Basel Committee On Banking Supervision 239 (aka BCBS239): *A Template for Data Governance?*

January 2016

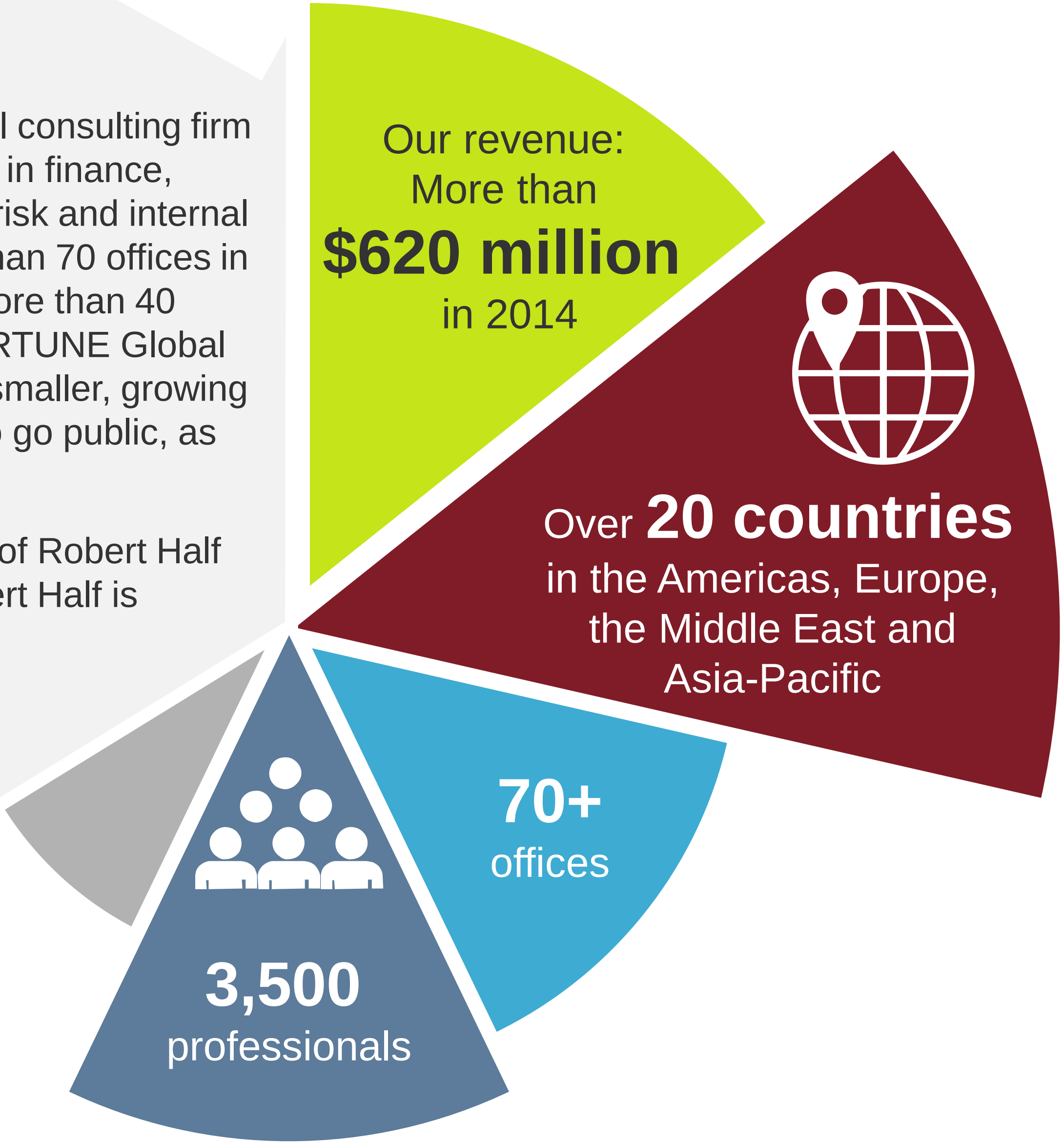
Powerful Insights.
Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.

WHO WE ARE

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.



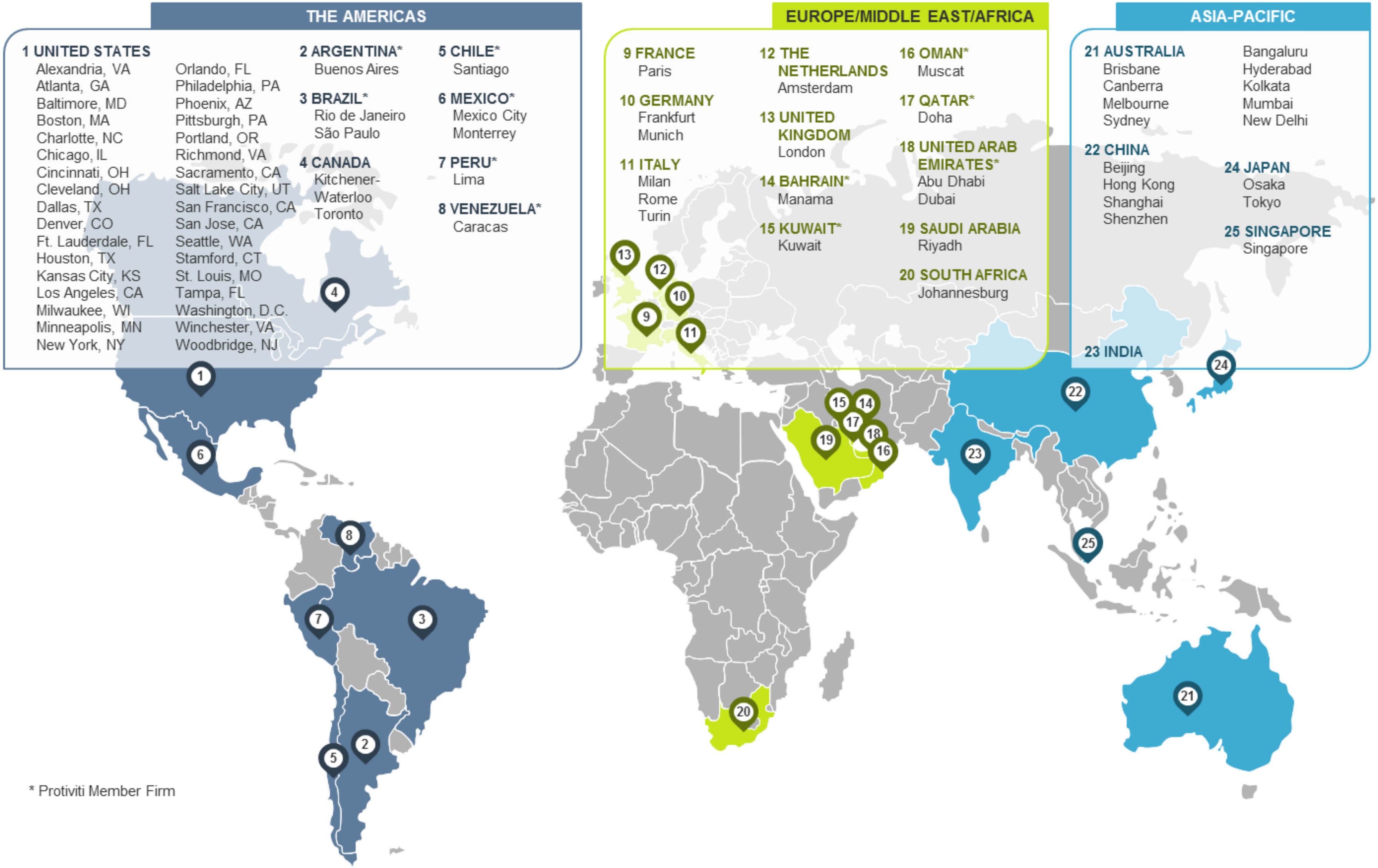
Our revenue:
More than
$620 million
in 2014

