Prioritizing Data Based on Criticality: Critical Data Elements (CDEs) in Context

Enterprise Data Management Council
Best Practice Program

November 2018, Version F1.1

Best Practice Work Group Scribes

Gareth Isaac, Director and Principal Consultant, Ortecha, a DCAM Authorized Partner

Mark McQueen, EDM Council Senior Advisor-Best Practice & Process Design

Table of Contents

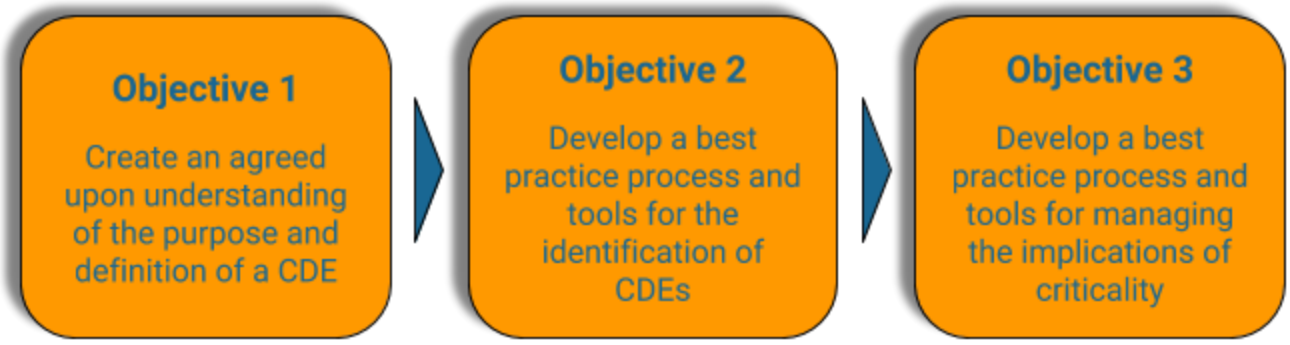
Executive Summary

Objective

One of the most significant regulatory directives following the 2008 financial crisis has been the introduction of the "Principles for Effective Risk Data Aggregation and Risk Reporting" or BCBS 239[1]. The Principles outlined in this directive require banks to establish sound information infrastructures to support their risk and risk reporting functions. As part of creating the required control environment, a common practice in the financial services industry is the establishment of CDEs or "Critical Data Elements".

In spite of this focus on CDEs by the financial service industry, in the 2017 Data Management Industry Benchmark Study conducted by the EDM Council, the management of CDEs was identified as a top challenge universally across the industry. Members report that there is uncertainty regarding the exact definition of a CDE, how is it designated, or how it should be used to satisfy the control requirement.

Subsequently, the EDM Council conducted 14 in-depth interviews with member firms to frame the issue. The research was organized to gain insight on how organizations define critical data, the process to identify critical data, and the implications for heightened levels of control on critical data. The research revealed both the purpose and approach to CDE management remained fragmented and siloed to each organization. To address this, the EDM Council formed a CDE Best Practice workgroup. The workgroup was charged with establishing a Best Practice for the identification and management of critical data covering these three objectives.



The Best Practice provides processes, procedures, and tools for the execution of the identification of critical data all aligned and integrated with the EDM Council Data Management Capability Assessment Model (DCAM™) Framework[2].

This document covers Objective 1 and Objective 2. Objective 3 will be covered in a later publication.

[1] BCBS 239 - Principles for Effective Risk Data Aggregation and Risk Reporting - https://www.bis.org/publ/bcbs239.pdf
[2] About DCAM

Key Observations

- Purpose of a CDE is to prioritize your data based on criticality - this allows you to identify a scope of the most important data to bring into a heightened level of control and accountability
- Determining criticality is a business process perspective based on the Data Consumer process - and thus is determined at the conceptual level - the actual physical level data elements aligned to the conceptual level inherit the criticality
- Organizations that attempted to use a precise calculation to identify criticality did not achieve adoption and ultimately abandoned the science for a more artful analysis which included a negotiation between the Data Producer and Data Consumer to agree upon prioritized data based on criticality
- Derived data can be deemed critical, however, the implications of criticality must be applied to the atomic data that is an input to the derived value
- Granular data used in a derivation should be independently evaluated for criticality based on the material impact each has on the derived value
- The implication of designating criticality requires a heightened level of control; these controls include governance, metadata, data flow/lineage, data quality, transformation and movement controls

How to Use This Best Practice

This Best Practice report covers the first two objectives as described above. The Best Practice workgroup continues to complete the analysis and best practice design related to the third objective: managing the implications of criticality. A subsequent Best Practice report will be issued as that work is completed.

The EDM Council approach to Data Management Best Practice is to develop member vetted material for executing Data Management processes to execute the capabilities defined in the DCAM Framework. The industry Best Practice by design is conceptual and requires customization for execution in an organization.

While the experience reflected in this Best Practice is primarily from representatives of the Financial Service industry the recommendations are applicable for all industries in the execution of their data management practice.

More information:

- EDM Council Best Practice Program[3]
- Best Practice Design Structure[4]
- Appendix: About the Critical Data Element (CDE) Work Group
- Appendix: Work Group Members

[3] **https://edmcouncil.org/page/bestpractice**
[4] **https://edmcouncil.org/blogpost/1624135/Anatomy-of-a-Best-Practice**

Issues Surrounding CDEs

To further understand the issue of managing CDEs, a set of questions were developed to understand the current state and establish the intended scope for the Best Practice.

- What is a CDE?
- How are CDEs identified?
- What makes a Data Element critical?
- What are the criteria for determining criticality?
- Who determines criticality?
- What is the impact of a data element identified as critical?
- What is an appropriate volume of CDEs?
- Can CDEs have different levels of importance?
- Are CDEs atomic elements, or derived?
- If a derived element is designated as a CDE, does this imply that the composite elements that were used to create the derived element are also CDEs?
- Is it possible to identify industry standard CDEs or is it an organization specific exercise?

These questions were used to learn more about actual experiences banks had with implementing CDEs. Fourteen EDM Council member organizations were interviewed based on the questions above. What was learned about the current state of CDE management is summarized in the following section, the full report was published in November 2017 and is available[5] to EDM Council members.

[5] CDE Member Research Interim Report, https://edmcouncil.site-ym.com/global_engine/download.asp?fileid=B5F64202-4906-4386-BE01-0D7B8B4E360E&ext=pdf

Current State Findings

The member organizations selected for interviews were those that the EDM Council had a prior awareness that they were actively managing CDEs. A high degree of engagement was validated but with significant variation across the organizations in CDE definition, volume, the process for identifying, and, the level of data management rigor applied to manage CDEs. Even from mature efforts, there was confusion and lack of confidence in how CDE management was being executed with little to no consistency across the organization.

Current State Finding 1: No Consistent Definition of a CDE

One of the most significant challenges is the lack of consistency in distinguishing a granular data attribute from a derived or calculated business measure. Many firms, in the hope to simplify, are using the same nomenclature to describe logical concepts, business objectives, calculation processes, derived elements and physical expression. The concepts described above are all real and essential *things* – but they are not the same thing - and by calling them all critical data elements leads to significant confusion.

Current State Finding 2: Inconsistent Process for Designating CDEs

General agreement that the business process defines criticality existed across the organizations but there was a lack of acknowledgment of all the business processes that may be consuming the same data. The concept of a data supply chain was not included in their approach. In addition, the full range of stakeholders of the data often was not included in determining criticality. There were, however, examples of organizations that recognized the identification of criticality as a negotiation between the data producer and the data consumer.

Some organizations had attempted to quantify criticality by applying a matrix formula to calculate an ***objective*** criticality measurement. Without exception, this absolute measurement had been abandoned for more ***subjective*** analysis. (See section: *Measuring Criticality: Art or Science*)

Current State Finding 3: Undefined Guidelines for Managing Criticality

The designation of a data element as critical means it is covered by the organizational policy and standards resulting in increased data management rigor being applied to achieve a heightened level of control. The following were common themes across the firms involved in the initial interviews and the subsequent analysis by the Best Practice Work Group. However, while the themes were consistent, the execution of each theme had a high variation across the organizations.

- **Definition and Meaning** - the number one issue is the challenge of locking down a precise meaning and harmonizing language.
- **Lineage** - minimally, an understanding of data flow is required, but the difficulty, cost, and inability to adequately maintain data lineage have escalated questions as to the role and value of data lineage across all CDEs.

- **Data Quality** - difficulty to negotiate agreement across multiple stakeholders on how fit-for-purpose criteria, quality tolerance ranges and thresholds, business rules, testing requirements and measurement criteria are expressed.
- **Governance** - managing the relationships between the data producer and one or more data consumer is the most intensive part of the governance challenge because it requires collaboration across multiple stakeholders who often do not have the framework, skills, or precious time from various business process subject matter experts.
- **Metadata** - the inconsistencies within individual organizations in the execution of standards for metadata capture led to difficulty stitching together the different approaches to metadata collection to provide an enterprise view. This has became more apparent with the higher rigor of metadata required for CDEs.

