Marrying
eGRC
and
Data Management
for
Better Governance

Agenda

Part I - F.U.D.

- Introductions
- Backgrounds/ Experience
- Strategy Domain
- Committee Domain
- Architecture Domain

Part II – R.O.T.

- Data / SoR Domain
- Metrics Domain
- Reporting Domain
- Marriage Goals
- Counseling
- Six steps to a healthy marriage

Peter Aiken, Ph.D.

- 30+ years in data management
- Repeated international recognition
- Founder, Data Blueprint (datablueprint.com)
- Associate Professor of IS (vcu.edu)
- DAMA International (dama.org)
- 9 books and dozens of articles
- Experienced w/ 500+ data management practices in 20 countries
- Multi-year immersions with organizations as diverse as the US DoD, Nokia, Deutsche Bank, Wells Fargo, Walmart, and the Commonwealth of Virginia

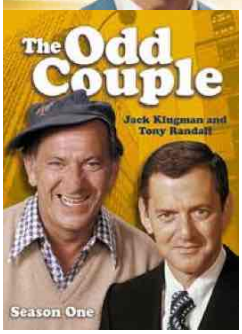
- **25 years in I.T. / Law & 18+ in eGRC, Audit, Cyber & Risk**
- **Head of Peer-Directed Research for eGRC.COM (Founder of the eGRC Advisory Board)**
- **Managing Consultant for eGRC.COM - eGRC Strategy / Integrations**
- **Creator of the eGRC Boot Camp Training Program (benefiting Veterans & Underserved)**
- **Diverse client types:** Healthcare, Financial Services, Retail, Technology, Energy, Government, Academia

Lorne O. Joseph II
CIPP, CGEIT, CISA, CISSP, ISSAP, ISSMP, ACC

Presented jointly by:

Lorne O. Joseph II
Founder, eGRC.COM

Peter Aiken
Founder, Data Blueprint



The Odd Couple!

Presentation Goals

1. To showcase an integrated model for eGRC & Data Management program management
2. To provide insights from both the eGRC & Data Management perspectives
3. To enumerate the overlaps created by managing these disciplines separately
4. To provide actionable steps to get started

Part 1 – (FUD Avoidance)

A Collaborative Risk Engagement & Aggregation Model

Definition of F.U.D. = Fear, Uncertainty & Doom

An acronym invented by Gene Amdahl after he left IBM to found his own company: “FUD is the fear, uncertainty and doubt that IBM sales people instill in the minds of the potential customers who might be considering [Amdahl] products.”

Source: *Dictionary.com*

FUD in Action

THE WALL STREET JOURNAL.

U.S. EDITION Wednesday, May 28, 2014 As of 1:58 PM EDT

Home | World | U.S. | Business | Tech | Markets | Market Data | Your Money | Opinion | Life & Culture | N.Y. | Real Estate

May 28, 2014, 1:58 p.m. ET

Target Shareholders Should Oust Directors, ISS Says

Article

Email | Printer Friendly | Share: facebook | Text

By Paul Ziobro

A prominent proxy adviser took the unusual step of recommending that Target Corp. shareholders oust seven of the company's 10 directors, citing what it called the board's failure to manage risk and protect the retailer from a massive data breach.

Institutional Shareholder Services, which advises big shareholders like mutual funds how to vote on corporate issues, focused on directors who serve on Target's audit and corporate-responsibility committees. Those committees are tasked with overseeing and managing risk, and the data breach showed the company was inadequately prepared for the threats posed by hackers.

"It appears that failure of the committees to ensure appropriate management of these risks set the stage for the data breach, which has resulted in significant losses to the company and its shareholders," ISS wrote.

Beth Jacobs abruptly resigned in March

Target’s CEO is out in wake of big security breach

1 - Strategy Domain

What is Strategy?

strat·e·gy

/stratəjē/

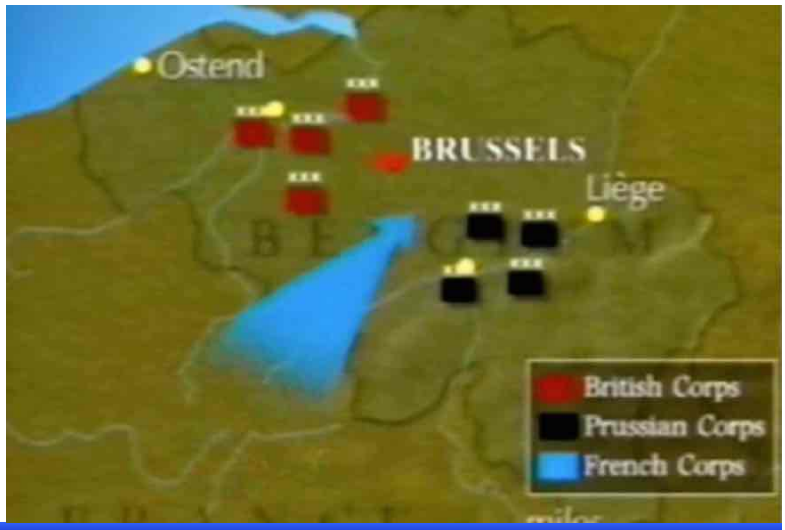
noun

1. a plan of action or policy designed to achieve a major or overall aim.
   "time to develop a coherent economic strategy"
   synonyms: master plan, grand design, game plan, plan (of action), action plan, policy, program; More

- Current use derived from military
- "a system of finding, formulating, and developing a doctrine that will ensure long-term success if followed faithfully [Vladimir Kvint]
- "a pattern in a stream of decisions" [Henry Mintzberg]

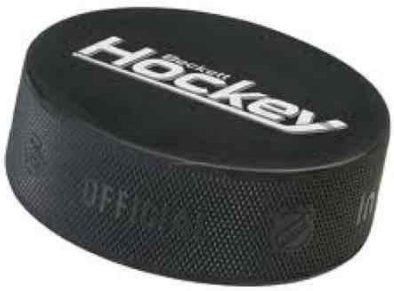
Strategy in Action: Napoleon defeats a larger enemy

- Question?
  - How to I defeat the competition when their forces are bigger than mine?
- Answer:
  - Divide and conquer!
  - "a pattern in a stream of decisions"



Wayne Gretzky's Definition of Strategy

He skates to where he thinks the puck will be ...



Data Strategy in Context

Organizational

IT Strategy

Data Strategy

Data Strategy Choices

Innovation

Q3
Creating strategic opportunities

Q4
Both

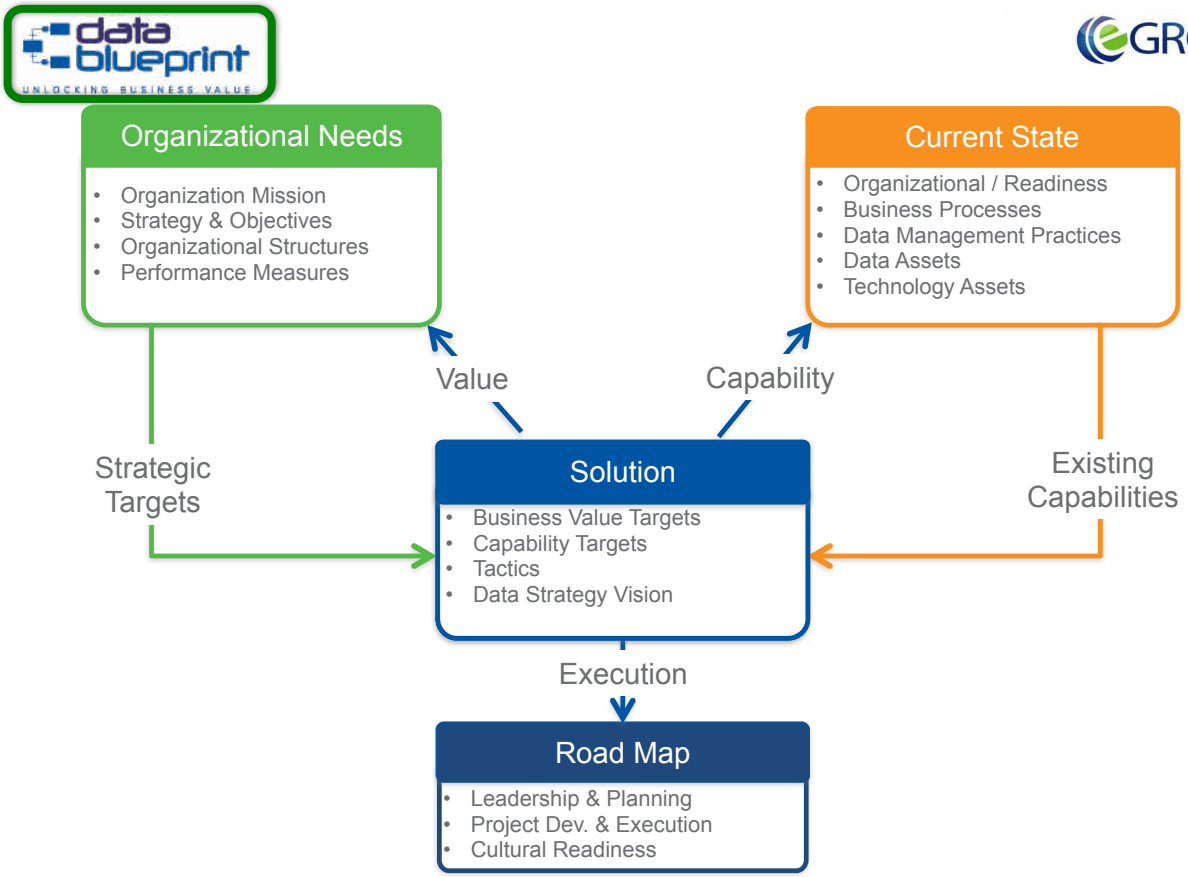
Only 1 is 10 organizations has a board approved data strategy!