Over **20 countries**
in the Americas, Europe, the Middle East and Asia-Pacific

70+
offices

3,500
professionals

GLOBAL PRESENCE



THE AMERICAS

1 UNITED STATES
Alexandria, VA
Atlanta, GA
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

2 ARGENTINA*
Buenos Aires

3 BRAZIL*
Rio de Janeiro
São Paulo

4 CANADA
Kitchener-Waterloo
Toronto

5 CHILE*
Santiago

6 MEXICO*
Mexico City
Monterrey

7 PERU*
Lima

8 VENEZUELA*
Caracas

EUROPE/MIDDLE EAST/AFRICA

9 FRANCE
Paris

10 GERMANY
Frankfurt
Munich

11 ITALY
Milan
Rome
Turin

12 THE NETHERLANDS
Amsterdam

13 UNITED KINGDOM
London

14 BAHRAIN*
Manama

15 KUWAIT*
Kuwait

16 OMAN*
Muscat

17 QATAR*
Doha

18 UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

19 SAUDI ARABIA
Riyadh

20 SOUTH AFRICA
Johannesburg

ASIA-PACIFIC

21 AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

22 CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

23 INDIA
Bangaluru
Hyderabad
Kolkata
Mumbai
New Delhi

24 JAPAN
Osaka
Tokyo

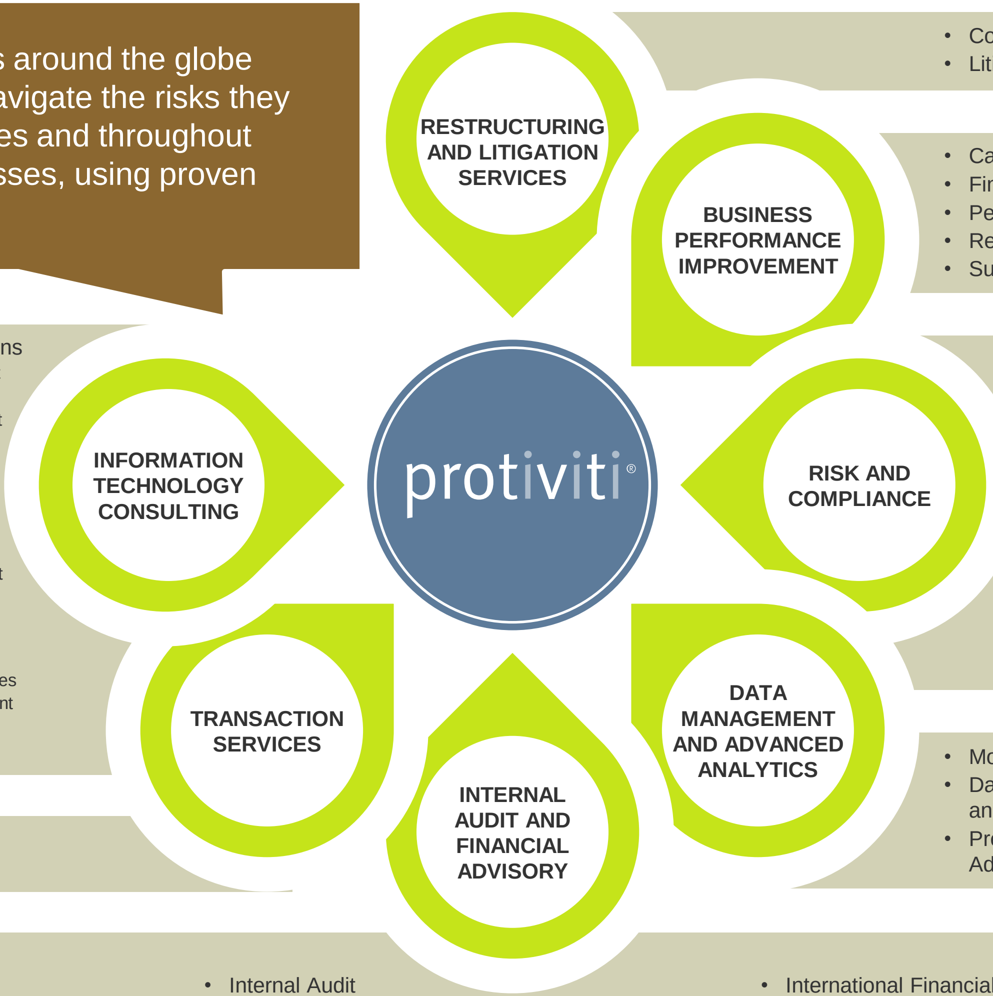
25 SINGAPORE
Singapore

* Protiviti Member Firm

protiviti®

PROTIVITI'S SOLUTION OFFERINGS

Protiviti helps companies around the globe identify, measure, and navigate the risks they face, within their industries and throughout their systems and processes, using proven **value-added solutions**:



protiviti®

RESTRUCTURING AND LITIGATION SERVICES

- Corporate Restructuring and Recovery
- Litigation Consulting

BUSINESS PERFORMANCE IMPROVEMENT

- Capital Projects and Contracts
- Finance Optimization Services
- Performance and Information Management
- Revenue Enhancement
- Supply Chain

RISK AND COMPLIANCE

- Credit Risk
- Customer Engagement
- Enterprise Risk Management (ERM)
- Market and Commodity Risk
- Model Risk and Capital Management
- Operational Risk
- Strategy Communications and Change Enablement
- Anti-Money Laundering
- Regulatory Compliance

DATA MANAGEMENT AND ADVANCED ANALYTICS

- Model Risk Management
- Data Governance, Warehousing and Business Intelligence
- Predicative Modeling and Advanced Analytics

INTERNAL AUDIT AND FINANCIAL ADVISORY

- Data Mining and Analytics
- Financial Remediation and Reporting Compliance
- Financial Investigations
- Internal Audit
- Fraud Risk Management
- Internal Audit Quality Assurance Reviews
- International Financial Reporting Standards (IFRS)
- IT Audit Services
- SOX and Financial Reporting Controls Compliance

TRANSACTION SERVICES

- M&A Divestiture
- Public Company Transformation

INFORMATION TECHNOLOGY CONSULTING

- Technology Strategy and Operations
  - IT Governance and Risk Management
  - IT Operations Improvement
  - IT Portfolio and Program Management
  - IT Strategy and Alignment
- Enterprise Application Solutions
  - ERP Solutions
  - Software Services
  - Business Intelligence
  - eDiscovery and Records Management
  - Risk Technologies
  - End-User Applications Services
- Security and Privacy Solutions
  - Security Program and Strategy Services
  - Data Security and Privacy Management
  - Identity and Access Management
  - Vulnerability and Penetration Testing

BCBS239

A TEMPLATE FOR DATA GOVERNANCE?

The Basel Committee on Banking Supervision (BCBS) 239, originally issued in January of 2013 with compliance dates of January of 2016 for larger Financial Institutions (G-SIBs), has further codified the requirements for specific steps around Enterprise Data Governance.   These guidelines are specific to helping organizations measure and aggregate their Risk (a.k.a. Risk Data Aggregation, or RDA) but offer several principles solely focused on governance for the Risk Data.

These guidelines focus on items such as understanding data definitions, linage, and quality throughout the full data lifecycle.   During our discussion we will walk through the Data Governance impacts of BCBS239 on Banking, along with providing ideas on how some of these data governance principles might be applied to other industries as best practices.

BCBS239

LEARNING OBJECTIVES / OVERVIEW

- Overall Enterprise Data Governance Drivers within Financial Services
  - Why now?
  - Major regulatory drivers;

- BCBS 239 / RDA – what is it?
  - Definitions for the Guidelines;
  - Areas of coverage;
  - Specific Principles;
  - Risks / Compliance concerns;

- Different components / approach examples;

- Q&A

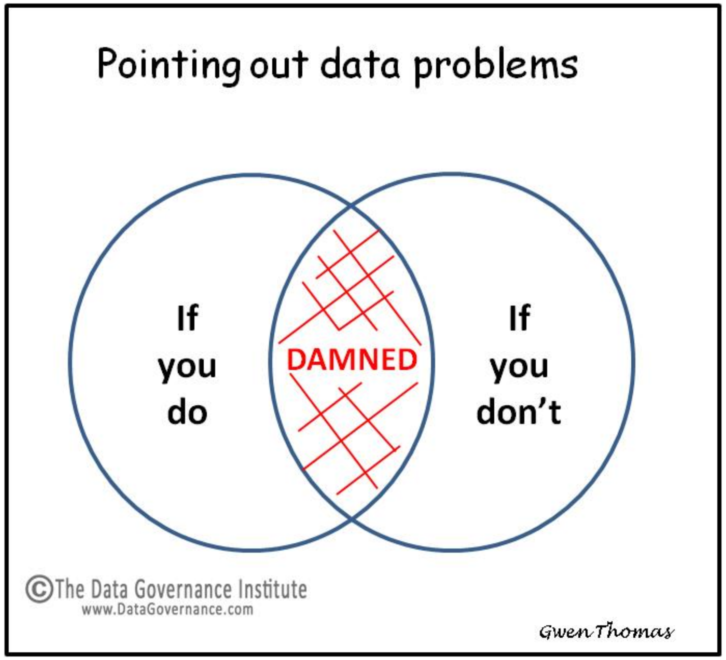
ENTERPRISE DATA GOVERNANCE

DRIVERS WITHIN FINANCIAL SERVICES

Regulators – especially post the Banking Collapse – are paying increased attention to Data Governance, especially when viewing the data they receive from firms responding to compliance reporting.

"One of the most significant lessons learned from the global financial crisis that being in 2007 was the banks' information technology (IT) and data architectures that were inadequate to support the broad management of financial risks."

- Introduction sentence to the BCBS Principles for Effective Risk Data Aggregation;



FSI / DATA GOVERNANCE

RECENT TRENDS

Financial Services firms are continuing to face pressure to effective management their Enterprise Data assets. Regulators, such as the Fed and OCC, are specifically looking to understand existing Enterprise Data Governance programs that are in place and how those are being leveraged to address specific stress testing and other questions within the Institutions.

CCAR Stress Testing

❑ 14M/Q are predominately a data sourcing and aggregation exercises to complete the templates

❑ 14A model development needs current + historical data in order to develop an effective models

❑ Regulators demand strong data governance, data quality and internal controls around data processes

❑ Regulators demand strong data infrastructure to include business glossary, data dictionary, lineage, issues management

❑ Data quality (edit checks) requires demonstrated improvement by the bank

❑ Data must be reconciled to FR Y-9C and other financial reports

AML

❑ Significant concern across most banking institutions

❑ Key business processes require high quality customer data for customer risk scoring and transaction monitoring

❑ Consistently defined customer data is required to drive customer due diligence, enhanced due diligence, customer risk scoring and transaction monitoring processes

❑ Data quality and integrity problems lead to increased operational costs due to false positives; Subsequently the lack of quality data increases the risk of not identifying AML activities which could lead to significant fines and regulatory action

❑ Data governance standards across customer data improve

Risk Data Aggregation (BCBS 239)

❑ Common set of principles across all risk types (Credit, Market, Operational, Fiduciary, Interest-Rate, Liquidity, etc)

❑ Regulatory driven requirements to improve risk data

❑ Applicable to G-SIBs by January 2016—Recommended to be rolled out across D-SIBs subsequently (tentatively 2017-2018)

❑ Principles are driving significant improvements in data governance and infrastructure as foundation for improving risk data aggregation and reporting

❑ Basic principles align closely with data governance best practices

protiviti®

FSI REGULATORY MAPPINGS

FOR DATA GOVERNANCE

Transparency

- **Dodd-Frank Act Title IV, VII, X, XIV =** US framework for regulation of swaps markets, hedge funds, CFPB, mortgage, Volker
- **EMIR** – European Market Infrastructure Regulation (EU version of Dodd-Frank Title VII on derivatives transparency).
- **Regulation AB2** = regulations on asset backed securities (unravel links between loan, tranches, pool, etc.).
- **FATCA** = individual reporting of foreign accounts and FSI reporting of foreign financial accounts about US clients
- **UCITS** = Undertakings for Collective Investment in Transferable Securities (EU Directive on simplification of prospectus and their expression using clear, accessible and standardized data).
- **AIFMD** – Alternative Investment Fund Managers Directive (EU proposed law to provide more oversight and transparency to hedge funds and private equity).

Capital Risk/Stress

- **Dodd-Frank Act Title I =** the financial stability component (creates Financial Stability Oversight Council and OFR)
- **EU System of Financial Supervision =** establishment of the European Systemic Risk Board (and ESFS)
- **Basel Principles for Effective Risk Data Aggregation and Reporting** = implementation of a "data control environment" and healthy "risk appetite framework" within systemically important financial institutions
- **Basel III** – global regulatory standard on bank capital adequacy, stress testing and market liquidity risk.
- **CCAR** = Comprehensive Capital Analysis and Review (stress test methodology in the US; CCAR reporting is putting lots of pressure on data alignment and comparability. This includes the FR Y-9C (Bank Holding Company Capital Report) and FR Y-14Q (detailed 'show your calculation methodology work for BHC). This is the US version of Basel III.
- **Solvency II** – EU Directive that harmonizes insurance regulation (requirements for capital reserve and reduction of risk of insolvency) – to be implemented January 2014.

Harmonization

- **MiFID II** – Revised Markets in Financial Instruments Directive (mostly about trading, but does require common instrument identification for consolidated pricing).
- **ACORD** – Insurance standards development body (UK) likely to be mandated as the format for reporting.
- **Regulation SCI** – SEC proposed Regulation Systems Compliance and Integrity (to ensure that core infrastructure is functional)
- **COREP** = Common Reporting requirements (developed by Committee of European Banking Supervisors (CEBS) with the goal of developing a supervisory reporting framework based on common data standards and formats.
- **FSB Templates** = Common Data Template for G-SIB's seeking to harmonize the data compounding methodology for reporting.

** Source: EDM COUNCIL – Protiviti is a member of the EDM Council.*

BCBS 239 / RISK DATA AGGREGATION

WHAT IS RISK DATA AGGREGATION?