What is a Critical Data Element?

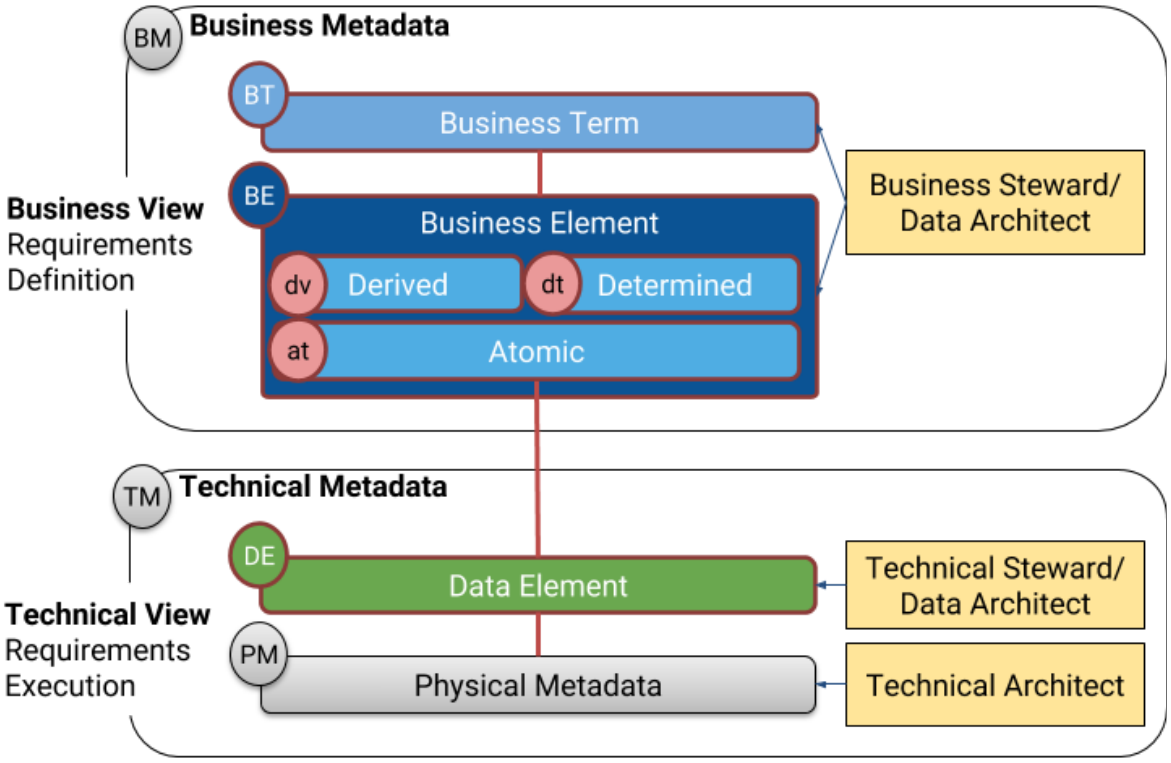
***Objective**: Create an agreed upon understanding of the purpose and definition of a CDE*

To accurately define a CDE, it is necessary to put a CDE in the context of other *things in the same neighborhood* with a CDE.

The Data Neighborhood

The following is a construct that defines and creates relationships between all the things in the data neighborhood. It is a business-friendly representation of the data architecture that presents an understanding of the components and their relationships. With an understanding of the components, a process to identify criticality can be designed.

Business Element / Data Element Construct



Construct Components

- **Business Term** - The name(s) and meaning of common business language.
- **Business Element** - A unit of information that has a specific business meaning in the context of a business process or collection of processes within a domain.
- **Data Element** – A unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes. ISO 11179-1
- **Business Metadata** - Provides context about the data from the perspective of the business process.
- **Technical Metadata** - Used to describe the creation, organization, movement, change and storage of the data from the perspective of the physical implementation.
- **Physical Metadata** - Metadata that describes the physical location of data.

Business Element Types

- **Atomic** – Lowest level of detail, factual meaning. (i.e. Interest Rate)
- **Derived** – Data (concepts, information) that are created from other data or calculated. (Objective i.e. Value at Risk)
- **Determined** – Data elements that are subjective thereby including an element of opinion or human interpretation. (Subjective i.e. Gold Customer - alias: Interpreted)

Critical Designation

- **Critical Business Element (CBE)** - a Business Element that is deemed materially important to one or more business processes.
- **Critical Data Element (CDE)** - a Data Element that is aligned to a Critical Business Element and is deemed materially important.

Diagram 1: Business Element / Data Element Construct

The construct contains a business view and a technical view in relationship to each other. As depicted in the diagram, the players in the neighborhood include business and technical oriented resources. Separating the two views creates clearly defined accountability for the business to manage the Business Element and technology to manage the Data Element.

The ***business view*** defines the business process requirements for the data produced by the process. The business that owns the process is accountable for defining the requirements for the data including the data criticality. The requirements are defined as Business Terms and Business Elements with all the appropriate business metadata. The Best Practice workgroup determined there was sufficient difference between a Business Term and Business Element they warranted clear separation, and both were different than a Data Element.

Similarly, the ***technical view*** is an interpretation of the business process requirements for data transformed into technical data requirements. The data requirements are defined as a Data Element with all the appropriate technical metadata including the physical metadata. The use of the Data Element term is aligned to ISO Data Element standard to ensure architecture consistency with other standards.

The Business Element is conceptual, and the Data Element is the technological execution of the Business Element. The ISO standards body have defined a “Data Element”, and the EDMC Data Neighborhood reflects the ISO definition and clearly distinguishes that from a “Business Element”.

Determining whether data is critical is from the perspective of the business process that is consuming the data. Criticality is a business designation based on an assessment of the material impact the data has on the outcome of a business process. It is this principle that places accountability on the business to identify critical data as part of the requirements for data, so the identification is part of the requirements for the Business Element. Therefore, a Business Element that is critical is a Critical Business Element (CBE) and will also have a corresponding Critical Data Element (CDE).

This will be presented more fully in the section titled Data Producer / Data Consumer Relationship.

Validation

Two approaches were used to validate the Business Element / Data Element Construct worked in real life examples and were consistent with other architectural viewpoints.

1. **Use Case** - apply the construct to actual data that have different type and levels of complexity
2. **Data Architecture & Modeling** - align the construct with traditional data architecture and modeling standards

Use Case Scenarios

To validate the Best Practice, four scenarios were solicited from the group. These scenarios are not considered an exhaustive set of CDE scenarios – instead, they are used as a mechanism for a practical demonstration of the concepts defined in the proposed Business Element / Data Element Construct.

As presented the scenarios generally move from the most simple to the more complex. ***The language and concepts defined in the Business Element / Data Element Construct were deemed to be viable in all provided scenarios.***

Credit Maturity Date - Represents a scenario where different business requirements for a similar Business Element exists in the enterprise, and how to disambiguate the various concepts used.

Total Cumulative Return - Represents a complex derived Business Element and the need to deconstruct the derivation into its atomic parts.

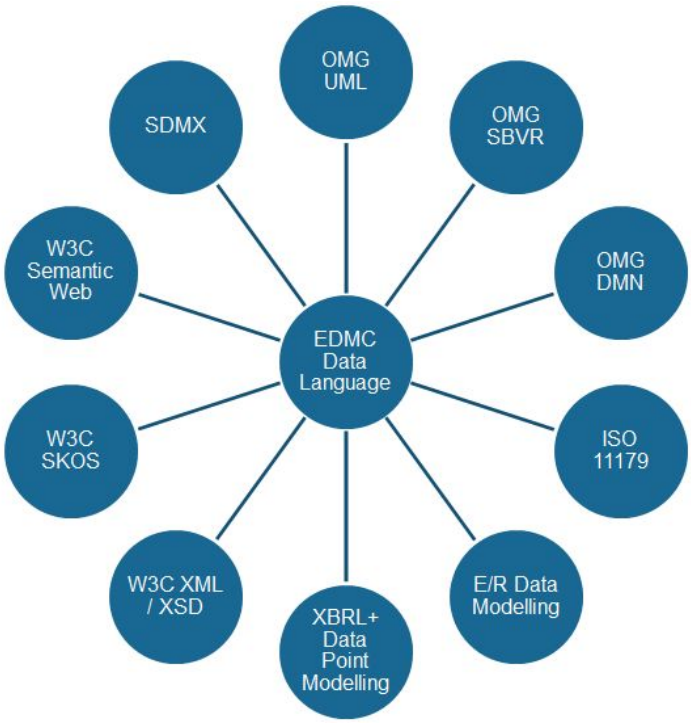
Registered Address - Introduces the concept of compound or composite data that has meaning with other contextual information. Addresses are common but are complicated to handle as critical data as they are often persisted in different ways, and managed differently depending on the role they are playing and the technology platforms used. This scenario identifies one way an Organization may identify and manage CDE's representing a *Registered Address*. Note the actual implementation and approach may be different depending on underlying data and platforms, and there is significantly more complexity when using this in a large federated environment. The implementation pattern choices could make up an entire chapter on its own. However, this use case serves as one way of identifying the data management concepts in this scenario.