Q1
little or no proactivity

Q2
Increasing organizational efficiencies/effectiveness

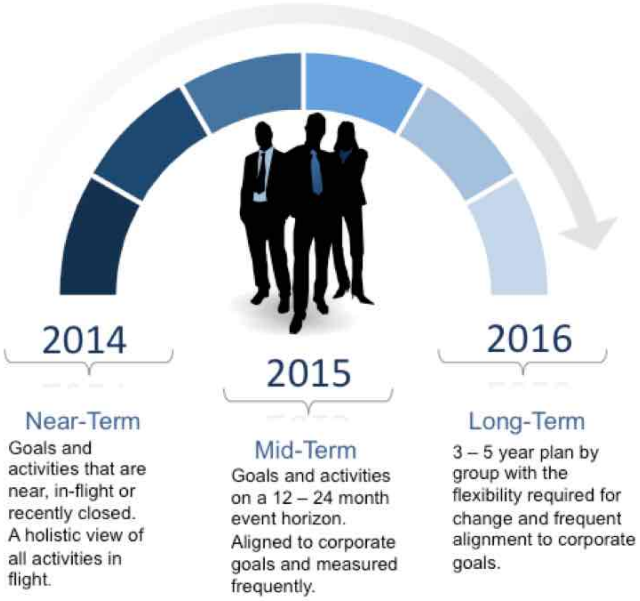
Walmart

Improve Operations



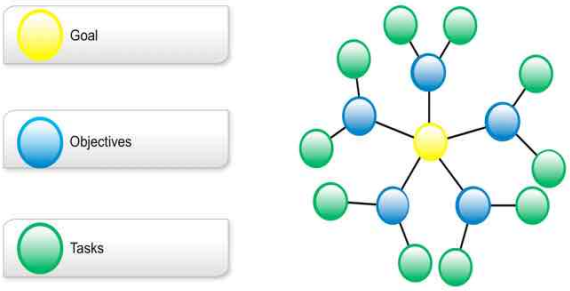
Strategy Domain

- Easiest to implement, most challenging to garner support
- Needed to align GRC program with corporate goals and objectives
- Constant monitoring will ensure executive support
- A feedback loop will serve to provide visibility in real-time



Strategy Goals

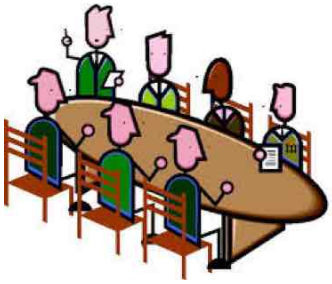
- Develop a process to consistently and repeatedly measure alignment to corporate goals and objectives.
- Align Tasks to Objectives and Objectives to goals to ensure consistent alignment and expectations are managed.
- Continuously provide reporting to senior management to ensure collaboration and reinforcement of your eGRC direction.
- Utilize Objectives Management tools to measure and track progress and report at the task and objectives level.



2 – Committee Domain

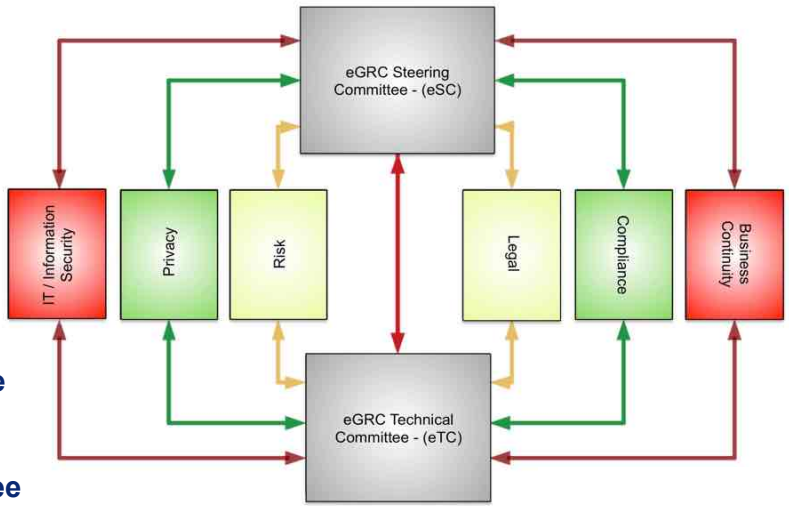
Committee Goals

- Establish an eGRC Steering Committee (eSC) comprised of leaders from all risk assessing functions (including those not currently using your eGRC Tool).
- Establish an eGRC Technical Committee (eTC) comprised of all Application Owners and System Administrators who are responsible for integrating, maintaining and changing the eGRC Tool Solutions in your environment.
- Create a single channel for the flow of risk information to ensure that you manage your internal sound to noise ratio.
- Ensure a consistent flow of communication is fostered; this will allow natural information channels to emerge.



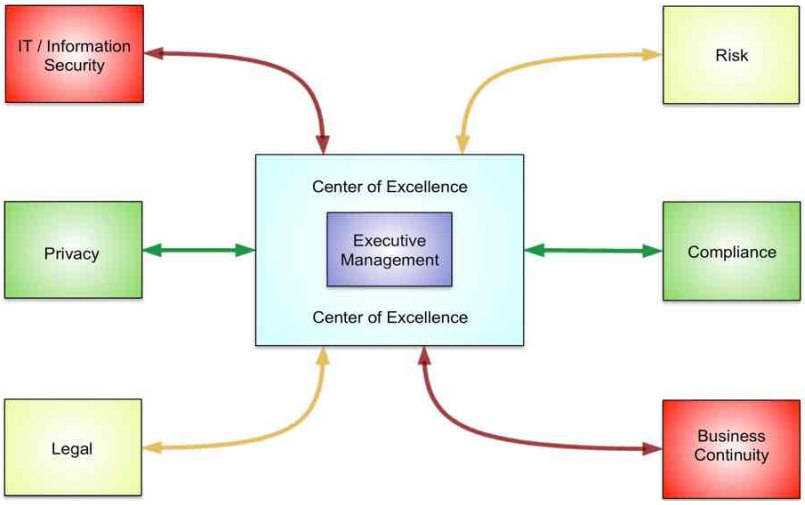
Unstructured Communications

- **Too much communication exacerbates the problem**
- **Current structures allows information to flow in all directions creating more noise than sound**
- **Having a committee structure does not ensure efficacy**
- **eGRC Steering Committee (eSC) made up of leaders**
- **eGRC Technical Committee (eTC) made up of workers**
- **You need to establish a hierarchy**