The Basel Committee on Banking Supervision (BCBS) issued a set of 14 principles (the Principles or BCBS 239) to strengthen banks' Risk Data Aggregation (RDA) capabilities and risk reporting practices. Of these, 11 focus on the key areas listed below with the remaining three being focused on Supervisory Review.

Overarching Governance & Infrastructure

- Risk data aggregation capabilities and risk reporting practices should be subject to strong governance and high standards of validation.
- A bank should design, **build and maintain data and IT architecture** that fully supports risk data aggregation and risk reporting practices in both normal and stress/crisis scenarios.
- A bank should establish **integrated data taxonomies, architecture, and uniform naming conventions across the banking group**.
- Roles and responsibilities should be established as they relate to **ownership and quality of risk data**.

Risk Data Aggregation Capabilities

- A bank should be able to generate **complete**, **accurate**, and **reliable risk data in timely manner** in both normal and stress/crisis scenarios.
- A bank should measure and monitor the accuracy and completeness of data and develop appropriate escalation channels and action plans to rectify poor data quality.
- A bank should have a "dictionary" of concepts so that data is defined consistently
- Risk data aggregation capabilities should be flexible and adaptable to meet a broad range of demand /ad hoc requests.

Risk Reporting Practices

- Risk management reports **should accurately, precisely, and clearly convey aggregated risk data** across all material risks areas within the organization. Reports should be easy to understand, yet comprehensive enough to facilitate informed decision-making.
- The board and senior management (or other recipients as appropriate) should set the frequency of risk management reporting production and distribution frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change.
- Risk management reporting should be distributed while ensuring confidentiality is maintained.

BCBS 239 / RISK DATA AGGREGATION

WHO IS IMPACTED AND WHEN?

BCBS 239 had an initial deadline of January 1st, 2016 for compliance. A drafting of the Principles was released in 2012 with the original publication being released in January of 2013. There are a limited set of Global Financial Services organizations (G-SIBs, or Globally Systemically Important Banks) that were covered under the initial publication and due date of January 2016.

A few Interesting facts on compliance:

- *Though published by the Basel Committee, Domestic Regulators (e.g. US Fed) are responsible for reviewing compliance for their own regulated entities and there is not a set penalty structure established;*

- *Banks were asked to provide a self assessment of their overall compliance and it has been reported that up to 14 of 31 Banks may not be in full compliance; and*

- *D-SIBs, or Domestic Systemically Important Banks were not specifically mandated within the initial publication of BCBS239 the Committee "Strongly Suggested" that National Supervisors look to hold them to the same standards within three years of their designation as a D-SIB.*

BCS 239 / RISK DATA AGGREGATION

WHAT ARE WE TRYING TO ANSWER?

Best Practices published through the EDM Council note that an effective RDA should be able to address the following, at a minimum:

Can you *identify your authoritative sources of data?*
Can you *define your data lineage?*
Can you *uniquely identify your counterparties?*
Can you *identify your risk to counterparty exposures?*
Can you *rapidly respond to a contagion or risk crisis?*

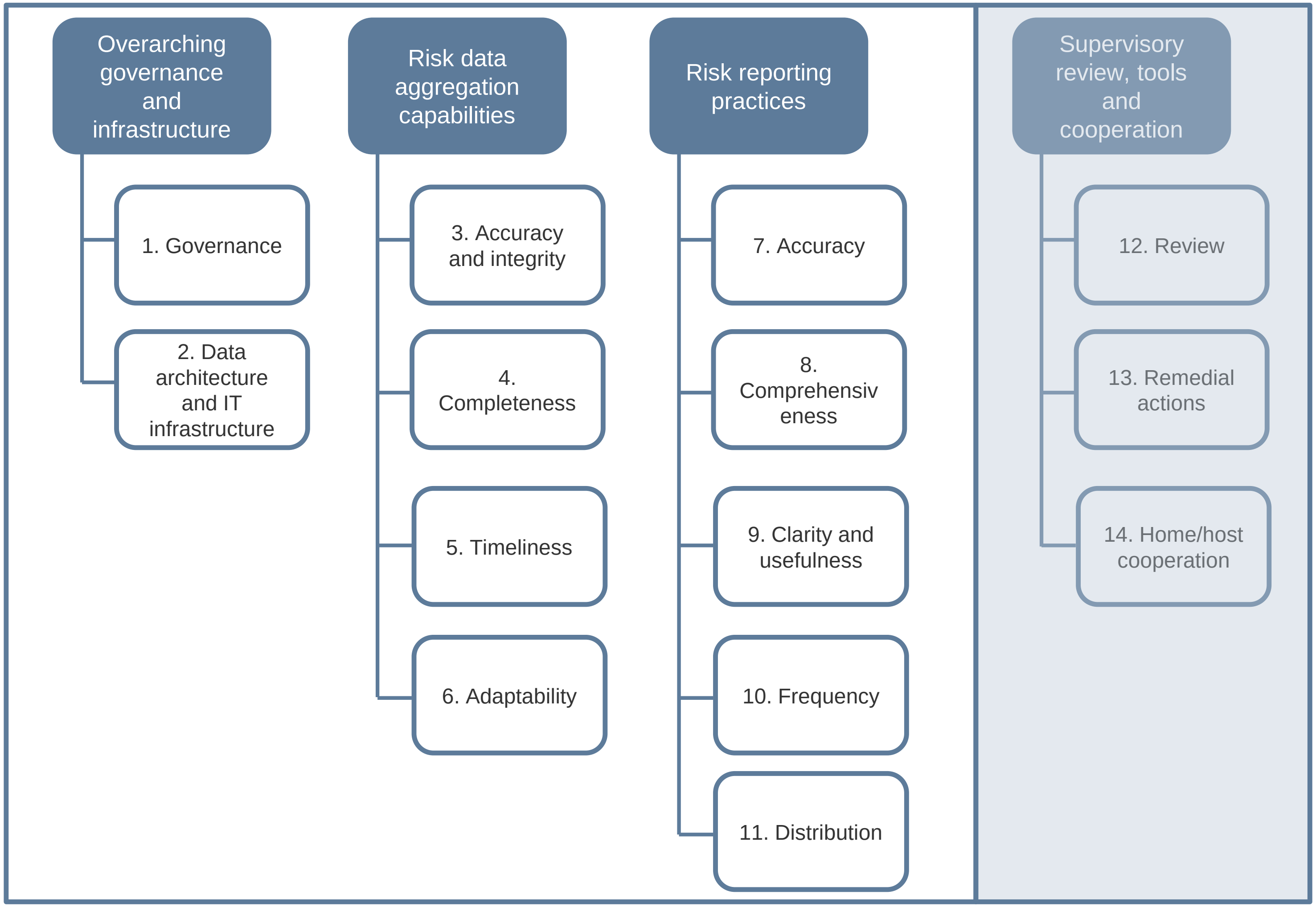
Do you *have the infrastructure to properly manage your data?*
Do you *have the governance in place to define and harmonize your data?*
Do you *have the governance in place to ensure appropriate use of your data?*
Do you *have the org structures in place to ensure data is aligned to critical business and risk operations?*

Will you *be able to fund and prioritize your infrastructure changes?*
Will you *be able to harmonize your data using common language?*
Will you *be ready to provide evidence of infrastructure progress by 2016 January?*

BCBS 239

WHAT ARE THE PRINCIPLES?

Overall the principles are broken into 4 high level categories:



Overarching governance and infrastructure
- 1. Governance
- 2. Data architecture and IT infrastructure

Risk data aggregation capabilities
- 3. Accuracy and integrity
- 4. Completeness
- 5. Timeliness
- 6. Adaptability

Risk reporting practices
- 7. Accuracy
- 8. Comprehensiveness
- 9. Clarity and usefulness
- 10. Frequency
- 11. Distribution

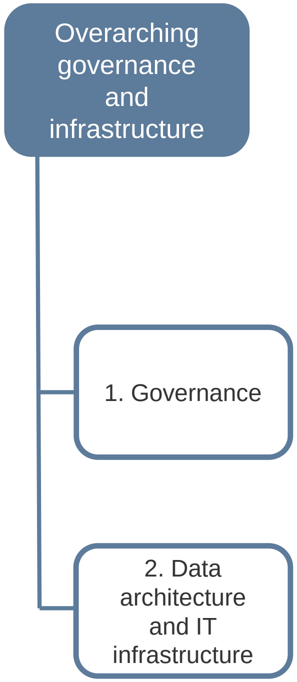
Supervisory review, tools and cooperation
- 12. Review
- 13. Remedial actions
- 14. Home/host cooperation

Not discussed Here

protiviti®

BCBS 239

OVERARCHING GOVERNANCE AND INFRASTRUCTURE


Overarching governance and infrastructure

1. Governance

2. Data architecture and IT infrastructure

A bank should have in place a strong governance framework, risk data architecture and IT infrastructure. These are preconditions to ensure compliance with the other Principles included in this document. In particular, a bank’s board should oversee senior management’s ownership of implementing all the risk data aggregation and risk reporting principles and the strategy to meet them within a timeframe agreed with their supervisors.

A bank’s risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Basel Committee

A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting the other principles

**See http://www.bis.org/publ/bcbs239.pdf*

BCBS 239

RISK DATA AGGREGATION CAPABILITIES

Risk data aggregation capabilities

Banks should develop and maintain strong risk data aggregation capabilities to ensure that risk management reports reflect the risks in a reliable way (ie meeting data aggregation expectations is necessary to meet reporting expectations). Compliance with these Principles should not be at the expense of each other.

3. Accuracy and integrity

A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimize the probability of errors.

4. Completeness

A bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, region and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations and emerging risks.

5. Timeliness

A bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the bank.

6. Adaptability

A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

**See http://www.bis.org/publ/bcbs239.pdf*

protiviti®

BCBS 239

RISK REPORTING PRACTICES (1/2)

Risk reporting practices

Accurate, complete and timely data is a foundation for effective risk management. However, data alone does not guarantee that the board and senior management will receive appropriate information to make effective decisions about risk. To manage risk effectively, the right information needs to be presented to the right people at the right time. Risk reports based on risk data should be accurate, clear and complete.

7. Accuracy

Risk Management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.

8. Comprehensiveness

Risk management reports should cover all material risk areas within the organization. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.

9. Clarity and usefulness

Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. Reports should include meaningful information tailored to the needs of the recipients.

…..Next Slide..

**See http://www.bis.org/publ/bcbs239.pdf*

BCBS 239

RISK REPORTING PRACTICES (2/2)

Risk reporting practices

Accurate, complete and timely data is a foundation for effective risk management. However, data alone does not guarantee that the board and senior management will receive appropriate information to make effective decisions about risk. To manage risk effectively, the right information needs to be presented to the right people at the right time. Risk reports based on risk data should be accurate, clear and complete.

10. Frequency

The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.