Risk FX Vega - Introduces a tabular concept used to contain several related values to holistically represent a Business Element (in this case FX Vega). Vega is the measurement of an option's price sensitivity to changes in the volatility of the underlying asset. Vega represents the amount that an option contract price changes in reaction to a one percent change in the implied volatility of the underlying asset. This is a Risk metric used to measure portfolios containing options and is made up of several data points (table). This is the first scenario where a Data Element is comprised of many calculated elements based off more than one dimension (Currency Pair & Tenor).

The actual documented use cases are presented in the Appendix: Business Element / Data Element Use Case Validation.

Data Architecture & Modeling Validation

As the group evolved the language surrounding CDEs that resonated with the business community, it was necessary that the architecture viewpoint be considered to ensure the language did not contradict any architecture standards or principles.



To achieve alignment, the data architecture subgroup ensured the language and definitions were compatible with other architectural standards. The rationale is that the EDMC language and meaning should not contradict any industry standards to avoid confusion by users of those standards. The investigated standards were:

- OMG
- W3C
- ISO
- Other standards
  (ArchiMate, XBRL, O-DEF, E/R, etc.)

It is worth noting that the studied industry standards had been created over time by different groups with different perspectives. While it wasn't possible to keep 100% alignment with all the standards, compatibility was maintained with the major standards.

It is also worth restating, the ultimate data language needs to be simple enough to be adoptable by business users that will not have a rigorous architecture background, while also being relevant to the language of the technical users in the organization.

A separate smaller Data Architecture group worked through the various standards to ensure the language used in the Business Element / Data Element Construct was consistent in language, meaning, and usage with the other standards. Additionally, a logical model was created to ensure the concepts could be modeled in a way to ensure every concept is clearly distinct from other concepts. Whilst the logical model is not formally part of this whitepaper it serves as a useful tool that architects can use to clearly see how the different terms relate to each other. The model is presented in the Appendix: Alignment to Data Architecture & Modeling Analysis.

CDE Purpose - Prioritizing Data

The objective of prioritizing the data is to identify which data is critical to the business processes consuming the data and thus requires heightened levels of control to ensure the data is fit-for-purpose.

The Basel Committee on Banking Supervision's standard titled *Principles for Effective Risk Data Aggregation and Risk Reporting* (more commonly referred to as BCBS 239[6]) is often cited as requiring the identification of "Critical Data Elements" (CDEs), when actually, the language is "data that is critical". BCBS 239 citings follow:

> **BCBS 239: Paragraph 16** - The Principles and supervisory expectations contained in this paper apply to a bank's risk management data. This includes data that is critical to enabling the bank to manage the risks it faces. Risk data and reports should provide management with the ability to monitor and track risks relative to the bank's risk tolerance/appetite.
>
> **BCBS 239: Paragraph 30 -** Senior management should also identify data critical to risk data aggregation and IT infrastructure initiatives through its strategic IT planning process.
>
> **BCBS 239: Paragraph 43 -** Supervisors expect banks to produce aggregated risk data that is complete and to measure and monitor the completeness of their risk data. Where risk data is not entirely complete, the impact should not be critical to the bank's ability to manage its risks effectively.

BCBS 239 is targeting the bank's Risk Management data but the concept applies to all data for all business processes, not just Risk or Finance organizations.

Prioritizing Data Based on Criticality

***Objective**: Develop a best practice process and tools for the identification of CDEs*

Overview

Since not all data has the same significance or impact the highest risk data needs to be addressed first. This section covers an approach using criticality to enable the organization to prioritize and bring under control its data assets. ***Prioritization is a key part of a successful data management program***, without appropriate prioritization the program is at risk of being overwhelmed with too much data to manage sooner than the organization can deliver.

[6] BCBS 239 - Principles for Effective Risk Data Aggregation and Risk Reporting - https://www.bis.org/publ/bcbs239.pdf

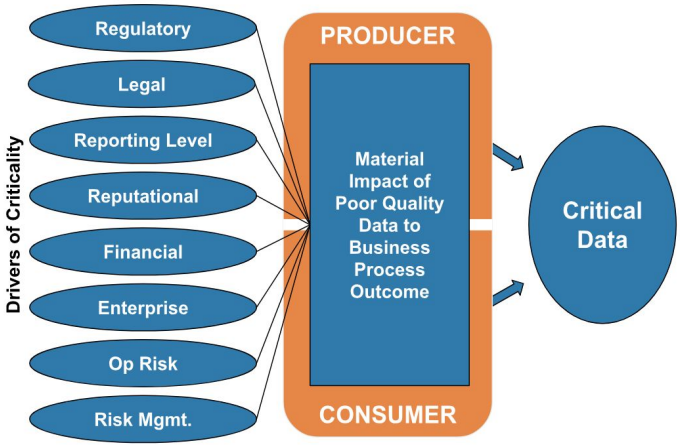
Drivers of Criticality with Materiality Overlay

To identify *criticality*, one must introduce the concept of **materiality** which aligns with the standard notion of a risk-based approach.

> **Materiality** - the degree to which the use of a data element in the business process could result in a substantive impact to the financial, operational or reputational position of the organization.

Some organizations have introduced levels of materiality with the highest level identified as *Critical*.

- Critical
- Important
- Significant
- Unimportant
- Not Reviewed



What makes data critical is the material impact it has on the outcome of a business process.

- Criticality comes from the perspective of the business process that is consuming the data (Data Consumer)
- Determining materiality is a negotiation between the Data Producer and Data Consumer
- It is common, for a Consumer to assume that all data are critical
- There are drivers associated (see next section for more details) with criticality that can guide the negotiation
- Criticality has not been successfully quantified using well defined rules, leaving it to be determined through an artful analysis rather than a hard science

Measuring Criticality: Art or Science?

Using the drivers of criticality as outlined above, a Criticality Evaluation Matrix is a valuable tool to support the decision-making process.

Many organizations initially attempted to approach identifying criticality with a quantified calculation. This is represented in the **Objective Rating** row in the matrix below. This may include weighting of the relative importance of any of the criterion. This rating scale needs to be driven by the risk appetite of the organization.

However, member organizations that tried to quantitatively measure data criticality experienced poor adoption and ultimately switched the approach to use the spirit of the measurement as art versus science as represented in the **Subjective Rating** row of the matrix.

Essentially, the subjective approach uses the matrix as a guideline to identify potential critical data and assess the scope of the impact of the critical data (Global, Regional, Local). This is done to inform a negotiation between the Data Producer and Data Consumer to reach an agreement on the data that is truly critical.

	Criticality Dimension							
	Regulatory	**Legal**	**Reporting Level**	**Reputational Impact**	**Financial Impact**	**Enterprise Performance**	**Operational Risk**	**Risk Management**
	Indicates whether the data attribute is mandated by regulatory entities to be used and managed in a particular way. Data provided to regulators. Data is subject to audit or traceability.	Indicates whether the data attribute has a risk of a large number of proceedings and the payment of consequential damages and/or criminal sanctions.	Indicates the level at which the data is consumed in the organization; Board or Management Team exposure carries higher risk.	Indicates whether a data attribute is relied upon by clients or third parties… if it is wrong, reputation and trust is placed at risk.	Indicates a quantifiable financial result to poor data quality.	Indicates whether the data attribute is essential for the management of the business and to help manage the firm's ability to meet strategic or operational objectives.	Indicates whether the data attribute helps manage operational outcomes. Operational processes, upstream or downstream, would fail if data was not present or was incorrect.	Indicates whether the data attribute enables us to anticipate or manage potential risk to the business.
Objective Rating (Sample Scale)	4 - Global 3 - Regional 2 - Local	4 - Global 3 - Regional 2 - Local	4 - Global 3 - Regional 2 - Local	4 - Global 3 - Regional 2 - Local	4 - >$X 3 - >$X - <$X 2 - <=$X	4 - Global 3 - Regional 2 - Local	4 - Global 3 - Regional 2 - Local	4 - Global 3 - Regional 2 - Local
Subjective Rating	High / Medium / Low							

Diagram 2: Criticality Evaluation Matrix

Considerations

- ➔ Private or sensitive data are not identified as a criterion of criticality. While private or sensitive data can be designated as critical, it is due to the material impact of the data on the business process outcome - this is different than information security or privacy concerns. Measuring the materiality of poor quality private data is by using the criteria in the construct (e.g. Regulatory, Reporting Level, Reputational Impact, etc.). More background is available in a report on GDPR published by EDM Council in May, 2018[7].
- ➔ In practice, the harder job is identifying data that is *not* critical.
- ➔ An alternative to artfully measuring the drivers of criticality across all data may be first to prioritize based on the level of Data Consumer (e.g., Enterprise level-most important, External level-second, two or more business processes-third, etc.). The data consumed at the highest level would be first for evaluating criticality.