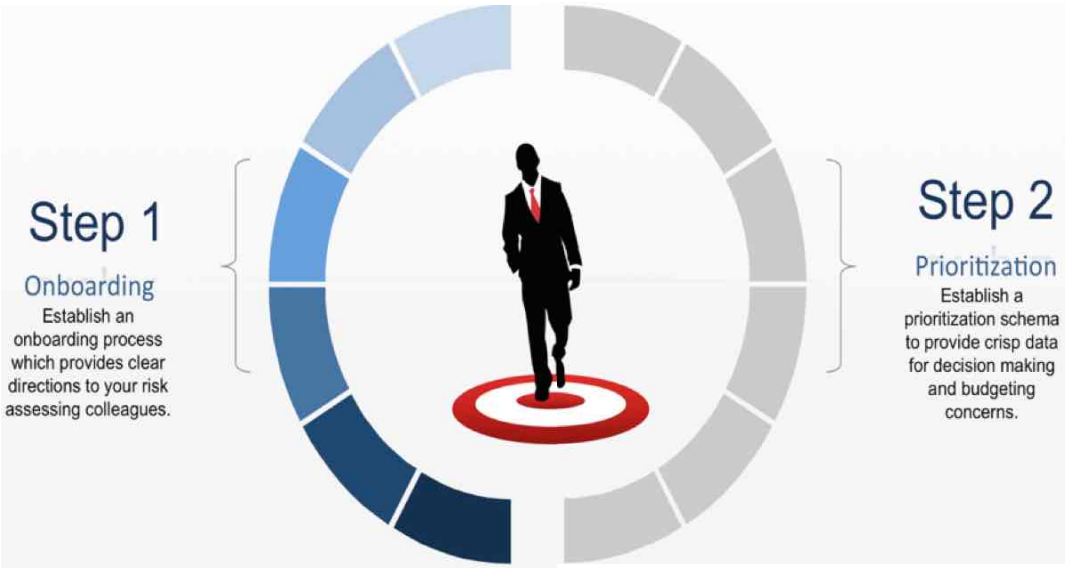


Structured Communications

- eSC functions to drive strategy and identify and track goals
- Create or implement a function to capture requests, validate maturity, manage changes and provide reporting for the eTC
- CoE provides enhanced Communications Management
- Support for gathering business metrics and centralized reporting



Center of Excellence Goals



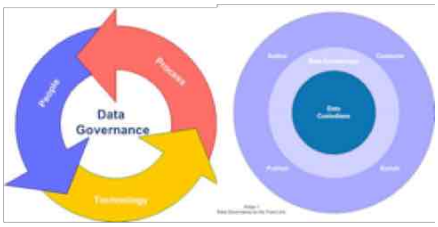
Typically Managed Architectures

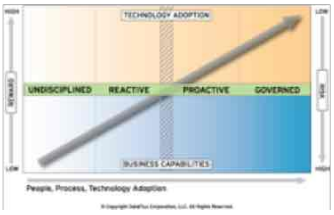
Technical committees

- Process Architecture
  - Arrangement of inputs -> transformations = value -> outputs
  - Typical elements: Functions, activities, workflow, events, cycles,
- Systems Architecture
  - Applications, software components, interfaces, projects
- Business Architecture
  - Goals, strategies, roles, organizational structure, location(s)
- Security Architecture
  - Arrangement of security controls relation to IT Architecture
- Technical Architecture/Tarchitecture
  - Relation of software capabilities/technology stack
  - Structure of the technology infrastructure of an enterprise, solution or system
  - Typical elements: Networks, hardware, software platforms, standards/protocols
- Data/Information Architecture
  - Arrangement of data assets supporting organizational strategy
  - Typical elements: specifications expressed as entities, relationships, attributes, definitions, values, vocabularies

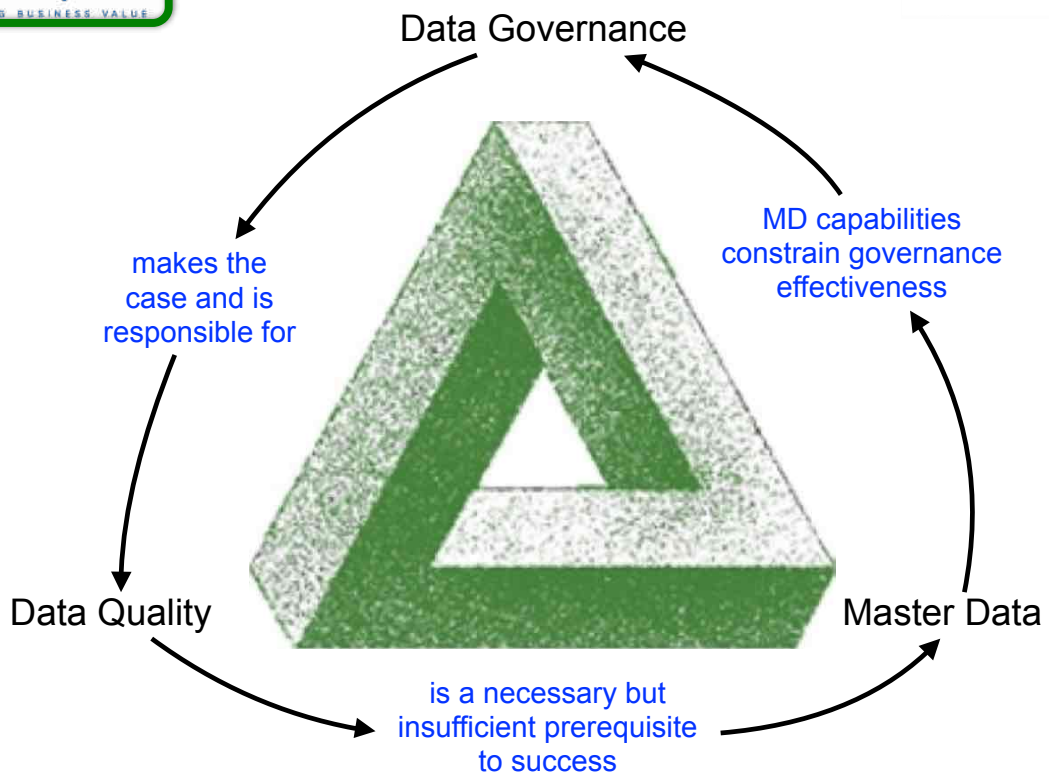
Organizational Data Governance Purpose Statement

- What does data governance mean to my organization?
  - Managing data with guidance
  - Getting some individuals (whose opinions matter)
  - To form a body (needs a formal purpose/authority)
  - Who will advocate/evangelize for (not dictate, enforce, rule)
  - Increasing scope and rigor of
  - Data-centric development practices
- Version 1



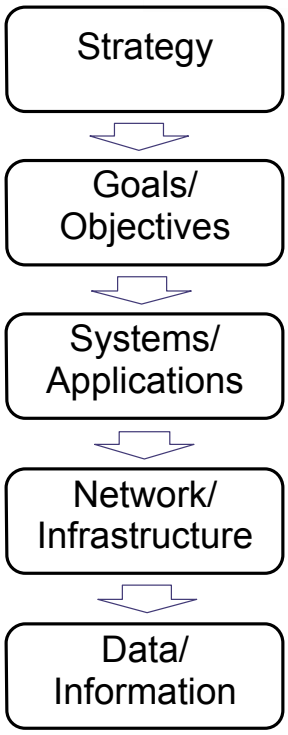


Interdependencies



Application-Centric Development

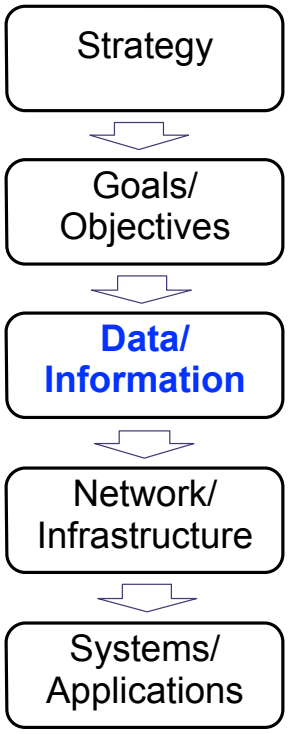
- In support of strategy, organizations develop specific goals/objectives
- The goals/objectives drive the development of specific systems/applications
- Development of systems/applications leads to network/infrastructure requirements
- Data/information are typically considered after the systems/applications and network/ infrastructure have been articulated
- Problems with this approach:
  - Ensures data is formed to the applications and not around the organizational-wide information requirements
  - Process are narrowly formed around applications
  - Very little data reuse is possible