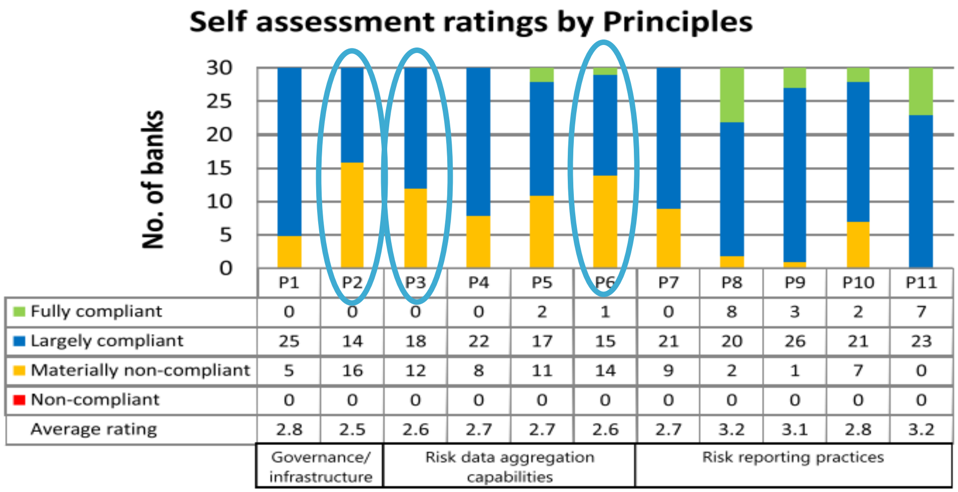
11. Distribution

Risk management reports should be distributed to the relevant parties and while ensuring confidentiality is maintained.

**See http://www.bis.org/publ/bcbs239.pdf*

BCBS239

SELF ASSESSMENT – AREAS OF GREATEST STRUGGLES



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
🟩 Fully compliant	0	0	0	0	2	1	0	8	3	2	7
🟦 Largely compliant	25	14	18	22	17	15	21	20	26	21	23
🟨 Materially non-compliant	5	16	12	8	11	14	9	2	1	7	0
🟥 Non-compliant	0	0	0	0	0	0	0	0	0	0	0
Average rating	2.8	2.5	2.6	2.7	2.7	2.6	2.7	3.2	3.1	2.8	3.2
	Governance/ infrastructure		Risk data aggregation capabilities				Risk reporting practices				

Principle #2 (Data Infrastructure)

- Lowest rating among the 11 Principles
- 70% are materially non-compliant on integrated data taxonomies and glossaries
- 60% are material non-compliant on data production and control across data lifecycle

Principle #3 (Accuracy and Integrity - data quality)

- Third lowest rating among Principles
- 40% are materially non-compliant on IT alignment across repositories (generation of enterprise risk)
- 60% are materially non-compliant on level of dependency on manual data reconciliation processes

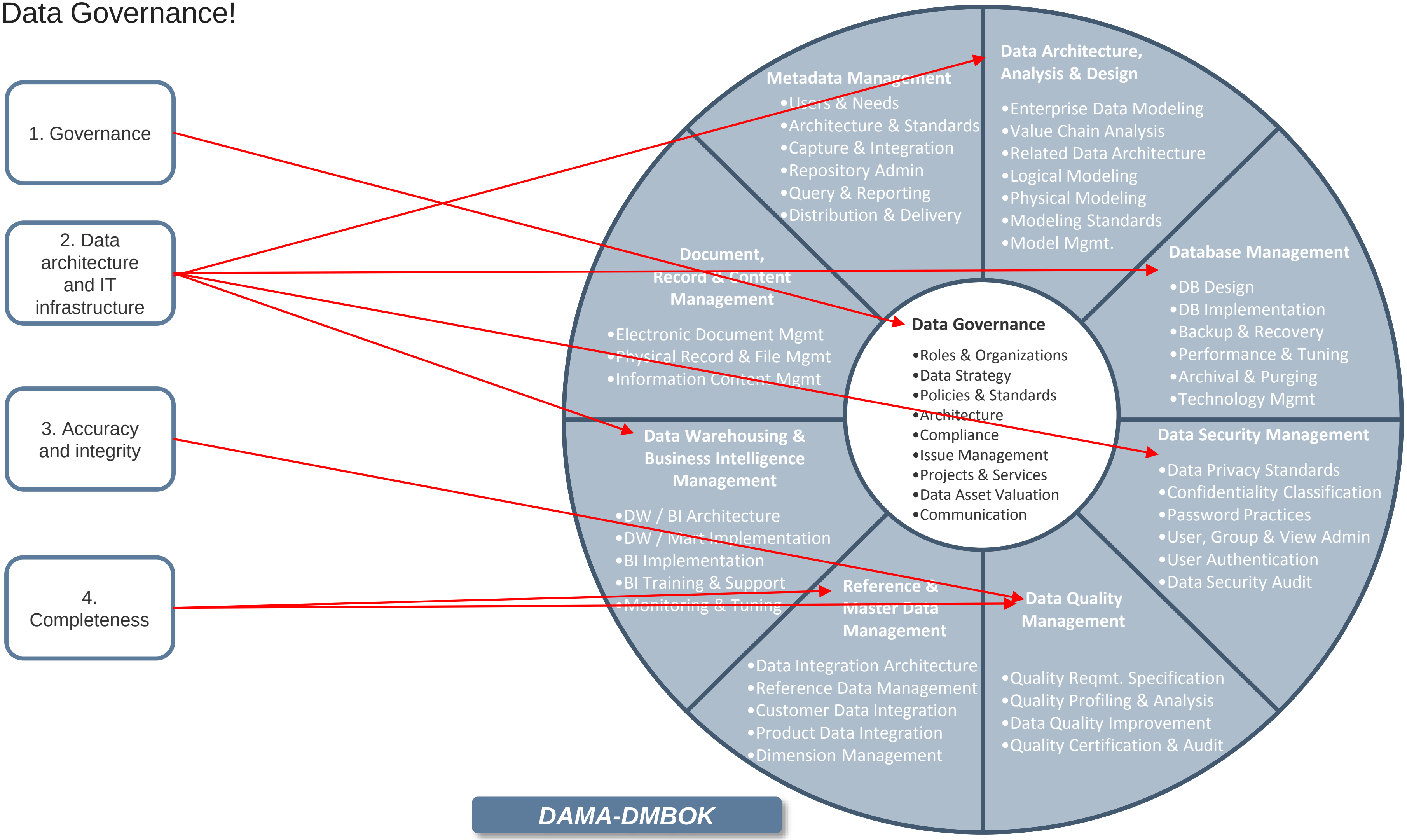
Principle #6 (Adaptability)

- Second lowest rating among Principles
- 83% are materially non-compliance on ability to meet ad hoc requests

BCBS239

PULLING IT BACK TOGETHER – COMMON GOALS (1/2)

Overall many of these Principles can be directly linked back into basic fundamentals of good Enterprise Data Governance!



1. Governance

2. Data architecture and IT infrastructure

3. Accuracy and integrity

4. Completeness

Metadata Management
- Users & Needs
- Architecture & Standards
- Capture & Integration
- Repository Admin
- Query & Reporting
- Distribution & Delivery

Data Architecture, Analysis & Design
- Enterprise Data Modeling
- Value Chain Analysis
- Related Data Architecture
- Logical Modeling
- Physical Modeling
- Modeling Standards
- Model Mgmt.

Database Management
- DB Design
- DB Implementation
- Backup & Recovery
- Performance & Tuning
- Archival & Purging
- Technology Mgmt

Data Security Management
- Data Privacy Standards
- Confidentiality Classification
- Password Practices
- User, Group & View Admin
- User Authentication
- Data Security Audit

Data Quality Management
- Quality Reqmt. Specification
- Quality Profiling & Analysis
- Data Quality Improvement
- Quality Certification & Audit

Reference & Master Data Management
- Data Integration Architecture
- Reference Data Management
- Customer Data Integration
- Product Data Integration
- Dimension Management

Data Warehousing & Business Intelligence Management
- DW / BI Architecture
- DW / Mart Implementation
- BI Implementation
- BI Training & Support
- Monitoring & Tuning

Document, Record & Content Management
- Electronic Document Mgmt
- Physical Record & File Mgmt
- Information Content Mgmt

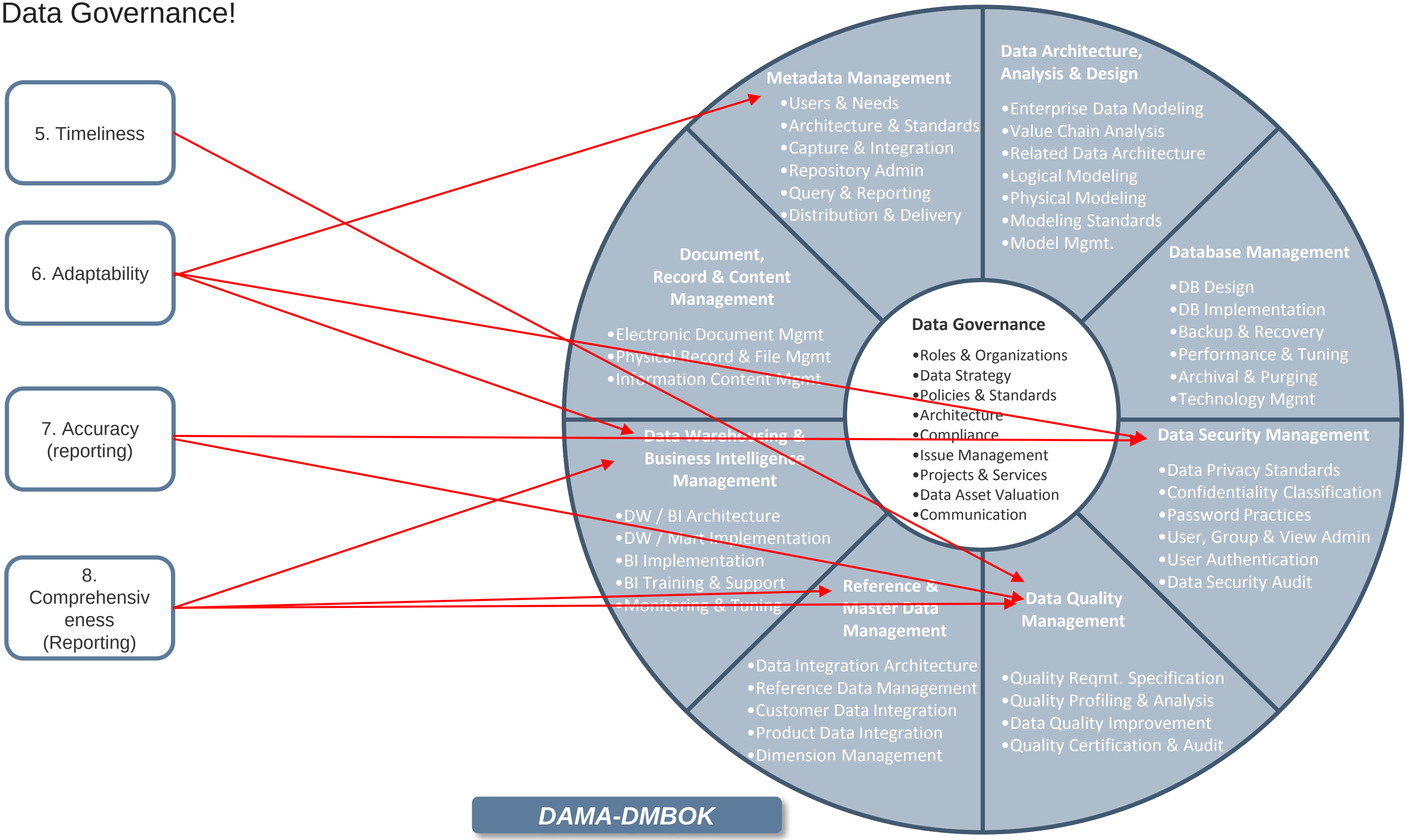
Data Governance
- Roles & Organizations
- Data Strategy
- Policies & Standards
- Architecture
- Compliance
- Issue Management
- Projects & Services
- Data Asset Valuation
- Communication

DAMA-DMBOK

BCBS239

PULLING IT BACK TOGETHER – COMMON GOALS (2/2)

Overall many of these Principles can be directly linked back into basic fundamentals of good Enterprise Data Governance!