[7] General Data Protection Regulation (GDPR): The Role of Data Management, https://edmcouncil.org/global_engine/download.aspx?fileid=D62B9151-DE65-4AE8-BA1B-B1DEB9B25D47&ext=pdf

Prioritizing Criticality

Different than the objective for *prioritizing data based on criticality*, the objective of *prioritizing the critical data* is to identify the most important data based on business objectives in ranked priority. Those ranked priorities are then used to apply a heightened level of control within the time and resource constraints of the organization. There are three primary approaches to set the scope of critical data.

- **Everything**: Identifying all critical data across the organization
- **Scoping Strategy**: Prioritizing a subset of data by prioritized Use Case
    - Regulatory oriented - high-risk reports or programs (e.g. BCBS 239)
    - Business Process oriented criticality (business problem oriented)
    - Application oriented criticality
    - Project oriented (Fix forward - remediate backward)
- **Hybrid**: Set a volume or percentage of data that can be critical (set a target %)

Regardless of the approach to setting the scope, if the volume of identified elements exceeds the current capacity of the organization, it will need to prioritize the sequence of the work further.

Prioritization Approach	Pro	Con
Subset	The benefit of prioritizing a subset of data aligned to a priority use case is that it is quick and easy and can gain attention and support from senior management.	The risk is that you create a false impression that this is the full scope of critical data.
Comprehensive	The benefit of a comprehensive inventory of all critical data is that you set accurate expectations for the scope of work.	The volume of in-scope data can be overwhelming and dilute the attention and support of senior management.
Hybrid	Manages the expectations of the management team.	Often cannot predict the effort or timelines associated with the effort.

Data Producer / Data Consumer Relationship

Data Supply Chain

Understanding how data exists in the Data Supply Chain is key to understanding the relationship between Data Producers and Data Consumers.

A Domain consumes data from upstream producers, produces data and consumes that data within the domain, and, a domain also produces data for downstream consumers. Domain management includes reconciling all requirements for data across the data supply chain.

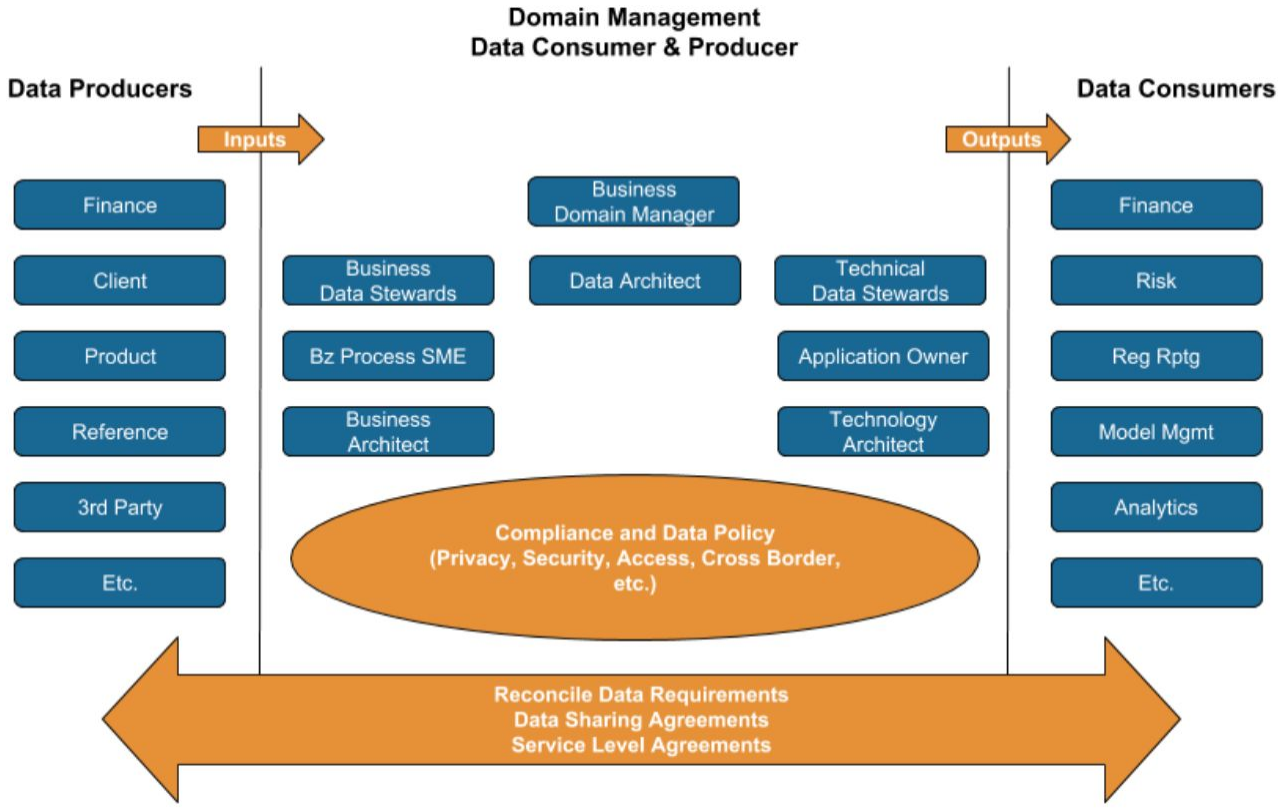


Diagram 3: Data Supply Chain Construct

Business Process Perspective

Accountability for data is with the owner of the business process that creates the data - the Data Producer. This adds another perspective to understanding the relationship between Data Producer and Consumer. The Data Consumer is responsible to ensure that the data is appropriately used and fit for purpose for their business process.

- A business process has requirements for data as inputs and outputs of the process.
- The “owner” of the business process that creates data is the Data Producer.

- A business process that consumes data from another data domain is a Data Consumer and is responsible for defining requirements for data and holding the Data Producer accountable.
- A Data Producer is responsible for meeting the data requirements of the Data Consumer. These requirements include precision of meaning, data quality dimensions, access, and authorization of use, monitoring, measuring, etc.
- A Data Producer is also usually a Data Consumer. Every Data Producer consumes their data to support their process, but often they also consume data from upstream of their operation.
- Criticality of a Business Element is proposed by the Data Consumer and validated and accepted or rejected by the Data Producer.
- The Data Producer must first determine that the requested Business Element is within the scope of their data domain before assessing the proposed criticality of the Business Element.
- The entire process between the Data Consumer and Data Producer is based on the requirements for data and use of the data in the consumer's business process.
- The heightened level of control applied to a Critical Business Element is what permits Data Producers and Data Consumers to agree to the "fit-for-purpose" of the data consumed.

The Negotiation

When the Data Consumer proposes criticality, the natural inclination is to declare all data consumed as critical to their business process. If the organization's funding model places the accountability for funding solely on the Data Producer, there is no financial consequence to the Data Consumer for the cost of the enhanced control applied to Critical Data Elements. This results in a strain on the negotiation process between the Data Producer and Data Consumer. The Data Producer and Data Consumer will have to agree to operate within mutually defined resource constraints. The negotiation is further complicated when a Data Producer is managing priorities from multiple Data Consumers at which point the Data Governance framework must provide an escalation protocol for mediating priorities that exceed resource capacity of the Data Producer. The reality of resource constraints, even at the Enterprise level, requires the organization to define the level of resources that can be applied to achieve the implications of managing criticality.

Setting resource constraints aside, even when an assessment of Criticality Dimensions is used to inform the criticality designation there will be differences in opinion that will need to be negotiated. The Data Producer needs to understand the actual use of data by the Data Consumer to reach an agreement for criticality and to ensure the data are fit-for-purpose by the Data Consumer.

As stated above, the negotiation process is compounded because it is not one-to-one but a one-to-many negotiation (multiple consumers who may have variation in their requirements). One of the roles of the Data Producer is to align and manage Data Consumer requirements to develop as simple a data set as possible.

Governance of the process of agreeing to criticality needs to include an opportunity for escalation when the Data Producer and Data Consumer data domains cannot reach an agreement on criticality or prioritize criticality within the resource constraints.

Considerations

- ➔ For the negotiation to be effective it must be fact-based with transparency between the Data Consumer requirements and the Data Producer assessment of the requirements. This transparency is even more critical when the level of subject matter expertise about the business process and the data exists on only one side of the negotiation.
- ➔ Alignment to the organization's funding model is critical.
- ➔ Alignment to the organization's governance model is critical.