Original articulation from Doug Bagley @ Walmart

Data-Centric Development

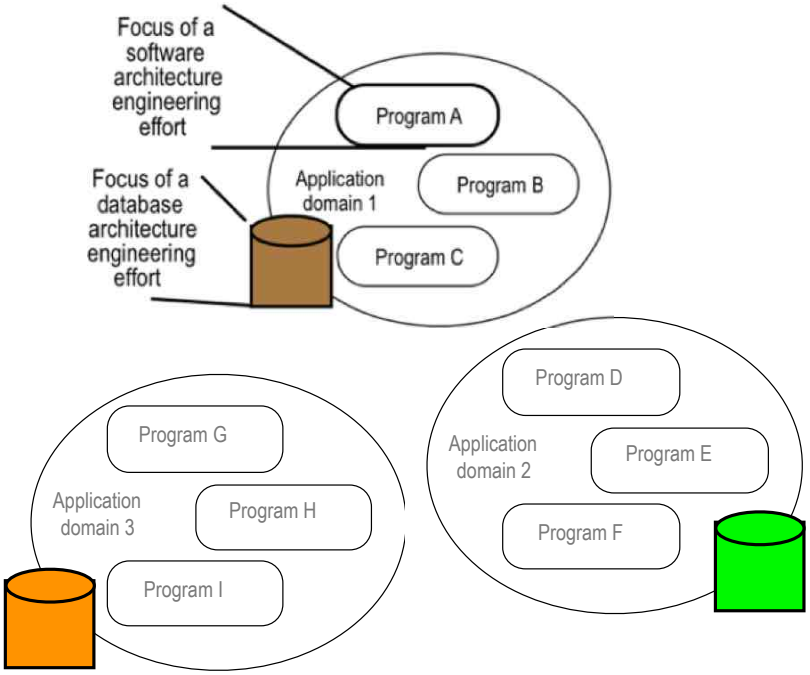
- In support of strategy, the organization develops specific goals/objectives
- The goals/objectives drive the development of specific data/information assets with an eye to organization-wide usage
- Network/infrastructure components are developed to support organization-wide use of data
- Development of systems/applications is derived from the data/network architecture
- Advantages of this approach:
  - Data/information assets are developed from an organization-wide perspective
  - Systems support organizational data needs and compliment organizational process flows
  - Maximum data/information reuse



Original articulation from Doug Bagley @ Walmart

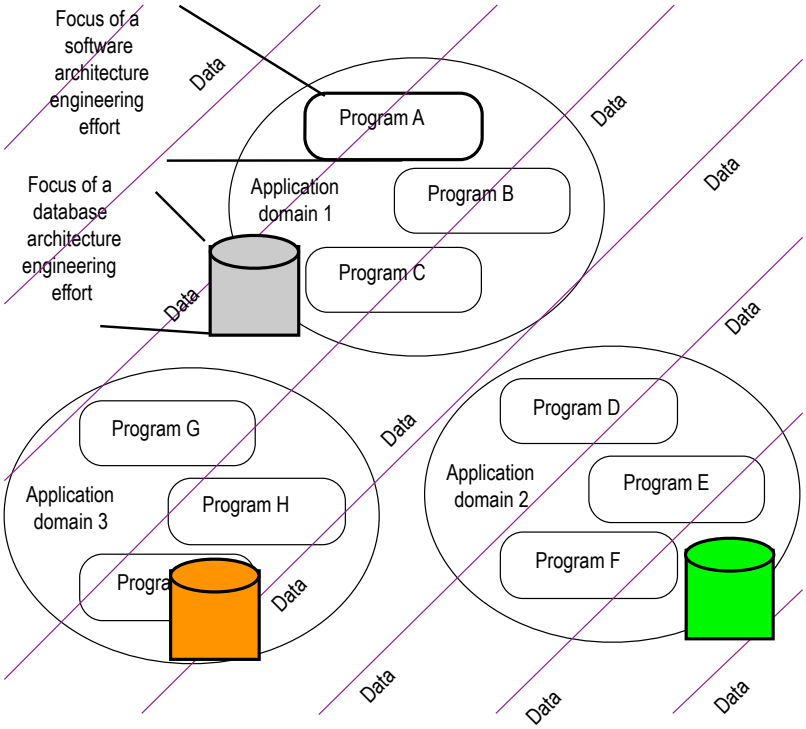
3 – Architecture Domain

Database Architecture Focus

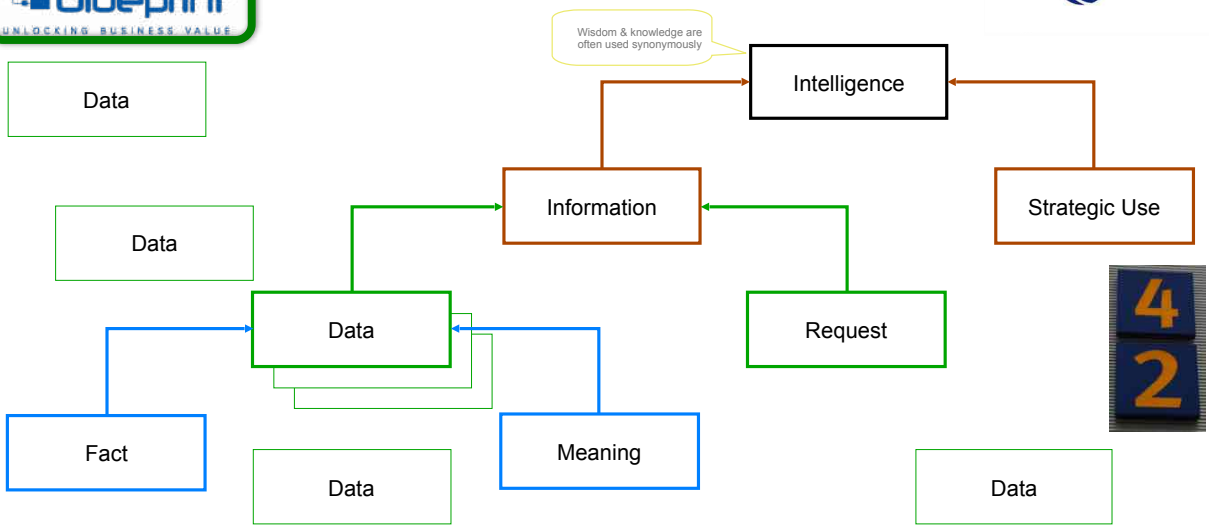


Data Architecture Focus has Greater Potential Business Value

- Broader focus than either software architecture or database architecture
- Analysis scope is on the system wide use of data
- Problems caused by data exchange or interface problems
- Architectural goals more strategic than operational



Strategic Information Use: Prerequisite



1. Each FACT combines with one or more MEANINGS.
2. Each specific FACT and MEANING combination is referred to as a DATUM.
3. An INFORMATION is one or more DATA that are returned in response to a specific REQUEST
4. INFORMATION REUSE is enabled when one FACT is combined with more than one MEANING.
5. INTELLIGENCE is INFORMATION associated with its STRATEGIC USES.
6. DATA/INFORMATION must formally arranged into an ARCHITECTURE.

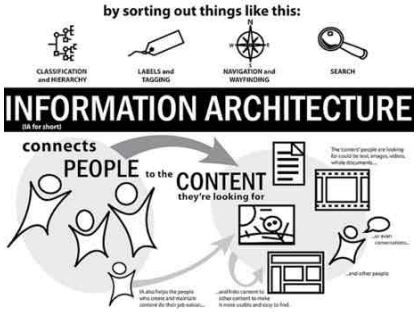
[Built on definitions from Dan Appleton 1983]

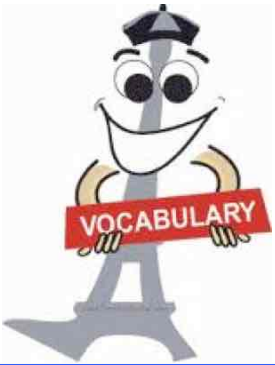
Information Architectures

- The underlying (information) design principals upon which construction is based
  - Source: http://architecturepractitioner.blogspot.com/
- … are plans, guiding the transformation of strategic organizational information needs into specific information systems development projects
  - Source: Internet
- A framework providing a structured description of an enterprise's information assets — including structured data and unstructured or semistructured content — and the relationship of those assets to business processes, business management, and IT systems.
  - Source: Gene Leganza, Forrester 2009
- "Information architecture is a foundation discipline describing the theory, principles, guidelines, standards, conventions, and factors for managing information as a resource. It produces drawings, charts, plans, documents, designs, blueprints, and templates, helping everyone make efficient, effective, productive and innovative use of all types of information."
  - Source: Information First by Roger & Elaine Evernden, 2003 ISBN 0 7506 5858 4 p.1.
- Defining the data needs of the enterprise and designing the master blueprints to meet those needs
  - Source: DM BoK

Data Architecture – Better Definition

- All organizations have information architectures
  - Some are better **understood** and **documented** (and therefore more **useful** to the organization) than others.
- Common vocabulary expressing integrated requirements ensuring that data assets are stored, arranged, managed, and used in systems in support of organizational strategy *[Aiken 2010]*





Architecture Domain

- **Identity Governance (IG) tops the list!**
- **IG feeds into Access Controls**
- **Hardware / Software aligned to IG**
- **External Access Needs defined by policy and monitored by IG**
- **Insider threat monitored by good IG**

Architecture Domain Goals

- **Step 1** - Establish or adopt a process to manage controls for access to eGRC Tool data, this requirement applies across all stakeholders.
- **Step 2** - Establish or adopt a process to appropriately size, monitor and manage your eGRC hardware and software (application, database & web).