5. Timeliness

6. Adaptability

7. Accuracy (reporting)

8. Comprehensiveness (Reporting)

Metadata Management

- Users & Needs
- Architecture & Standards
- Capture & Integration
- Repository Admin
- Query & Reporting
- Distribution & Delivery

Data Architecture, Analysis & Design

- Enterprise Data Modeling
- Value Chain Analysis
- Related Data Architecture
- Logical Modeling
- Physical Modeling
- Modeling Standards
- Model Mgmt.

Document, Record & Content Management

- Electronic Document Mgmt
- Physical Record & File Mgmt
- Information Content Mgmt

Data Governance

- Roles & Organizations
- Data Strategy
- Policies & Standards
- Architecture
- Compliance
- Issue Management
- Projects & Services
- Data Asset Valuation
- Communication

Database Management

- DB Design
- DB Implementation
- Backup & Recovery
- Performance & Tuning
- Archival & Purging
- Technology Mgmt

Data Warehousing & Business Intelligence Management

- DW / BI Architecture
- DW / Mart Implementation
- BI Implementation
- BI Training & Support
- Monitoring & Tuning

Data Security Management

- Data Privacy Standards
- Confidentiality Classification
- Password Practices
- User, Group & View Admin
- User Authentication
- Data Security Audit

Reference & Master Data Management

- Data Integration Architecture
- Reference Data Management
- Customer Data Integration
- Product Data Integration
- Dimension Management

Data Quality Management

- Quality Reqmt. Specification
- Quality Profiling & Analysis
- Data Quality Improvement
- Quality Certification & Audit

DAMA-DMBOK

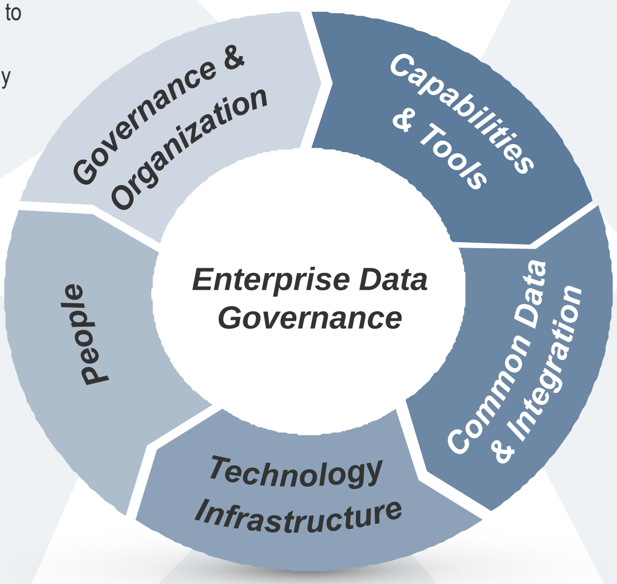
ASSESSING BCBS 239

DATA GOVERNANCE APPROACH EXAMPLE

How do you even get started assessing and organizing an approach?

- Identification of data owners and stewards improves accountability across the end-to-end data lifecycle
- Data owners are established and accountable for the end-to-end quality and definition of the data
- Business SME’s are engaged in data governance activities to drive definitions, standards, remediation, etc.
- Executive level ownership and sponsorship on data strategy and program implementation
- Enterprise policies and standards applied across risk data and driving BCBS 239 compliance

- Establishing common terminology in data dictionaries, consistent metadata and enterprise taxonomies
- Identification of common data across key business processes and programs will simplify data infrastructure and allow for more timely integration.
- Robust data quality controls, business processes, lineage, data transformations and rules are documented by a comprehensive data dictionary
- Consistent application of a data quality framework will be applied to risk data assets for ongoing monitoring, issue identification and remediation
- Holistic and transparent view of data used across risk reporting using data governance capabilities and tools
- Clear understanding and supporting documentation of data used in risk processes from end-to-end


Governance & Organization
Capabilities & Tools
Enterprise Data Governance
People
Common Data & Integration
Technology Infrastructure

- Clear visibility, transparency and executive sponsorship of the BCBS 239 Program objectives
- Strong enterprise governance model supporting cultural awareness and driving adoption of program objectives
- Enterprise resources are assigned to maturing data governance across enterprise
- Data stewards and custodians have specific responsibilities for the quality of data assets
- Information architects are part of project and strategic initiatives to ensure data models are easily integrated and consumed across the data lifecycle

- Identification and application of common data taxonomy across risk reporting (key business processes and programs will simplify data infrastructure and allow for more timely integration.)
- Common data elements are identified, defined and standardized at the enterprise level to drive consistent understanding across risk reporting’
- Business glossary and metadata supporting risk data and reporting
- Common data will be managed by consistent tools and will drive common terminology within reporting by creating data dictionaries, consistent metadata and integrated data taxonomies.

- Simplify and improve data infrastructure for ensuring data availability and frequency supports regular and ad hoc risk reporting across departments and legal entities
- Developing IT infrastructure to more easily aggregate a broader range of risk data automatically and reduce reliance on manual workaround
- Integrate risk and finance data infrastructure

BCBS239

WHY SHOULD EVEN NON-FSI FOLKS CARE?

In a recent McKinsey & Company Study the average G-SIB is expected to spend $230M to comply with BCBS239, and the average D-SIB will spend $75M for compliance.*

This level of investment is forcing innovation and new product development around all aspects of Enterprise Data Governance!

An issue – Data Governance – that has been around since the advent of computing is finally getting the spotlight and attention it deserves.

A recent Akin Gump Survey of 10 Ten Topics for Board of Directors** had three Data Related issues - #2: Cyber security, #3: uses for Big Data, and #6: risk reporting.   Data Governance is rapidly becoming a common Board level question from our clients.

**McKinsey & Company: Capturing value from BCBS 239 and beyond, June 2015*

***Akin Gump: Top10Topics for Directors in 2015*

BCBS 239 ROLLOUT CONSIDERATIONS

HONESTLY ASSESS YOUR CAPABILITIES AND MATURITY

Through our existing professional relationship with the EDM Council*, Protiviti leverages tools such as the EDM Council Data Management Capability Assessment Model. EDM Council has created this framework through industry collaboration, rationalization of core data management principles, and alignment with control environment measurement standards (such as BCBS 239 Principles for Risk Data Aggregation).

DCAM

Data Management Capability Assessment Model

EDM COUNCIL DCAM MODEL – 8 CORE COMPOENTS

DATA MANAGEMENT STRATEGY

Defines the long term goal of the data management program. The blueprint to gain internal alignment among stakeholders and to define how the organization will approach the management of data content

BUSINESS CASE & FUNDING MODEL

The justification for the data management program. The mechanism for ensuring sufficient and sustainable capital. The approach for measuring the costs and benefits of EDM

DATA MANAGEMENT PROGRAM

The mechanism for EDM implementation. Stakeholder engagement. Communications program and education on the concepts of data CONTENT management. Engagement model and operational routines

DATA GOVERNANCE

The rules of engagement for implementation of the data management program. The focus is on implementation of policies, standards and operational procedures necessary to ensure that stakeholders "behave"

DATA ARCHITECTURE

The "design of information content" including the identification of data domains, establishment of taxonomies, alignment with contractual obligations, documentation of metadata and designation of CDEs

TECHNOLOGY ARCHITECTURE

The "design of physical architecture" including the platforms and tools in support of data management implementation. This is domain of IT and defines how data is acquired, stored, integrated and distributed

DATA QUALITY

Deliver to business users data that is fit-for-purpose. The goal is data that users trust and have confidence in to be exactly what they expect it to be without the need for reconciliation and data transformation

DATA CONTROL ENVIRONMENT

Coordination of the components into a cohesive operational model; ensure that controls are in place for consistency across the lifecycle; align with organizational privacy and security policies

The DCAM Model Scoring Methodology is based on three criteria: (1) Engagement of functional / process components; (2) Formality of documented, repeatable and coordinated efforts; and (3) Evidence of capabilities as sanctioned and operational.

** EDM COUNCIL – Protiviti is a member and professional partner of the EDM Council Organization.*

BCBS 239 ROLLOUT CONSIDERATIONS

KNOW YOUR RISKS

- ***Politics***
- ***Culture/Social***
- ***Organizational***
- ***Physical***

People

- ***Inertia (Profit)***
- ***No Burning Platform***
- ***Lack of Leadership***
- ***No Driver/Line of Sight***

Business

- ***Understanding***
- ***Maturity***
- ***Improvement***

Process

- ***Silo Thinking***
- ***Immaturity***
- ***Not Interoperable***
- ***Lack of Solutions***