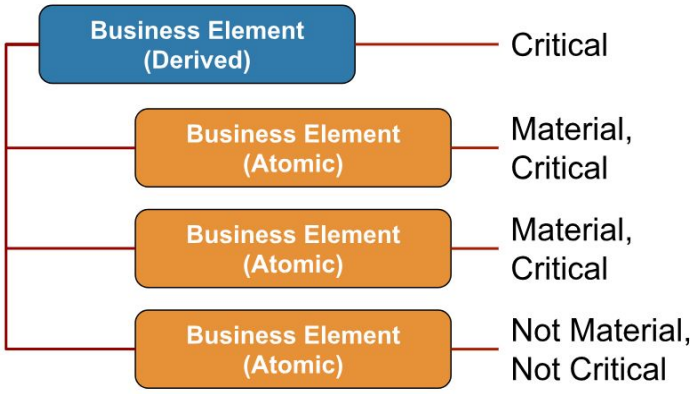
Derived Data

As part of the exploration of the Data Neighborhood there are often questions if Derived Data could be considered critical, or even if it should be managed. This section aims to defined what "Derived Data" is and how that fits into criticality and broader data management.

EDMC has defined Derived Data as:

Data (concepts, information) that are created from other data or calculated.

While a derived data value can be a Critical Business Element, managing criticality is at the atomic level. In the case of a derived Critical Business Element, the Data Producer should evaluate the inputs to determine if they are also critical. Each input value should be judged separately for material effect on the fit-for-purpose quality of the derived value. Do not assume that all inputs will have a material impact on the quality of the derived output and ultimately on the business process outcome.



Furthermore, if the inputs to the derived CBE are themselves derived Business Elements then first determine the material impact of poor quality of each of the derived inputs. If it is deemed to be material, then the Business Element should be defined as critical, and its inputs will then need to be evaluated for material impact. This deconstruction process must continue until all inputs are at an atomic level (or back to a point where the adequate control of the element is demonstrated), and this helps inform the Data Lineage effort often associated with Critical Elements. The quality of a derived Critical Business Element is managed at the atomic level of its "critical" inputs.

The quality of the inputs and the *execution* of the business logic of the derivation is a Data Management accountability. The actual *business logic* of the derivation is a business process accountability.

When derivations create new Business Elements, they should be recorded and an accountability review performed on the new Business Elements. If the subject matter expertise for the new data lies with the

Data Consumer or the data is derived from multiple Data Producers then the accountability should shift from the original Data Producer(s) to the producer of the new derived data. Regardless of who has accountability the principle of Authoritative Provisioning Point should be maintained so that all consumers of the Business Element obtain the element from a single point of provisioning.

Considerations

➔ How far back do you go to get to and manage the inputs? (This will be addressed by the final work of the Best Practice Work Group: Implications of Criticality.)

Process Integration

The EDM Council industry standard process design utilizes a 6 level model as defined below. Practically, an industry standard can only design to Level 3. Beyond Level 3 a standard becomes organization and role specific.

- Level 0: Value Chain - Components
- Level 1: Process Groupings - Process Groups based on Component
- Level 2: Core Processes - Activities and Tasks based on Process Group
- Level 3: Business Process Flow - Processes and Sub-processes based on Functional Role

- Level 4: Operational Process Flow - Process Documentation based on Role
- Level 5: Detailed Process Flow - Procedures (step-by-step documentation) based on Role

Stakeholder Data Management Component Responsibilities - Level 2

The Level 2 process is presented at the Component level with alignment back to DCAM Framework Capabilities and Sub-capabilities.

The table below represents the Components that are required to execute the Data Domain Management process.

Component	Detailed Description
Data Control Environment	• The process of data domain management is in the Data Control Environment Component. • The process of prioritizing data based on criticality resides within the data domain management process.
Data Architecture	• The process of prioritizing data based on criticality is dependent on defining requirements for data, identifying data, defining data, and profiling data.
Data Quality Management	• The process of prioritizing data based on criticality does not require the Data Quality Management Component. Data Quality Management is part of the overall Data Domain Management and will be integral to the process of managing the implications of

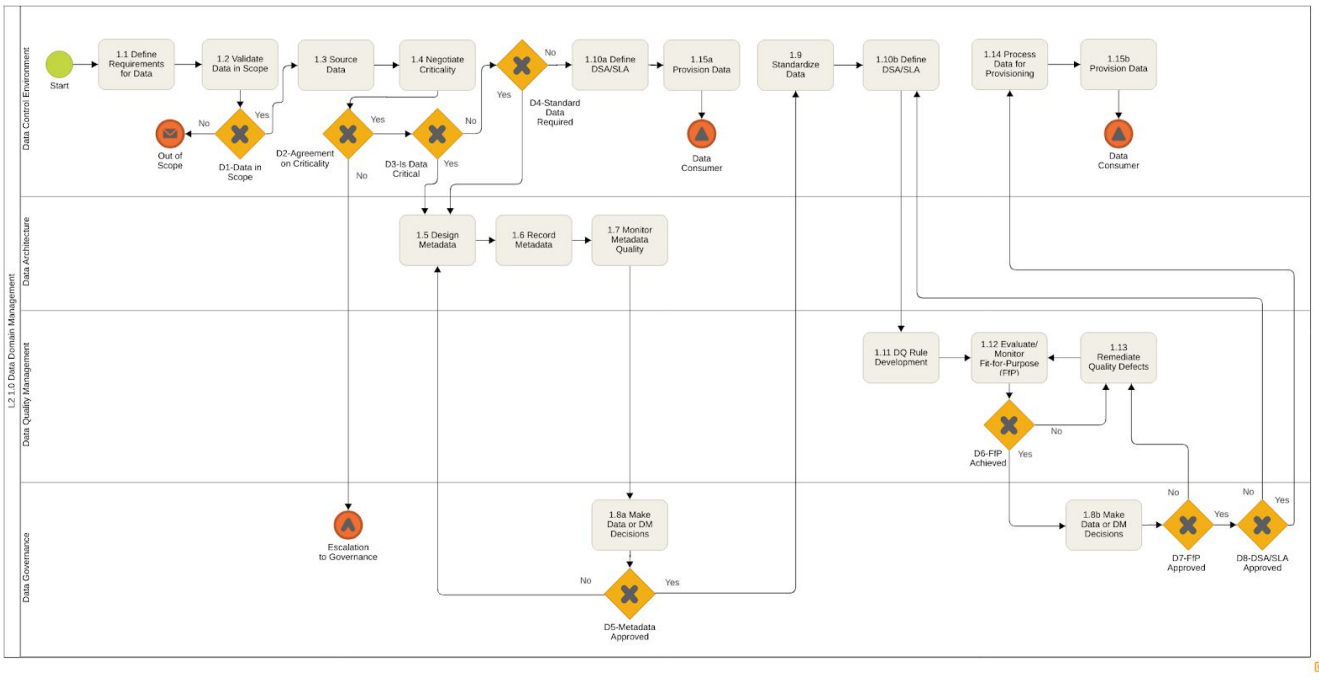
	criticality.
Data Governance	• The process of prioritizing data based on criticality leverages the Data Governance Component for approving the metadata and the criticality designation.

Level 2 1.0: Data Domain Management Process

Summary

The Data Domain Management Process is where the DCAM Framework Components of Data Governance, Data Architecture, and Data Quality are brought together to execute on a specific set of data in the Data Control Environment.

Process Flow



Process Flow 1: L2 1.0 Data Domain Management Process

Process Details

The Tasks outlined in red support the process of prioritizing data based on criticality as defined in this report. However, achieving the means of prioritizing data based on criticality and managing the criticality is dependent upon the complete Data Domain Management Process.

Task ID	Function	Task Description
1.1	Data Control Environment	Define Requirements for Data ● The business process consuming the data (Data Consumer) develops requirements for data as an input to their process. ● The requirements include proposed criticality with a description of material impact to business process as a result of poor quality data.
1.2	Data Control Environment	Validate data in Scope ● The business process producing the data (Data Producer) determines whether the requested data is within the scope of their domain.
D1	Data Control Environment	Data in scope? ● If yes, move to Task 1.3. ● If no, is there a referral for which domain may be in scope. Communicate to Data Consumer the scope outcome and recommendation if applicable. Process stops.
1.3	Data Control Environment	Source Data ● Go through appropriate steps to analyze the requirements, identify the data, locate the data, source the data (access data for analysis and preparation for provisioning) and record basic metadata.
1.4	Data Control Environment	Negotiate Criticality ● Data Producer reviews Data Consumer's proposed critical designation based on analysis of material impact to business process of poor quality data. ● Agreement of Critical Elements is reached or disagreement is escalated.
D2	Data Control Environment	Agreement on Criticality? ● If yes, move to D3, is it critical ● If no, escalate criticality decision
D3	Data Control Environment	Is data critical? ● If no, move to D4, is standard data required. ● If yes, move to Task 1.5 to design metadata.
D4	Data Control Environment	Standard data required? ● Does the Data Consumer require standardized data? ● If no, move to Task 1.14a to provision non-standard data with appropriate controls on use. ● If yes, move to Task 1.5 to design metadata.
1.10a	Data Control Environment	Define Data Sharing Agreement (DSA) & Service Level Agreement (SLA) ● Establish restrictions on the use of non-standard data and