- **Step 3** - Define the need for external access early in your rollout process. This decision will impact everything from architecture to security requirements.

END - Part 1

Have a GREAT Lunch!

Part 2 – Right After Lunch

Part 2 - (Reducing R.O.T.)

You can't secure what you can't manage

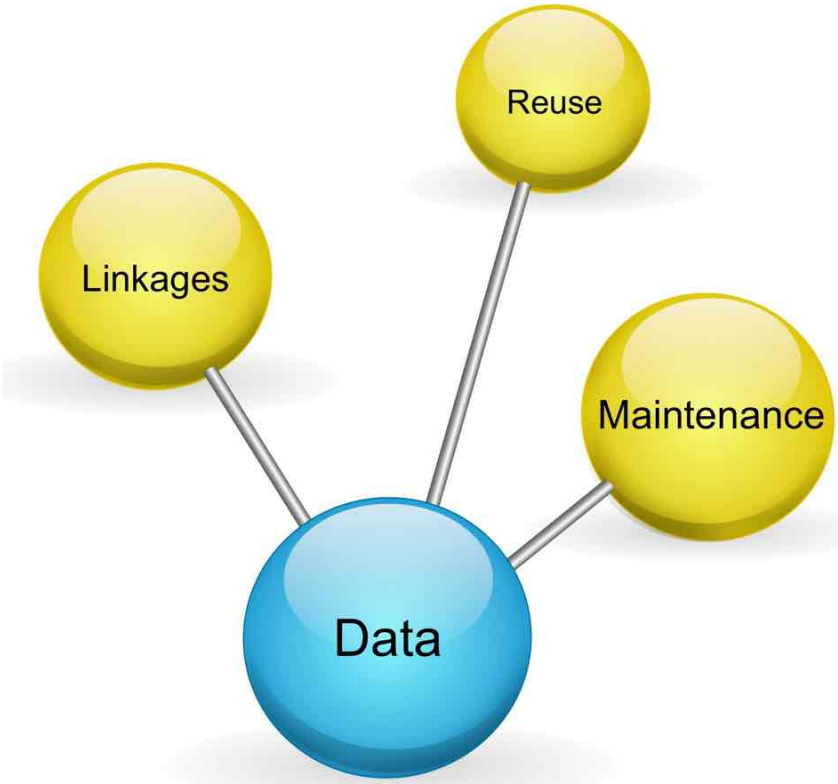
Definition R.O.T. = Redundant, Obsolete or Trivial

(origin unknown)

80% of organizational data is ROT

4 – Data Domain

Data Domain



- Data Linkages
- Data Reuse
- Data / SoR Maintenance

Data Domain Goals

- eGRC program efficacy can be easily determined by the maturity of the internal Data Governance program maturity.
- Business unit risk assessments can yield a treasure trove of data from both an eGRC perspective and from a Data.
- Data reuse can work for or against you (e.g. Business Unit).
- Data from multiple systems of records create an opportunity for a phenomenal constellation or a great.
- One of the primary goals of this union is to manage GOVERNANCE!

Governance Data vs. the Governance of Data

Asset: A resource controlled by the organization as a result of past events or transactions and from which future economic benefits are expected to flow [Wikipedia]

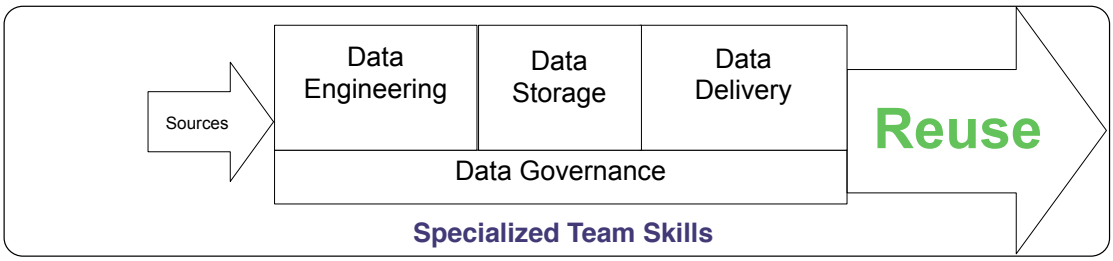
- Today, data is the most powerful, yet underutilized and poorly managed organizational asset
- Data is your
  - Sole
  - Non-depleteable
  - Non-degrading
  - Durable
  - Strategic
- Asset
  - Data is the new oil!
  - Data is the new (s)oil!
  - Data is the new bacon!

	Data Assets	Financial Assets	Real Estate Assets	Inventory Assets
Non-depletable	Available for subsequent use	Can be used up		Can be used up
Non-degrading	√	√	Can degrade over time	Can degrade over time
Durable	Non-taxed		√	√
Strategic Asset	√	√	√	√

- Our mission is to unlock business value by
  - Strengthening your data management capabilities
  - Providing tailored solutions, and
  - Building lasting partnerships

We believe ...

What is Data Management?



Understanding the current and future data needs of an enterprise and making that data effective and efficient in supporting business activities

Aiken, P, Allen, M. D., Parker, B., Mattia, A., "Measuring Data Management's Maturity: A Community's Self-Assessment" *IEEE Computer* (research feature April 2007)

Measuring Data Management Practice Maturity: A Community's Self-Assessment

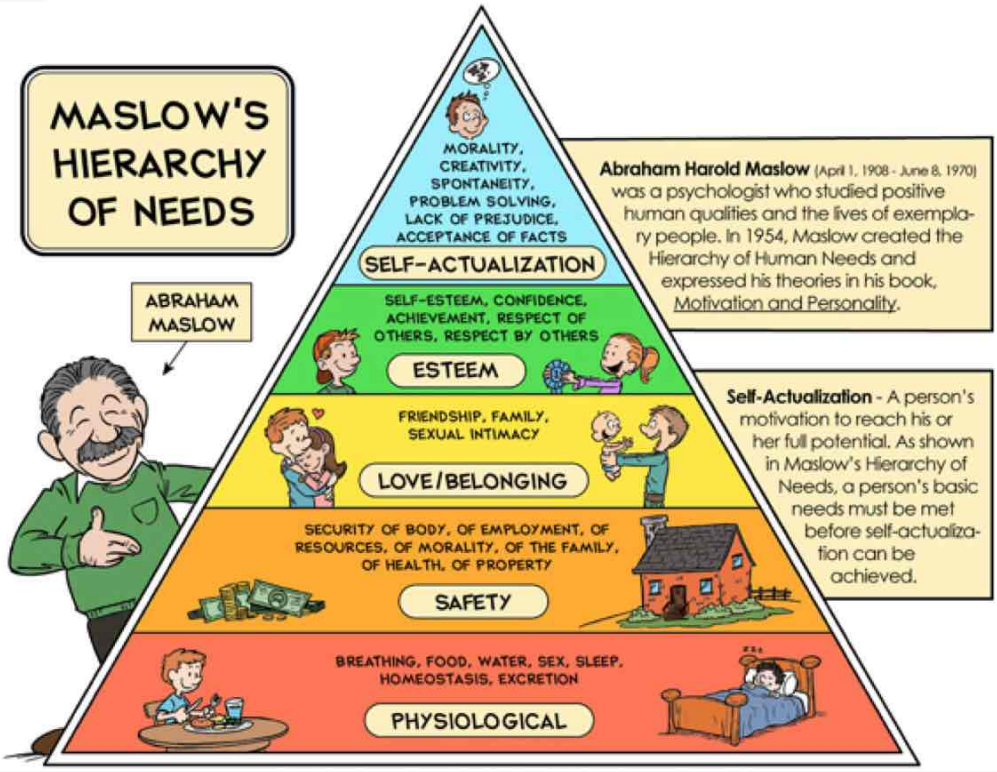
Data management practices connect data sources and uses in an organized and efficient manner