Technology

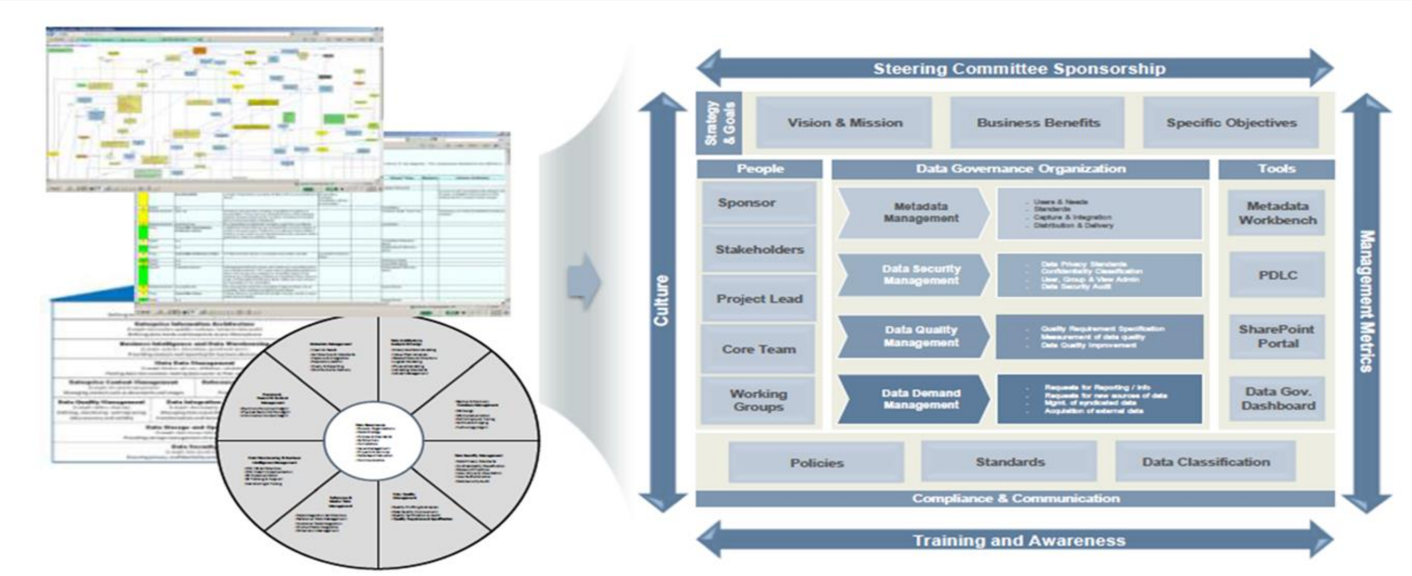
Source: Gartner, MDM Conference 2013

BCBS 239 ROLLOUT CONSIDERATIONS

WHAT IS YOUR OVERALL GOVERNANCE MODEL? (PRINCIPLE 1)

Take best of breed methodologies and learn from these – don't feel like you need to recreate the wheel. Data Governance challenges have been around forever – leverage what you can from other organizations.

EXAMPLE: PROTIVITI DATA GOVERNANCE MODEL

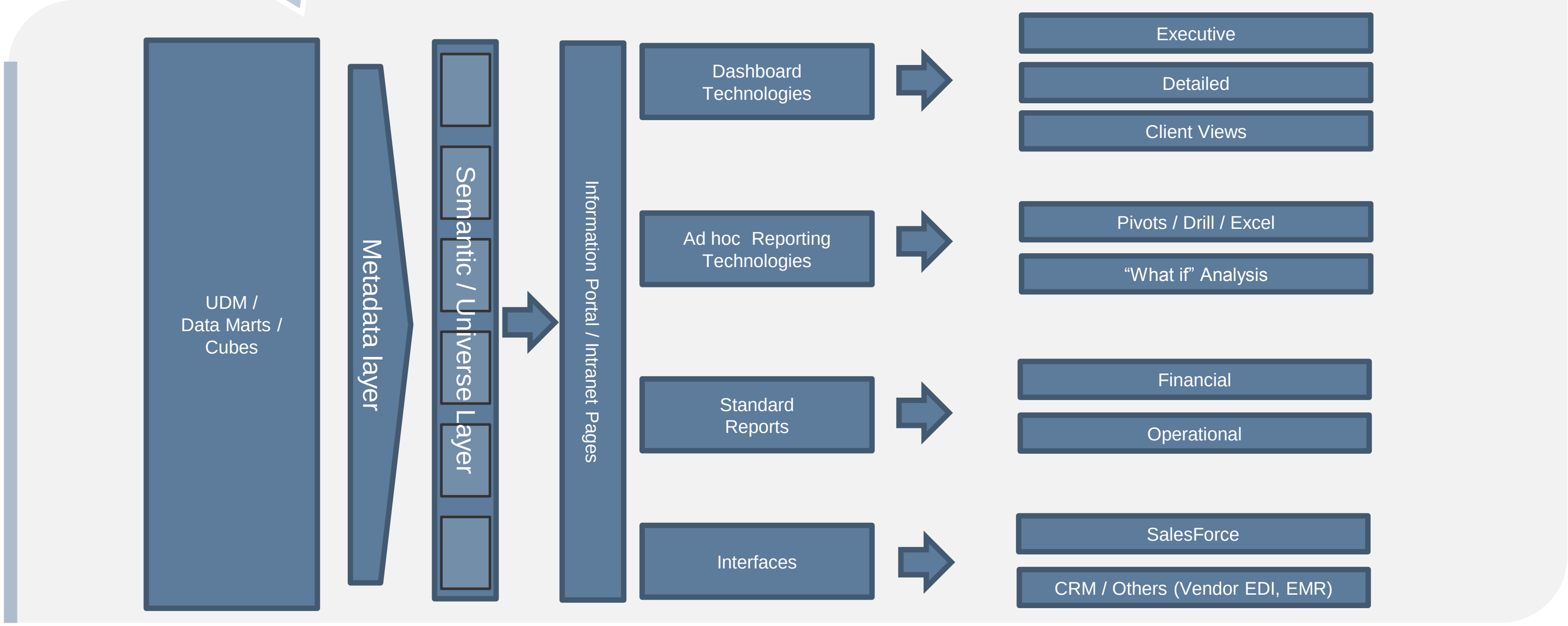


Data Governance is not a one size fits all prescription, but our methodology, framework and approach to effective Data Governance helps organizations solve for many components of current and future regulatory scrutiny. Establishing the right Data Governance program early will help solve for multiple areas of compliance.

BCBS 239 ROLLOUT CONSIDERATIONS

UNDERSTAND YOUR DATA AND IT INFRASTRUCTURE (PRINCIPLE 2)

You have to take full stock and inventory of all key systems, data stores, data movements, controls, reports – everything touching or leveraging for your Critical Data Elements! You must also ensure that you put the right tools in place to further help control your infrastructure.



BCS 239 ROLLOUT CONSIDERATIONS

DATA ACCURACY AND INTEGRITY (PRINCIPLE 3)

The specific characteristics or dimensions of data that are analyzed in a Data Quality program differ from one business to another based on the needs and priorities of that business. The following dimensions are commonly used:

Dimension	Short Description	Example
Uniqueness	A number or characteristic that identifies one and only one entry in a data set	Every customer should have a Customer ID and no two customers should have the same Customer ID
Accuracy	Data fairly represents what it is intending to represent	Correct amount for Outstanding Balance
Consistency	The same data from two or more sources should not conflict with each other	NAICS Code to Concentration Code
Completeness	Data records have values where they are required	Each record should have an Account Number
Timeliness	Data is available and accessible when needed by the business	Financial statements are received when due
Currency	The data is “up-to-date”	Customer contact information
Conformance	The data is stored in the correct format	Phone number has proper number of digits and format
Integrity	The relationships between data in different systems is maintained	The relationship between account number and Customer ID is not broken
Lineage	Changes to data are recorded and identifiable	Ability to audit changes made to Risk Rating

BCBS 239 ROLLOUT CONSIDERATIONS

DATA ACCURACY AND INTEGRITY (PRINCIPLE 3)

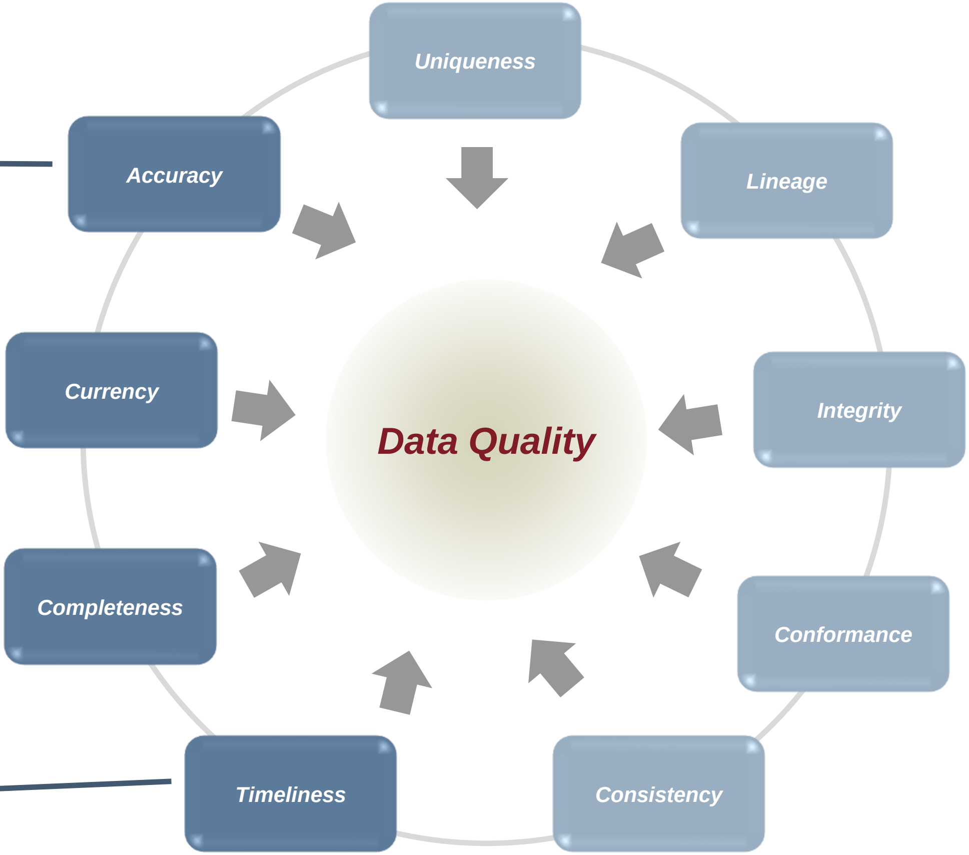
Data Quality should be measured and managed across several different “dimensions”. Each organization may determine which dimensions are of utmost importance to measure the quality of individual data elements as shown in the example below:

Accuracy
Data fairly represents what it is intended to represent.

Currency
Data is up-to-date and not stale.

Completeness
Data records have values where they are required.

Timeliness
Data is available and accessible when needed by the business.