		parameters of provisioning.
Tool		Data Sharing Agreement Service Level Agreement
1.15a	Data Control Environment	Provision Data ● Provision the non-standard data with appropriate controls on use (proportionate to the criticality of the data).
1.5	Data Architecture	Design Metadata ● Design metadata (data about the data) that is required for the appropriate level of control on the data. ● This task works in conjunction with the parameters of the Enterprise Policy and the proposed Data Sharing Agreement (DSA) which defines the required level of control on the data.
1.6	Data Architecture	Record Metadata ● Record d metadata about the data in the appropriate repository(ies).
1.7	Data Architecture	Monitor Metadata Quality ● Monitor the metadata quality for accuracy, completeness, and timeliness. ● Once metadata quality is deemed adequate, submit to the appropriate data governance body for approval.
1.8a	Data Governance	Make Data or Data Management Decisions ● Data governance body reviews metadata quality report gaps to validate alignment with Enterprise Policy.
D5	Data Governance	Metadata approved? ● If no, return to Task 1.5 to close identified gaps. ● If yes, move to Task 1.9 to standardize the data.
1.9	Data Control Environment	Standardize Data ● Apply logic to transform the data into the standardized form.
1.10b	Data Control Environment	Define Data Sharing Agreement (DSA) / Service Level Agreement (SLA) ● Data Producer and Data Consumer agree to all parameters in the DSA. ● Producing Technology Manager and Consuming Technology Manager in accordance with the DSA parameters agree to all parameters in the SLA.
1.11	Data Quality Management	DQ Rule Development ● Define the range of quality rules to run against each element to validate the fit-for-purpose of the data.
1.12	Data Quality Management	Evaluate / Monitor Fit-for-Purpose ● Execute the defined rules to generate defect reporting. ● Evaluate completeness of rule set.

D6	Data Quality Management	Fit-for-purpose achieved? ● If no, move to Task 1.13 to remediate quality defects. ● If yes, move to Task 1.8b to make data or data management decision.
1.13	Data Quality Management	Remediate Quality Defects ● Complete all processes to remediate quality defects.
1.8b	Data Governance	Make Data or Data Management Decisions ● Data governance body reviews metadata and data quality to approve data are fit-for-purpose and to validate alignment with Enterprise Policy and DSA / SLA.
D7	Data Governance	Fit-for-purpose approved? ● If yes, move to D6 to approve DSA / SLA. ● If no, return to 1.11 to close identified gaps.
D8	Data Governance	DSA / SLA approved? ● If yes, move to 1.14 to process data for provisioning. ● If no, return to 1.10 to close identified gaps.
1.14	Data Control Environment	Process Data for Provisioning ● Run all period close activities to prepare data for provisioning.
1.15b	Data Control Environment	Provision Data ● Execute provisioning routine defined in the SLA.

Stakeholder Functional Roles and Responsibilities - Level 3

The Level 3 processes are presented at the Functional Role level with alignment back to DCAM Framework Capabilities and Sub-capabilities.

The chart below details Data Domain Management functional roles and responsibilities aligned to the Data Management Functional Construct. These functional roles apply to all of the Level 3 processes detailed in the report.

Functional Role	Detailed Description
Business Data Management - Producer	A process, application or stakeholder that provisions data to one or more Data Consumers
Business Data Management - Consumer	A process, application or stakeholder that receives or uses data from a Data Producer.
Data Architecture	The function that defines and implements the data content strategy for a given subset of data.
Technology Delivery - Producer	The function that designs, builds, and runs the technical infrastructure supporting the Data Producer.

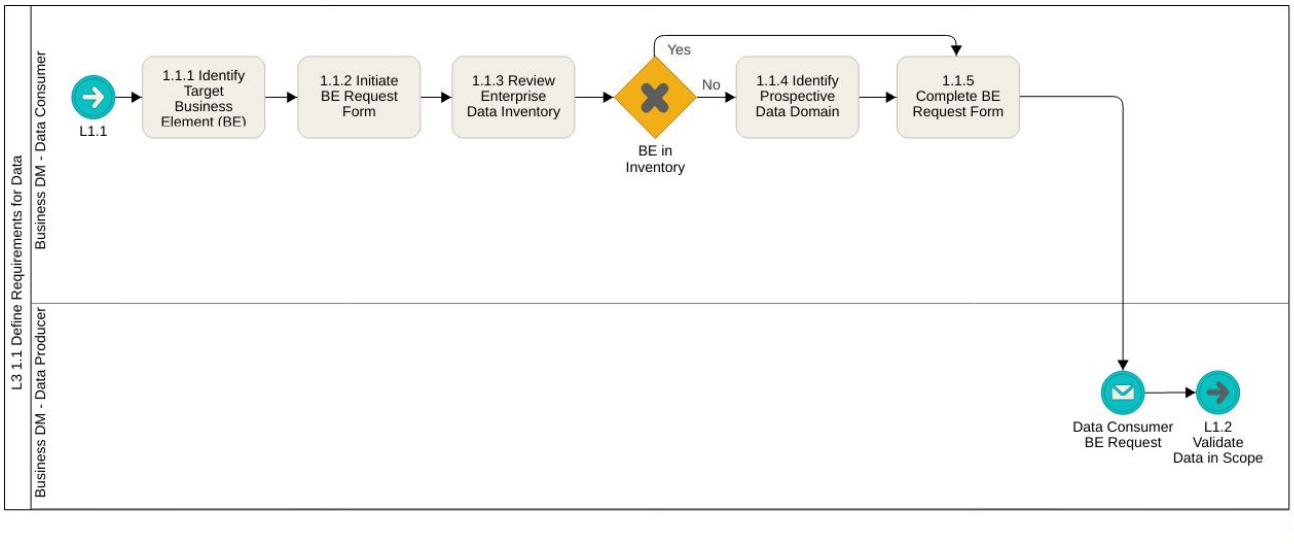
Technology Delivery - Consumer	The function that designs, builds, and runs the technical infrastructure supporting the Data Consumer.

Level 3 1.1: Define Requirements for Data

Summary

Within the Data Domain Management Process the activity of defining requirements for data are completed by the Data Consumer.

Process Flow



Process Flow 2: L3 1.1 Define Requirements for Data

Process Details

Task ID	Functional Role	Detailed Description
1.1.1	Business DM - Data Consumer	Identify Target Business Element (BE) • Based on the needs of the business process define the requirements for data
1.1.2	Business DM - Data Consumer	Initiate Business Element Request Form • Record all known requirements in the form
Tool		Business Element Request Form • The form includes a standard set of required and optional (if known) attributes necessary to accurately communicate the request to the Data Producer
1.1.3	Business DM - Data Consumer	Review Enterprise Data Inventory • Search the repository for a Business Element record that aligns to the defined requirements for data

D1	Business DM - Data Consumer	Is the Business Element in Inventory? ● If yes, move to 1.1.5 to complete the BE request form ● If no, move to 1.1.4 to identify suspect data domain
1.1.4	Business DM - Data Consumer	Identify Prospective Data Domain ● Based on Data Consumers understanding of the data select the most likely data domain
1.1.5	Business DM - Data Consumer	Complete Business Element Request Form ● If found in inventory, cite the BE ID and identify any requirement discrepancies in the Enterprise Data Inventory ● If not found in inventory, complete all required items and those optional items that are known
Com1	Business DM - Data Producer	Deliver Data Consumer BE Request ● Data Consumer delivers to the Data Producer of the suspect data domain