- Storage
- Engineering
- Delivery
- Governance

When executed, engineering, storage, and delivery implement governance

Note: does not well-depict data reuse

Maslow's Hierarchy of Needs

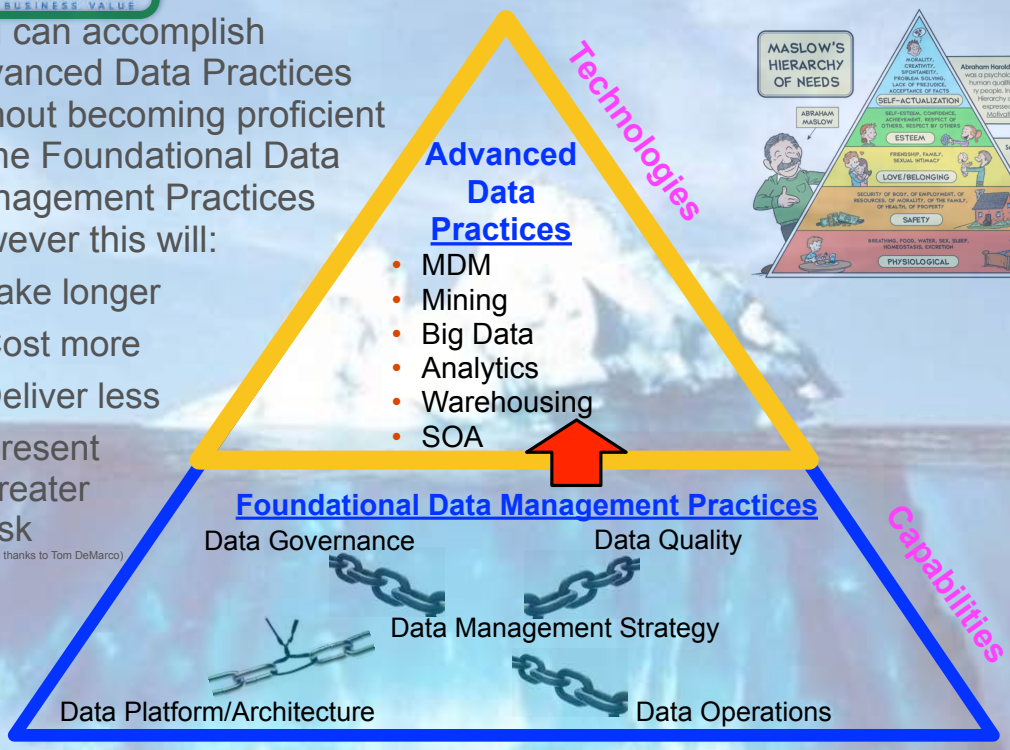


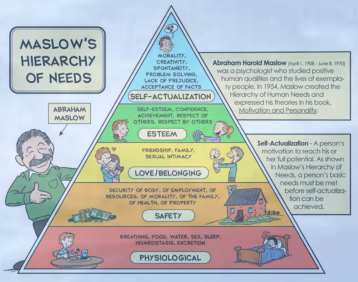
Data Management Practices Hierarchy

You can accomplish Advanced Data Practices without becoming proficient in the Foundational Data Management Practices however this will:

- Take longer
- Cost more
- Deliver less
- Present greater risk

(with thanks to Tom DeMarco)





DMM℠ Structure of 5 Integrated DM Practice Areas

Data Management Strategy
- Data Management Strategy
- Communications
- Data Management Function
- Business Case
- Funding

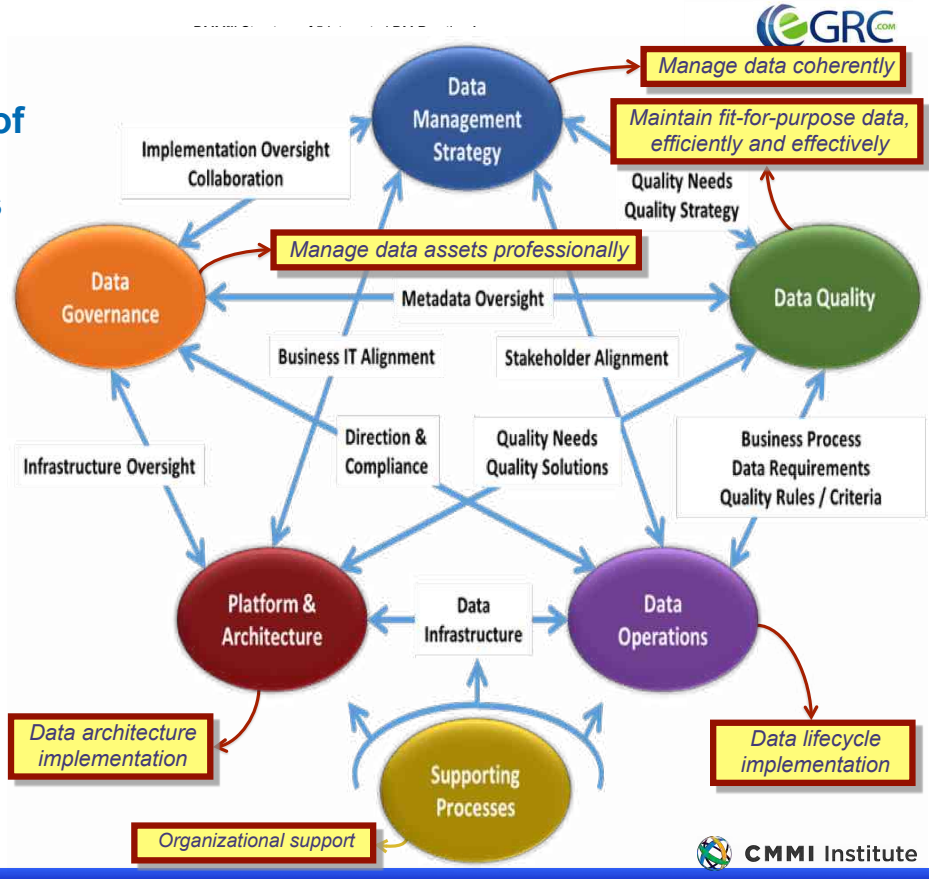
Data Governance
- Governance Management
- Business Glossary
- Metadata Management

Data Quality
- Data Quality Strategy
- Data Profiling
- Data Quality Assessment
- Data Cleansing

Data Operations
- Data Requirements Definition
- Data Lifecycle Management
- Provider Management

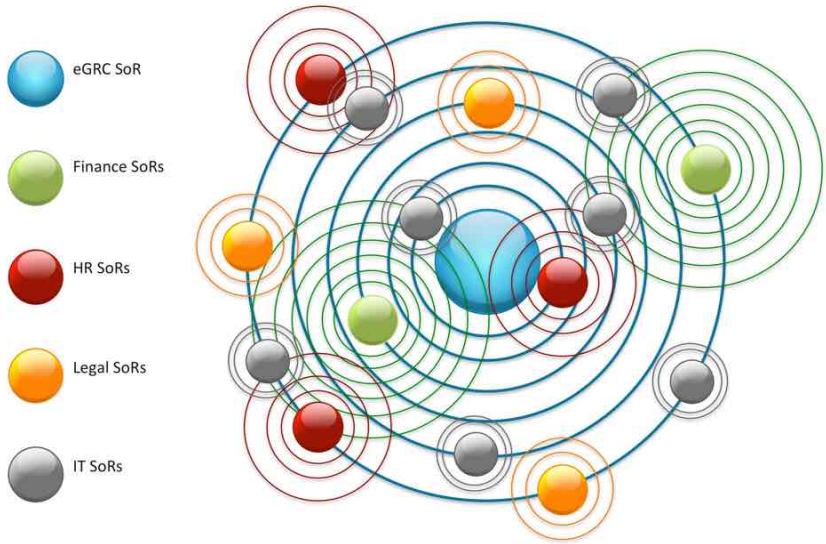
Platform & Architecture
- Architectural Approach
- Architectural Standards
- Data Management Platform
- Data Integration
- Historical Data, Archiving and Retention

Supporting Processes
- Measurement and Analysis
- Process Management
- Process Quality Assurance
- Risk Management
- Configuration Management



#5 – System of Record (SoR) Domain / Master Data Management

System of Record Domain



- Document SoRs Owners
- Identify SoR Refresh Cycle
- Ensure the continuity of SoR data

System of Record Owners

- Identify SoRs and their owners, both technical and business owners are required
- Understand what data is flowing between the two systems and how often
- Determine which system is authoritative and enforce adoption and maintenance roles
- Create and maintain a data dictionary of field types and owners to ensure consistency

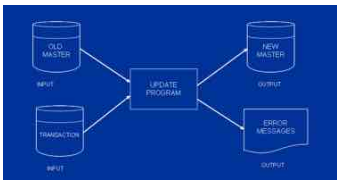
SoR - Change Control Goals

- Adopt a formal change control process that aligns with a rapid application development process. Ensure that each SoR has a change control program.
- Routine management of changes will provide the necessary controls. Tracking those controls will determine health of Governance program.