Uniqueness

Lineage

Accuracy

Currency

Integrity

Data Quality

Completeness

Conformance

Timeliness

Consistency

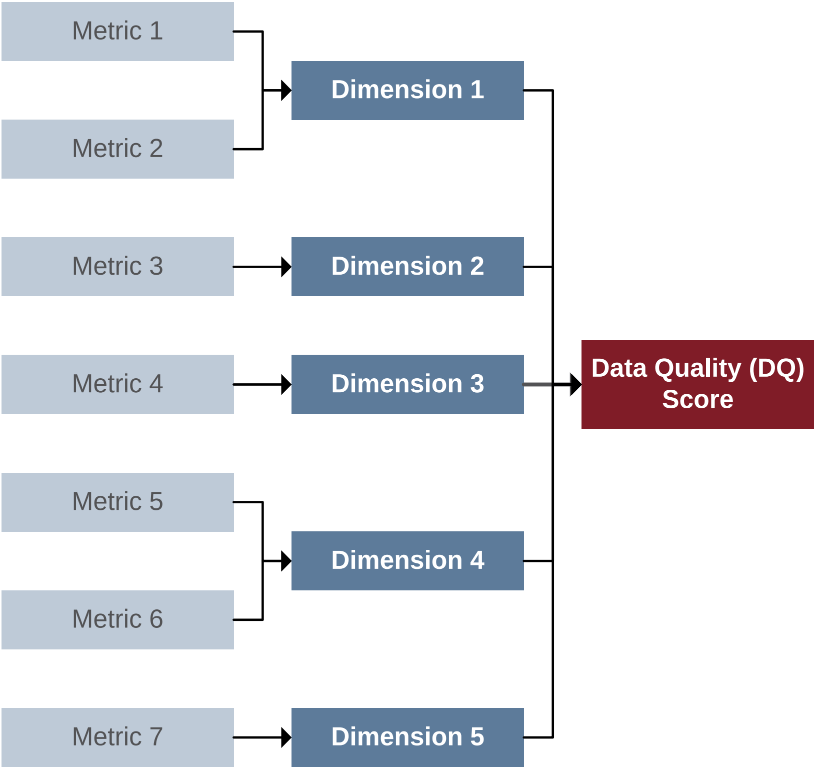
**Not every dimension is applicable to each data element.*

High Priority Dimensions

Standard Dimensions

DATA QUALITY

MEASURING DATA QUALITY – DATA QUALITY INDEX



- The population of elements subject to data quality monitoring has been identified through a prioritization process
- Specific dimensions are used to measure data quality
- Each dimension is measured by one or more metrics
- As seen in the illustration below, an element's data quality score is a weighted sum of underlying dimensions
- Scores range from 1 to 7, with 7 being the highest
- Individual element DQ Scores can be rolled up to create an aggregate DQ Score
- Metric calculations will be automated

$$\textit{Data Quality Score} = \sum_{i=n}^{n} \textit{Dimension}_i * \textit{Weight;}$$

$$= \textit{Dimension}_1 * x\% + \textit{Dimension}_2 * x\% + \textit{Dimension}_3 * x\% + \textit{Dimension}_4 * x\% + \textit{Dimension}_5 * x\%$$

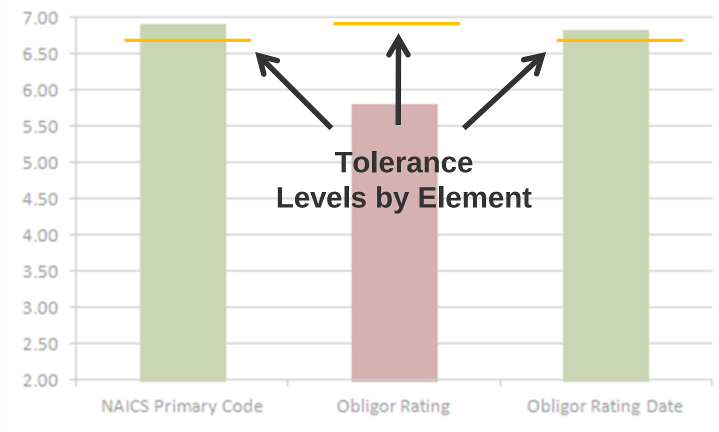
DATA QUALITY
MEASURING TOLERANCES

Tolerances are the minimum acceptable Data Quality Scores for data elements. The tolerances may be set to ensure that the data meets the banks reporting and regulatory needs.

The elements will be categorized into two groups as it relates to tolerance levels:

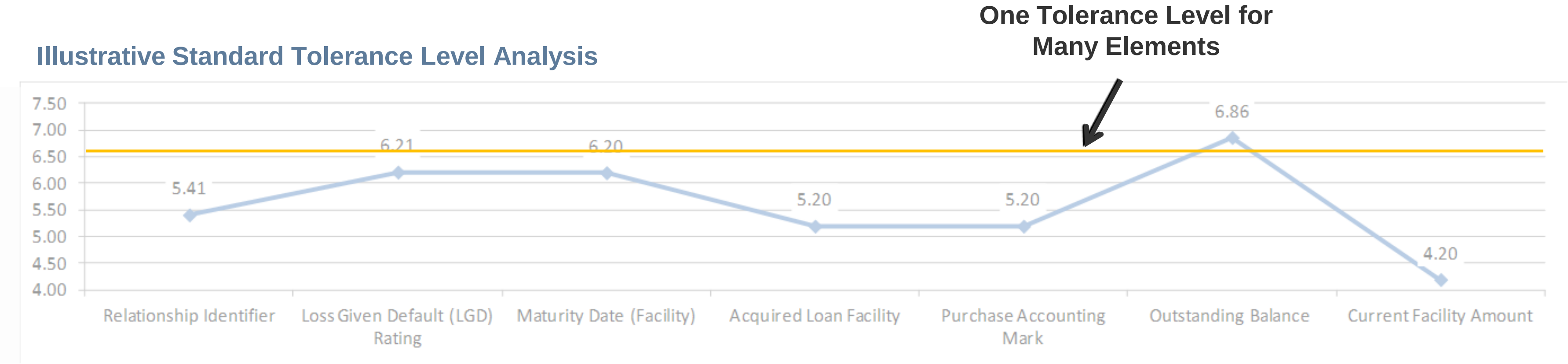
- Customized tolerances will be applied to the highest priority data elements.
- Standard tolerance levels will be applied to lower priority elements.

Illustrative Customized Tolerance Level Analysis



Illustrative Standard Tolerance Level Analysis

One Tolerance Level for Many Elements



DATA QUALITY
DATA GOVERNANCE LEADING PRACTICES

Per guidance from the EDM Council, mature processes on Data Quality are measured against the following capabilities. The tactical activities and tasks designed within the Data Quality Program strive to achieve success on each of these.

Data quality program is established

- The data quality strategy and approach is defined and socialized.
  - *Data quality strategy and approach have been communicated to all involved stakeholders DQ strategy has been endorsed by senior management.*
- Accountable parties have been identified and roles and responsibilities have been assigned.
  - *Individuals are held accountable for the performance of their DQ function via reviews and compensation.*
- The Data quality roles and responsibilities have been communicated.
  - *Senior management endorse and support the DQ accountability structure.*

Quality of existing stores of data are identified and assessed.

- All relevant data have been identified and prioritized.
  - *The scope of data subject to the DQ program is approved. CDEs are designated and actively maintained.*
- Data is profiled, analyzed and graded.
  - *In-scope data has been “graded” and catalogued. Metadata has been authorized.*
- Data remediation has been planned, prioritized and actioned.
  - *Data is being remediated and repaired.*

Quality of new data is monitored, analyzed and reported

- Data Quality ‘control points’ are in place along the full spectrum of the data supply chain.
  - *DQ control points are implemented and operational. Control remediation procedures are documented and evidenced.*
- Data Quality Metrics are captured, reported and used to drive data remediation.
  - *DQ metrics are routinely captured, reported to senior management and used to drive remediation.*
- Root-Cause analysis is performed.
  - *The root cause analysis processes are defined and corrective measures are being implemented.*
- Data Quality processes are auditable.
  - *Audit (or the equivalent organization) is performing data quality procedure examinations.*

DATA QUALITY

DATA PROFILING

Data profiling provides valuable insight about the current condition of data and is an important first step in managing the quality of your most critical information assets. Using any available existing tools, the Data Governance team can automatically identify inconsistencies, redundancies, and inaccuracies within relevant authoritative systems. This analysis will highlight the current state of uniformity in your data and support an enterprise-wide understanding of standard definitions and values associated with critical data entities. The results of automated data profiling facilitate the prioritization of data quality issues according to organizational impact as well as help to ensure quality of data is considered (and potentially improved) throughout any new system implementation or conversion process.

Profiling data helps the organization to begin to understand how much data is missing, outlier values in the data and many other anomalies. Examples include knowing if you have null fields or different ways data within a ‘phone number’ field is being represented.

Through profiling, the following issues may be discovered:

Data content issues – What are the minimum and maximum lengths of the table? What data type are the tables? What are the range of values? Do nulls exist? Is the table filled with the same value?

Data structure issues – Is the primary key unique? Can something else be used for a primary key? Does the metadata accurately describe the data?

Data quality issues – Is the data accurate and complete? Does it follow our own data quality business rules?

A challenge with profiling ad-hoc (i.e., querying without a proper profiling tool) is that by knowing what you aren’t aware are, it becomes difficult to identify anomalies that you weren’t originally searching for. By understanding all of these anomalies, the Data Governance team is in a better position to scope a data quality improvement project.

Profiling doesn’t always have to be a one time activity. It should be used within the project lifecycle when you begin a project and again to reassess at the end. Profiling data will also help business and technical users better to understand the landscape of a combined database from two different sources before it is actually completed and in production.

DATA QUALITY
ISSUE CENTRALIZATION, ESCALATION AND REMEDIATION

With many organizations, we often hear of complaints of poor data or incorrect reporting, yet there is rarely a centralized or standard way of formally reporting these issues so they can be understood, analyzed, investigated, validated, and escalated where appropriate in order to create a plan for remediation.

As such, issues may be identified proactively by the Data Governance team in real-time operations or as a result of incorrect information diagnosed by the business. Creating responsive functions will help your organization mitigate the existence of these risks.

» Coordination, Identification, and Tracking of Data Anomalies

Anomalies are anything unsuitable for the intended use because it is not conforming with standards. Examples include non-numeric data entered in a numeric-only field; incomplete or missing data, not following a prescribed format (e.g., ##-###), unique key fields not being unique, data that is incorrectly entered at input.

DG teams perform data quality profiling to discover anomalies. Results of profiling and fixing data anomalies can result into quality monitoring and reporting to ensure these anomalies stay fixed.

Using profiling and discovery of the anomalies will allow Data Governance to work with business and IT on small and large projects to make improvements (control checks, input validation, data fixes) to the overall “health” and conformity of the data set.

» Data Issue Escalation / Prioritization and Monitoring and Reporting

Establishing a data quality center to identify and correct data quality issues within and amongst applications and databases. This function will be centralized within the Data Governance team. Responsibilities include investigation into inquiries and identification of acceptable data quality ranges for critical values (to allow for the automation of new data issue discovery on previously treated / analyzed elements or reports).

BUSINESS GLOSSARY / DATA DICTIONARY

BUSINESS VALUE AND IMPLEMENTATION SEQUENCE

Overview:

The efforts to drive the Business Glossary and Data Dictionary will provide the organization with the enterprise reference guide to better understand the characteristics (both business and technical) related to the critical data elements relied upon within the organization through transactional operations and decision support reporting.   This common 'nomenclature' around data is an emerging emphasis of regulators as they look at items such as Risk Data Aggregation.

Business Value:

By providing the semantic layer between the technical systems and the business users, it will ensure the organization's data is understood, has supporting documentation (definitions, standards, acceptable values, etc.) and clear business accountability which will allow analysts to find and understand the information they need and make less incorrect assumptions which otherwise may limit strategic and operational decisions as well as being able to explain the overall composition of the data (and its classifications) within the systems to regulators and external parties.