Considerations

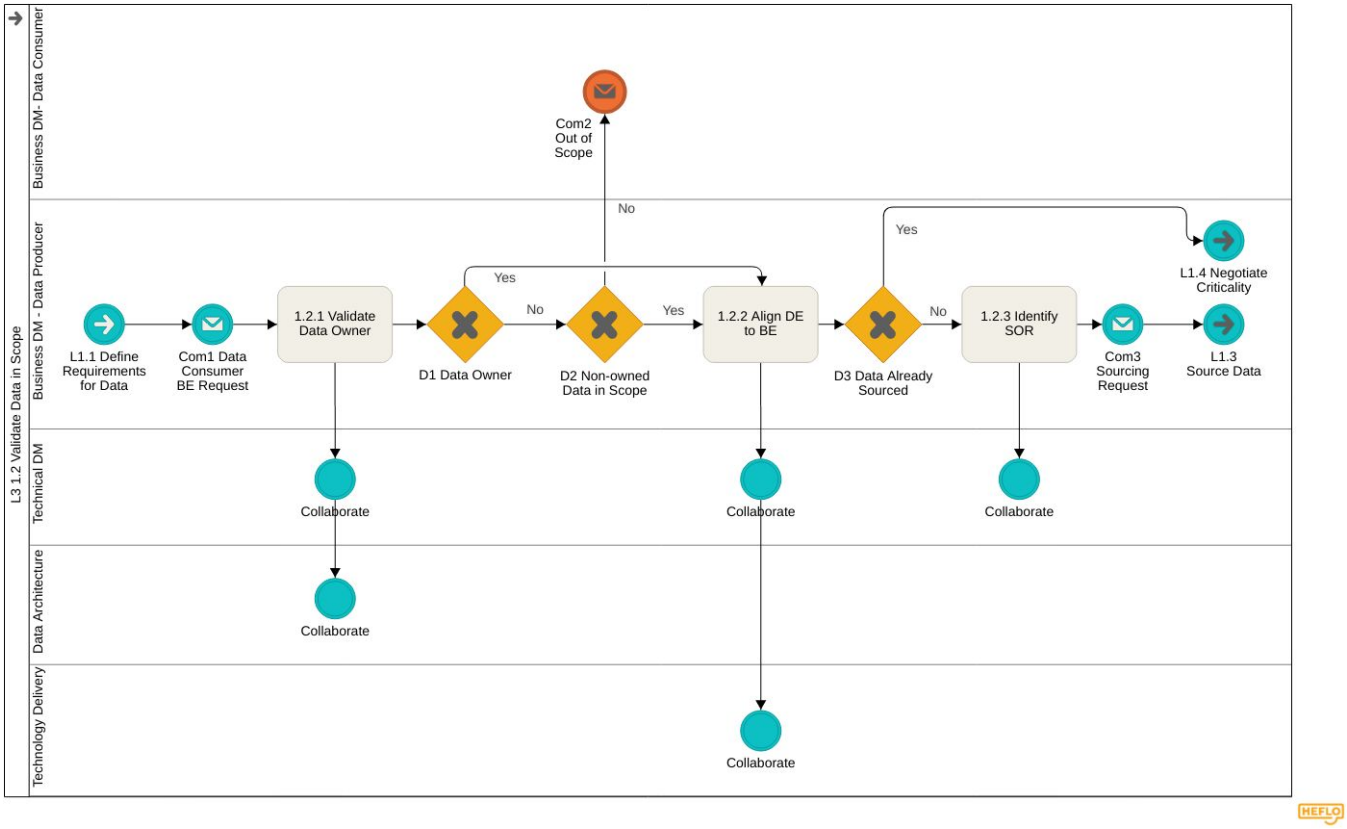
➔ When the target data are consumed by more than one domain some organizations support the definition of requirements for data through a centralized center of excellence.

Level 3 1.2 Validate Data in Scope

Summary

Within the Data Domain Management Process the activity of validating that the Data Consumer requested data are in scope is completed by the Data Producers.

Process Flow



Process Flow 3: L3 1.2 Validate Data in Scope

Process Details

Task ID	Function	Detailed Description
Com1	Business DM - Data Producer	Receive Data Consumer BE Request • Data Consumer delivers to the Data Producer of the suspect data domain
1.2.1	Business DM - Data Producer	Validate Data Owner • Using the request form information investigate whether the data are owned by the receiving Data Producer
D1	Business DM -	Is Data Owner correct?

	Data Producer	● If no, move to D2 to decide if the non-owned data are in scope ● If yes, move to 1.2.2 to align the DE to the requested BE
D2	Business DM - Data Producer	Is non-owned data in scope (Upstream Data Owner by DSA approves pass-through distribution non-owned data)? ● If yes, move to 1.2.2 to align the DE to the requested BE ● If no, move to Com2 to communicate data are out-of-scope
Com2	Business DM - Data Produce	Communicate Out-of-Scope ● Data Producer communicates to Data Consumer that the requested BE is not in scope to the Producer's Domain (Data Producer should share any suspected data domains if known)
1.2.2	Business DM - Data Producer	Align DE to BE ● Based on the requirements for the BE identify all the DEs that align with the requirements
D3	Business DM - Data Producer	Is data already sourced (available in Authoritative Provisioning Point)? ● If yes, move to Process 1.4 Negotiate Criticality (non-owned data can be in scope if the upstream Data Owner allows the pass-through distribution of the data) ● If no, move to 1.2.3 to identify the DE System of Record(s) (SORs)
1.2.3	Business DM - Data Producer	Identify SOR ● Based on the DE to BE alignment identify the SOR(s)
Com3	Business DM - Data Producer	Data Sourcing Request ● Request the DE(s) to be sourced by the Technology Delivery Producer

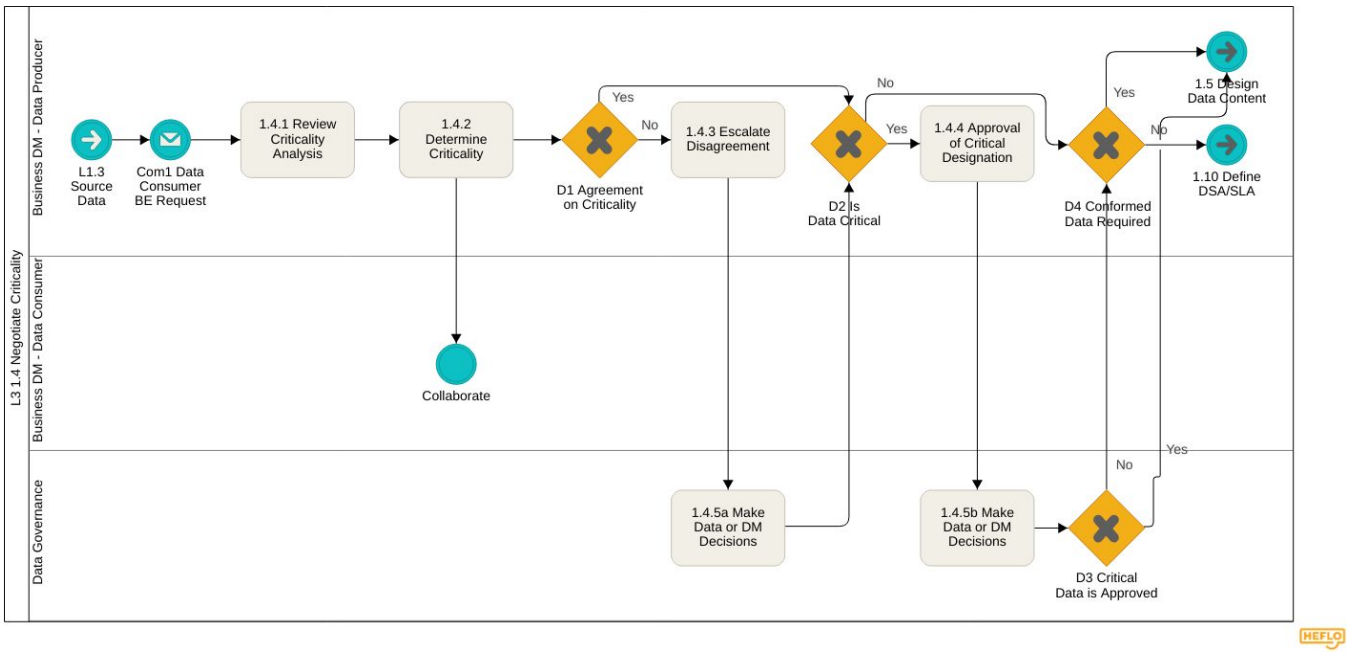
Level 3 1.4 Negotiate Criticality

- Data Producer reviews Data Consumer's proposed critical designation based on analysis of the material impact to the business process of poor quality data.
- Critical or Non-critical agreement is reached or disagreement is escalated.

Summary

Within the Data Domain Management Process the activity of negotiating criticality is completed by the Data Producer with the Data Consumer.