- A change reviewed in a group and on a consistent basis ensures that everyone is kept in the loop.
- Changes can be tracked by the Technical Committee and communicated to the Steering Committee to oversight and controls.

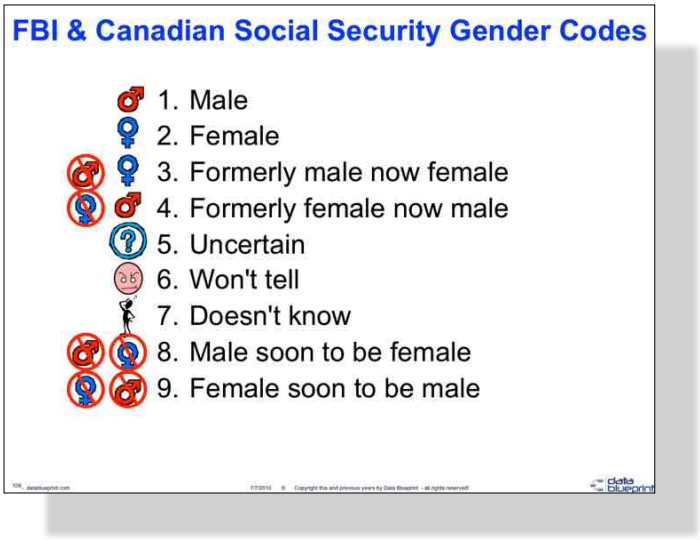
Master Data Management Definition

- as opposed to mobile device management
- Gartner holds that MDM is a discipline or strategy
  - "*… where the business and the IT organization work together to ensure the uniformity, accuracy, semantic persistence, stewardship and accountability of the enterprise's official, shared master data*"
- Sold as solution
- Official, consistent set of identifiers - examples of these core entities include:
  - Parties (customers, prospects, people, citizens, employees, vendors, suppliers, trading partners, individuals, organizations, citizens, patients, vendors, supplies, business partners, competitors, students, products, financial structures *LEI*)
  - Places (locations, offices, regional alignments, geographies)
  - Things (accounts, assets, policies, products, services)
- Provide context for transactions
- From the term "Master File"



Reference Data vs. Master Data

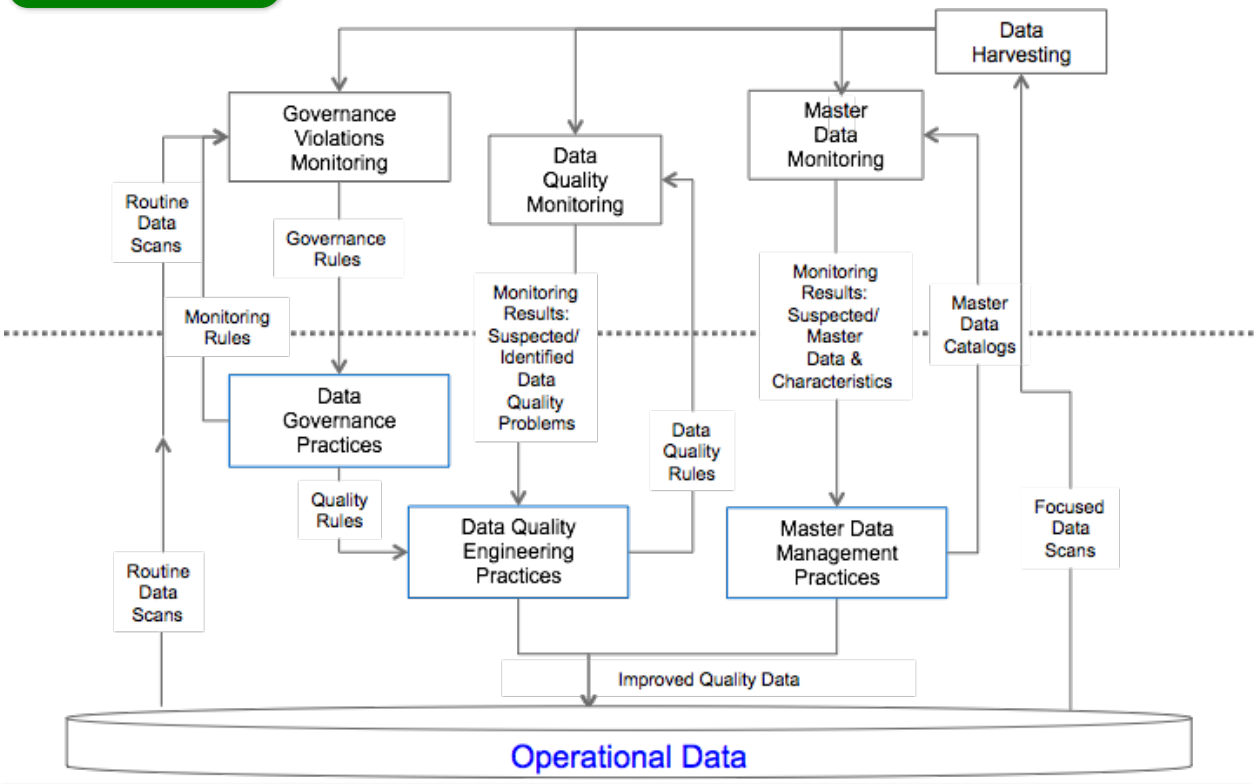
- Reference Data:
  - Control over defined domain values (vocabularies) for standardized terms, code values, and other unique identifiers
  - *The fact that we maintain 9 possible gender codes*
- Master Data:
  - Control over master data values to enable consistent, shared, contextual use across systems
  - *The "golden" source of the gender of your customer "Pat"*



Both provide the context for transaction data

from The DAMA Guide to the Data Management Body of Knowledge © 2009 by DAMA International

Interactions

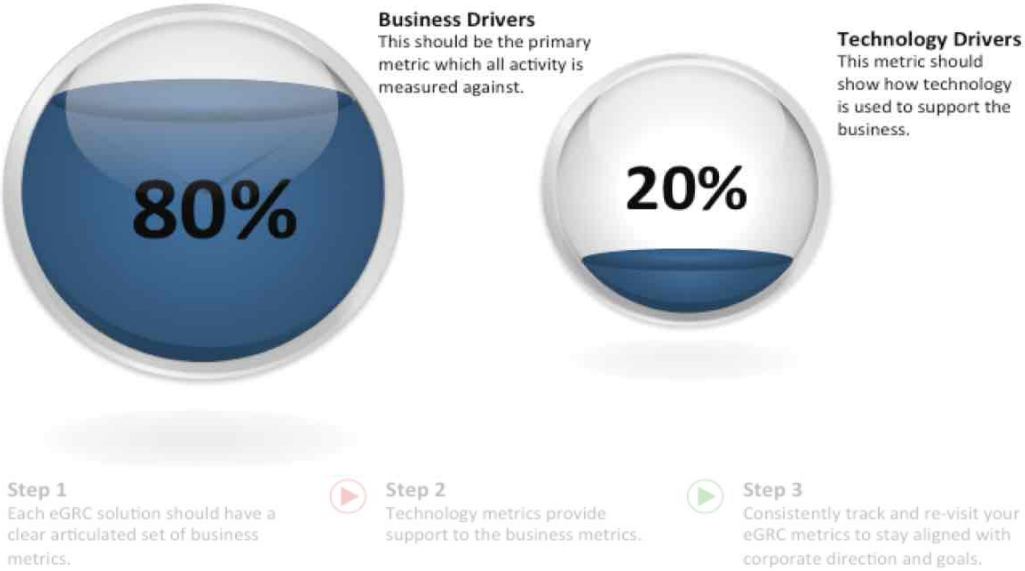


6 – Metrics / Reporting

Metrics Domain Goals

- Metrics determine whether the solutions are functioning as intended
- Metrics are different from reporting, both are equally important
- Metrics should be periodically validated with the stakeholders
- Metrics should align to the strategy and architecture sections of the program as well

Metrics Domain



Reporting Domain Goals

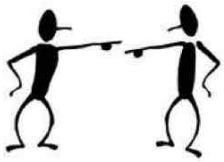
- The primary goal of the reporting domain is to ensure that each stakeholder has provided reporting requirements specific to their risk assessing functions.
- Alignment to leadership strategy will ensure continued visibility and support from the highest levels of management.
- Simplified reporting (Red, Yellow, Green) provides executives the opportunity to hone in on problem areas. Drill-down reporting allows curious leaders to dig deeper into trouble spots.
- Verify reporting requirements often and align with regulatory needs to ensure accurate data representation.