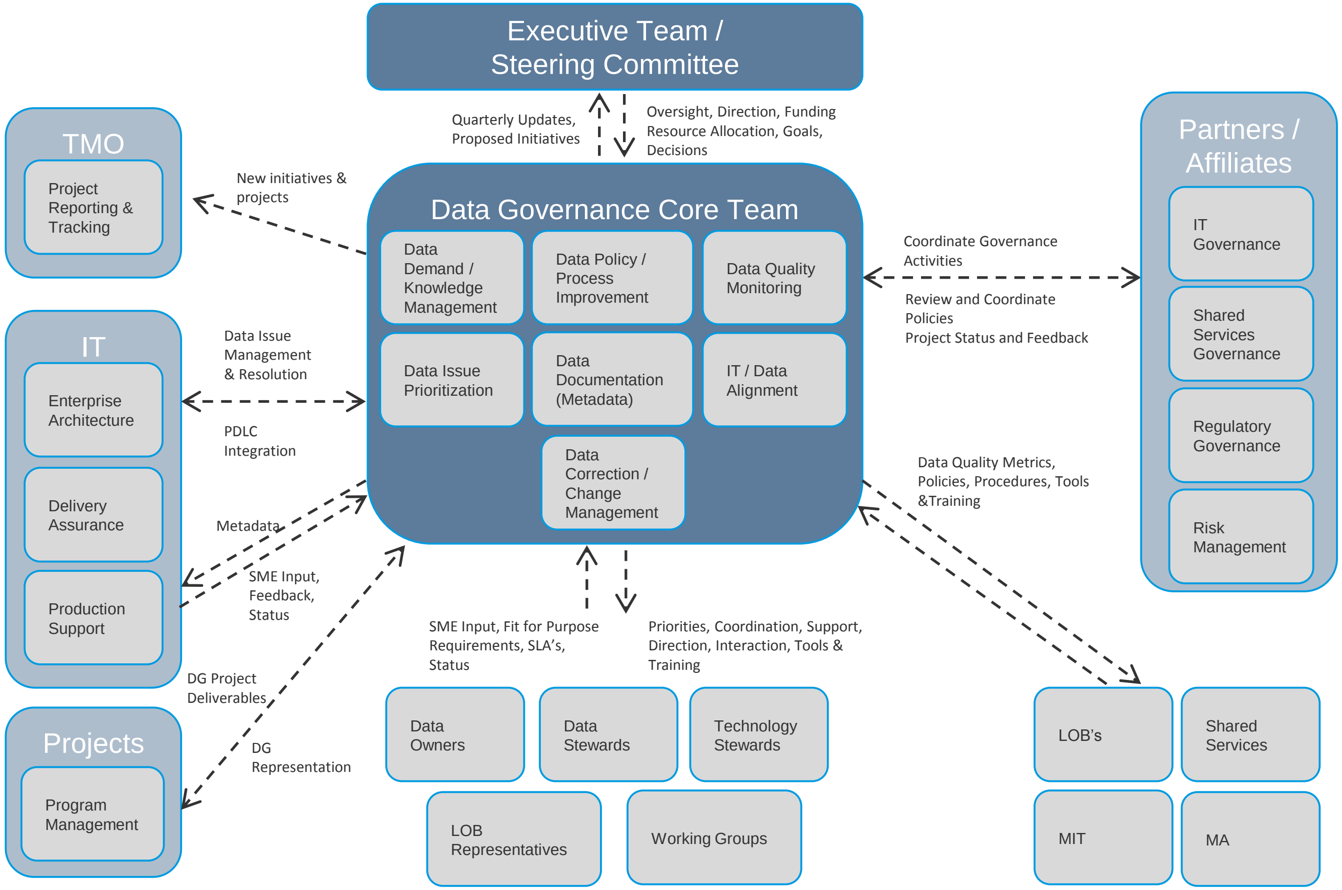
TACTICAL IMPLEMENTATION STEPS

- ✓ **Evaluate and Select a Business Glossary / Data Governance Tool**
  Determine requirements, create RFP, scorecard, vendor demos, recommended decision / IT work request
- ✓ **Business Glossary / Data Governance Tool technical implementation and admin training**
  Establish formal project plan, determine and document use cases, bus. Requirements, training, job aids, communication, and internal procedures for management and maintenance.
- ✓ **Initial business glossary information gathering and loading**
  Determine initial critical data entities and elements for inclusion, provide gathering templates and QA of steward entries.
- ✓ **Establish Librarian Process (additions and edits to existing definitions for Business Glossary)**
  Determine on-going expansion of business stewards to populate more metadata & determine wider communication plans.
- ✓ **Technical metadata initial loading and process for continuous population for lineage**
  Determine requirements for capturing technical data lineage, evaluate current toolsets, determine future toolset (leverage current vs. Buy), configure for needs, communicate and support training for resources.

ROLLOUT CONSIDERATIONS

CLEAR COMMUNICATION OF SCOPING AND INVOLVEMENT

As noted in scoping many times a Data Governance organization may have some core responsibilities, but to build an effective organization you must also be able to leverage and partner with other existing functions. This requires careful planning, agreement from all parties, and constant communication in order to properly function. The example below represents an example Interaction model built out for one of our clients.



Executive Team / Steering Committee

Quarterly Updates, Proposed Initiatives

Oversight, Direction, Funding Resource Allocation, Goals, Decisions

Data Governance Core Team

Data Demand / Knowledge Management

Data Policy / Process Improvement

Data Quality Monitoring

Data Issue Prioritization

Data Documentation (Metadata)

IT / Data Alignment

Data Correction / Change Management

TMO

Project Reporting & Tracking

New initiatives & projects

IT

Enterprise Architecture

Delivery Assurance

Production Support

Data Issue Management & Resolution

PDLC Integration

Metadata

SME Input, Feedback, Status

Projects

Program Management

DG Project Deliverables

DG Representation

Partners / Affiliates

IT Governance

Shared Services Governance

Regulatory Governance

Risk Management

Coordinate Governance Activities

Review and Coordinate Policies

Project Status and Feedback

Data Quality Metrics, Policies, Procedures, Tools &Training

SME Input, Fit for Purpose Requirements, SLA's, Status

Priorities, Coordination, Support, Direction, Interaction, Tools & Training

Data Owners

Data Stewards

Technology Stewards

LOB Representatives

Working Groups

LOB's

Shared Services

MIT

MA

ROLLOUT CONSIDERATIONS

CLEARLY DEFINED ACTIONABLE, ACCOUNTABLE ROLES

Reliance and roles / responsibilities within the business (Business Data Stewards) can be split among three major involvement areas:

Overall Business Alignment and Representation

- Business Function Representation – the Business Data Steward is the champion within a particular business area / function who covers an area such a ‘New Accounts’ or ‘Customer Service’.
- In this capacity, the Business Data Steward is responsible to understand all Data Governance established policies, standards and procedures and ensure they are being communicated and utilized into their business area by all associates.
- Establish a clear line of regular communication to the enterprise Data Governance function to alert and escalate of any potential issues.
- Work to identify the most important key business terms (definitions), as well as provide input in business requirements that affect data quality standards and overall usage.

Data Life-Cycle Management

- Help to establish priorities within business functions and continuously review requirements as part of new work requests or established work streams.
- Define the data, manage metadata and communicate new business data definitions and approved data usage standards to enterprise Data Governance.
- Take ownership and responsibility of metrics and monitoring overall compliance of data conforming to the established measures.
- Make recommendations on how data quality can be improved and protected as a result of any root cause analysis following any conflict resolution that has been escalated.
- Understand and assess any enterprise impacts to data change by participating in stewardship committees organized around new data and project initiatives.

Data Quality and Risks

- Establish acceptable levels of data quality that can be measured.
- Understand all uses and context of the data and be included in any actions or decisions for any new planned use of the data throughout the enterprise.
- Define improvement opportunities as a result of reviewing data quality metrics and analysis of root causes for any data falling below acceptable levels.
- Support new business cases for improvement projects to establish stronger data quality.

ROLLOUT CONSIDERATIONS
ENGAGE WITH KEY PROJECTS / MAJOR INITIATIVES

Data Governance practices should be incorporated and on-going in major project initiatives in the following ways and within these phases:

Project Preparation

- Identifying business objectives – focus on the short and long term goals related to data quality and understand if the data and information provided in the immediate project could also be leveraged further in the organization for additional value.
- Understand full scope of the project as it relates to data (e.g., capturing the data, transformation and movement of the data). As part of the scoping, the levels of quality should be identifying as well as existing or new sources of data.
- Assess the data risks by performing initial tasks such as profiling the source data information to determine if it's viable for supporting the business requirements and meeting all of the business expectations.

Plan

- Define standards that should be applied to data (e.g., conforming email addresses) and ensure the correct definitions and descriptions are established with the business team.
- Analyze any source data to find anomalies or potential problems with the data that should be escalated to the project team.
- Coordinate with data architecture teams to ensure platforms and data models meet requirements.

Implement

- Participate in test case scenarios creation to ensure any discovered data anomalies will be appropriately tested after implementation.
- Tune initially created business rules and standards for data for any potential updates or changes to expectations.

Rollout and Go Live

- Participate in the execution of the user acceptance testing.
- Review system conversion / production cutover plan and results of initial or cleansed data loads.
- Participate in problem resolution support team and post mortem reviews of lessons learned and exception logs.

Maintain

- Participate in data audits and other monitoring processes to ensure initial expectations related to data standards and quality continue to be met.
- Understand data issues and requirements for enhancement phases to the project to promote stronger data quality practices.

ROLLOUT CONSIDERATIONS

SET CLEAR GOALS AND MEASURE THEM OFTEN

Enterprise Data Management is difficult to implement, and in many cases will require additional work from already stretched resources. As such we must use certain guiding principles to simplify the exercise where ever possible, and to keep the group focused on what we are trying to achieve through EDM – better data! This is a destination that can be reached by many roads, and we must always be flexible.

Rule	Description
Clearly establish the goals and purpose	The overall vision and goals must be simple, clear, and precise.
Only put Governance where needed	Select sponsors, owners, and participants, and establish processes focused on results. Prioritize based on business need. Do not apply governance solely to build consensus or to react to momentary interest.
Keep it simple and pragmatic	Do not force added steps into otherwise simple processes unless absolutely needed. Keep the governance model as simple as possible and make sure that all tasks are adding value to the overall organization.
Design from the top down but implement from the bottom up	Design policies, standards, and processes for the entire organization; build and implement them practically starting with high impact areas.
Be flexible	Recognize that "one size does not fit all" when it comes to governance. Make it too difficult, and people will circumvent it. Make it customizable (within guidelines), and people will get a sense of ownership.
Provide clear communication to the point of over communication!	Communicate the activities often, and to all of the Data Governance Constituents. Make sure to share the wins and progress on activities, as well as the anticipated future planning activities.

KEY QUESTIONS

DISCUSSION / OPEN TOPICS

Open questions / additional topics

Powerful Insights.
Proven Delivery.®