilities by data subject area (such as customer, product, employee, supplier and so forth). These subject areas span multiple applications. The objective is to ensure the consistency and accuracy of data as it flows from one application to the next. As part of their day-to-day activities, subject-area data stewards implement governance tasks and must achieve data quality metrics pertaining to the accuracy

and completeness of information in their domain. Minimally, they are responsible for the elements that support data sharing and master data management objectives (such as official product hierarchies, valuation models, customer segmentation profiles, preferred suppliers and so forth). Subject area stewards support ongoing profiling activities and identify issues with source systems (such as calculation routines and missing values). They are also responsible for creating or updating document taxonomies and actively participate in the semantic reconciliation of data models.

Conclusion

Through 2009, the demands for consistent and transparent information across the organization to support business performance and enterprise agility will force EIM to mature as a discipline in 60 percent of Global 100 companies (0.8 probability).

To achieve success in EIM:

- Identify the various governance mechanisms, including the roles and responsibilities in your organization, recognizing that different levels perform different functions. Everyone is accountable for the proper governance of information assets. This extends from the boardroom to the mailroom.
- Define the scope of EIM governance and line up the resources.
- Determine how procedures will be enacted (legislated) and how they are to be enforced (judicial).
- Institute day-to-day stewardship processes to formalize governance accountabilities, tackling front-line needs first.
- Ensure that the IT organization fulfills a coordinating role in information governance.

RECOMMENDED READING

"The Essential Building Blocks for Enterprise Information Management"

"Strategic Focus on Data Quality Yields Big Benefits for BT"

This research is part of a set of related research pieces. See "Spotlight on Enterprise Information Management" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509