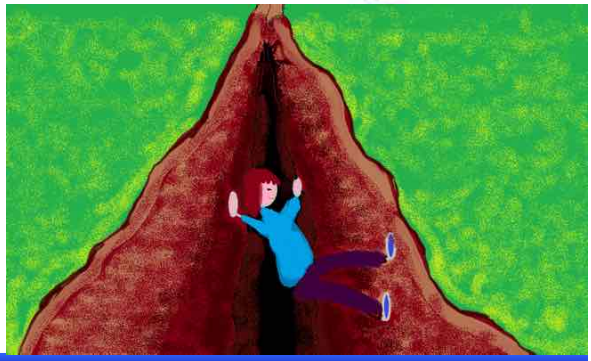
Reporting Domain

- Value of program goals becomes apparent
- One dataset provides different reports for different audiences
- Value of Data Governance important for reporting needs
- Reporting can save internal conflicts

Confusion

- IT thinks data is a business problem
  - *"If they can connect to the server, then my job is done!"*
- The business thinks IT is managing data adequately
  - *"Who else would be taking care of it?"*





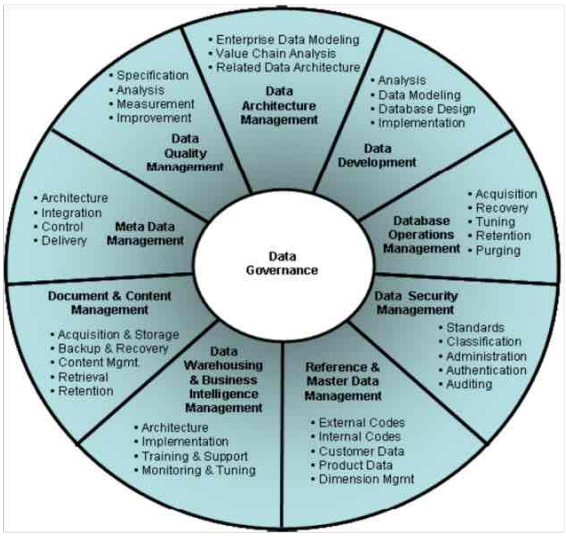
Systems Thinking

- A framework that is based on the belief that the component parts of a system can best be understood in the context of relationships with other systems, rather than in isolation.
- The only way to fully understand why a problem or element occurs and persists is to understand the part in relation to the whole.

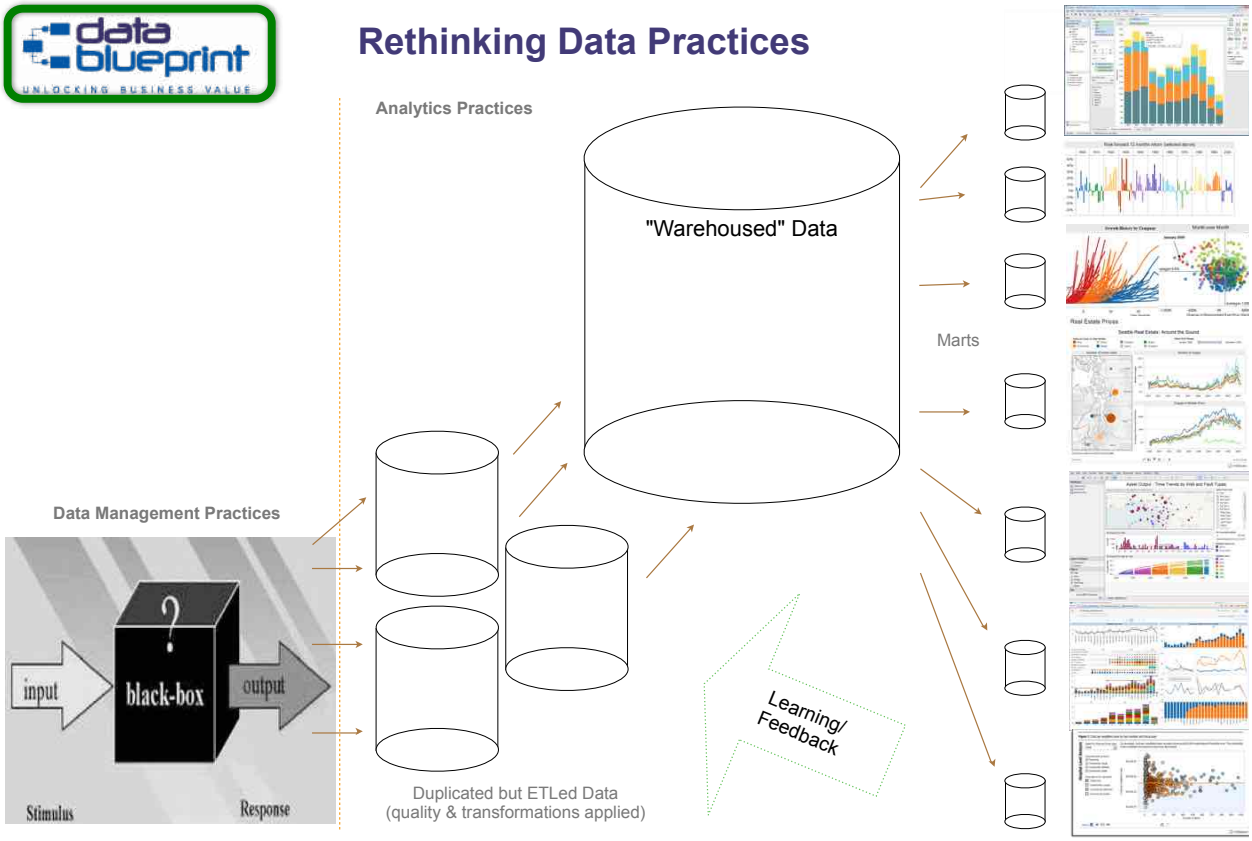
Capra, F. (1996) *The web of life: a new scientific understanding of living systems* (1st Anchor Books ed). New York: Anchor Books. p. 30

IT Projects Treated as Systems

- Beginning
  - Project context
  - Architecture
  - Master data management (MDM)
  - Project implementation (app-centric)
- Middle
  - Diagnosis
  - Systems thinking
  - Data quality engineering
- End
  - Data governance
  - Project success
  - Defining success (data-centric)
  - It is not really a project …



Rethinking Data Practices



Benefits of Marriage

- Optimized use of agency data across both domains eGRC & Data Management
- Clear marriage goals will ensure agency targets are accomplished efficiently
- Cost efficiencies are an additional benefit of this union
- Assess once, reuse often is a key element of this union

Marriage Counseling

- Both parties must agree that the problem exists
- Each side must be willing to give up some control and potentially budget
- Operational leaders are the children in the relationship, they are the reason to go forth
- The counselor must have the appropriate role to mediate to resolution (executive sponsorship)

6 Steps to Marital Bliss

Step 1	Commit to gains no matter the pains
Step 2	Data Governance vs. Governing of Data
Step 3	Know your data, increase your relationship maturity
Step 4	Data is the LOVE in this relationship
Step 5	Governance exists to bring harmony
Step 6	eGRC + Data Management = the perfect union in private/public Sectors

Contact Peter

Name: Dr. Peter Aiken

Peter@Datablueprint.com

Web: www.datablueprint.com

Phone: 804.382.5957

Twitter: @datablueprint

Contact Lorne

Name: Lorne O. Joseph II

Lorne.Joseph@eGRC.COM

Web: www.eGRC.COM

Phone: 855.WHY.eGRC

Twitter: @Whatisegrc