Process Flow



Process Flow 4: L3 1.4 Negotiate Criticality

Process Details

Task ID	Function	Detailed Description
Com1		Review Data Consumer BE Request Form
1.4.1	Business DM - Data Producer	Review Criticality Analysis • Data Producer reviews Data Consumer's proposed critical designation based on analysis of the material impact on the business process of poor quality data.
1.4.2	Business DM - Data Producer	Discuss Criticality • Data Producer discusses with Data Consumer rationale for material impact on the Consumer's business process of poor quality data

D1	Business DM - Data Producer	Agreement on Criticality? ● If no, move to 1.4.3 to escalate disagreement on criticality ● If yes, move to 1.4.5 for governance approval of the critical data designation
1.4.3	Business DM - Data Produce	Escalate Disagreement ● Escalate disagreement on criticality to appropriate Governance body for resolution
1.4.5a	Data Governance	Make Data or Data Management Decision ● Appropriate Governance body reviews escalated disagreement and resolves critical designation
D2		Is Data Critical? ● If yes, move to 1.4.4 to get approval of critical designation ● If no, move to D3 to determine if standardized data are required
1.4.4	Business DM - Data Produce	Approval of Critical Designation ● The Data Producer governance body must approve criticality designation
1.4.5b	Data Governance	Make Data or Data Management Decision ● Appropriate governance body decisions approval of critical designation
D3		Critical data are Approved? ● If yes, move to 1.5 Design Metadata ● If no, move to D4 Standard Data Required
D4		Standard Data are Required (standard value is required across the data set)? ● If yes, move to 1.5 Design Metadata ● If no, move to 1.10 Define DSA/SLA

Level 3 1.10 Complete DSA/SLA

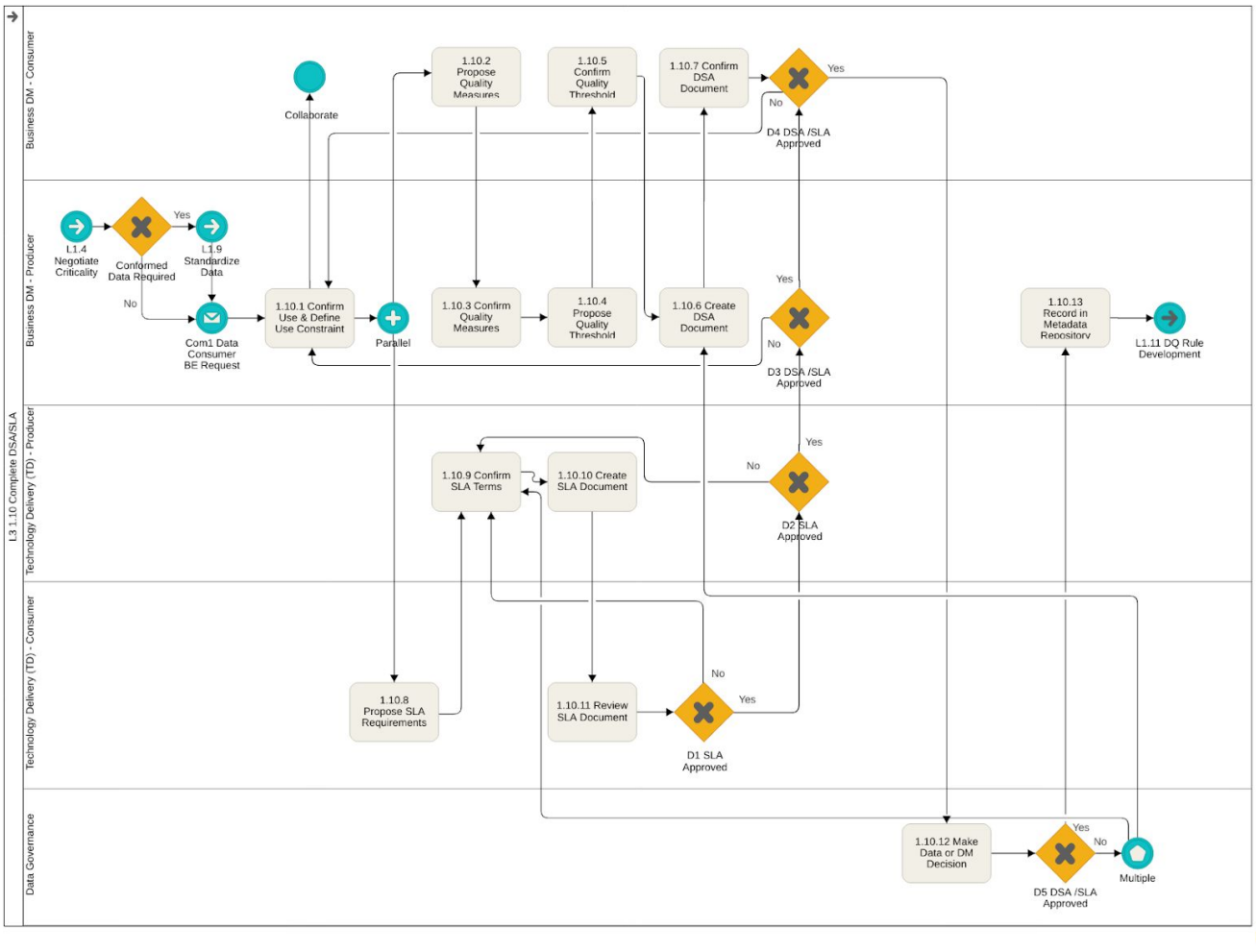
Summary

Within the Data Domain Management Process the activity of completing the Data Sharing Agreement is conducted by the Business Data Management-Data Producer with the Business Data Management-Data Consumer. Similarly, completing the Service Level Agreement is conducted by Technology Delivery Producer with the Technology Delivery-Data Consumer.

Considerations

- → The Data Sharing Agreement is a Domain-to-Domain agreement capturing the business parameters defining the consumer requirements for data and the producer constraints on the use of the data.
- → There is the possibility of business parameters at three levels:
  - Domain
  - Application
  - Element - Data Sets
- → Evaluate the maintenance of the DSA:
  - Frequency of review
  - Controls and compliance
- → The Service Level Agreement is an application-to-application agreement capturing the technical parameters defining the consumer technical requirements for data and the producer technical constraints on the availability of the data.
- → What are the implications to data that is not designated as critical? It may be necessary to establish minimum requirements for:
  - Metadata
  - Use control
  - Quality review and threshold

Process Flow



Process Flow 5: L3 1.10 Complete DSA/SLA

Process Details

Task ID	Function	Detailed Description
Com1		Review Data Consumer BE Request Form
1.10.1	Business DM-Data Producer	Confirm Use & Define Use Constraint • Review the consumer defined use in the BE Request Form • Define the use constraints on the data
1.10.2	Business DM-Data Consumer	Propose Quality Measures for Data Elements • Based on consumer business process, define measurements for data quality
1.10.3	Business DM-Data Producer	Confirm Quality Measures • Evaluate proposed measurements against current measurements and confirm agreed upon measures

1.10.4	Business DM-Data Producer	Propose Quality Threshold ● Evaluating current data quality and cost to enhance data quality, propose the threshold for quality
1.10.5	Business DM-Data Consumer	Confirm Quality Threshold ● Based on the cost of poor quality to the producer business process, confirm an acceptable threshold for quality
1.10.6	Business DM-Data Producer	Create DSA Document ● Create or modify existing DSA document to include all data shared between the producer and consumer data domains
1.10.7	Business DM-Data Consumer	Confirm DSA Document ● Review and confirm the completeness of the DSA document
1.10.8	Technology Delivery-Data Consumer	Propose SLA Requirements ● Based on the requirements of the consumer business process and the constraints of the technical infrastructure, define the application-to-application parameters for data consumption
1.10.9	Technology Delivery-Data Producer	Confirm SLA Terms ● Review and confirm the ability to perform according to the defined parameters
1.10.10	Technology Delivery-Data Producer	Create SLA Document ● Create or modify existing SLA document to include data elements and the parameters for consumption
1.10.11	Technology Delivery-Data Consumer	Review SLA Document ● Review and confirm the completeness of the SLA document
D1	Technology Delivery-Data Consumer	SLA Approved? ● If yes, move to D2 for Technology Delivery-Data Producer approval of the SLA ● If no, move to 1.10.9 to confirm the SLA terms
D2	Technology Delivery-Data Producer	SLA Approved? ● If yes, move to D3 for Business DM-Data Producer approval of the DSA and SLA ● If no, move to 1.10.9 to confirm the SLA terms
D3	Business DM-Data Producer	DSA /SLA Approved? ● If yes, move to D4 for Business DM-Data Consumer approval of the DSA and SLA ● If no, move to 1.10.1 to confirm use and define use constraints
D4	Business DM-Data Consumer	DSA /SLA Approved? ● If yes, move to 1.10.12 to obtain appropriate governance body approval of the DSA and SLA ● If no, move to 1.10.1 to confirm use and define use constraints

1.10.12	Data Governance	Make Data or Data Management Decision ● Appropriate governance body decisions approval of DSA and SLA
D4	Data Governance	DSA /SLA Approved? ● If yes, move to 1.10.13 to record documentation parameters in the metadata repository ● If no (DSA not approved), move to 1.10.1 to confirm use and define use constraints ● If no (SLA not approved), move to 1.10.9 to confirm SLA terms
1.10.13	Business DM-Data Producer	Record in Metadata Repository ● Record DSA and SLA documentation parameters in the metadata repository (critical designation, use constraints, consuming domain, quality threshold, DSA and SLA agreement IDs, etc.)

CDE Implications

***Objective**: Develop a best practice process, procedures and tools for managing the implications of criticality*

The final objective of the Best Practice project is a work-in-process to articulate the implications of criticality as the heightened level of control requirements for the Critical Data Elements. As the work is completed a subsequent report will be published. The target areas for analysis include the following.

Governance - Engaged Governance - executive owners and Business and Technical stewards in place for every CDE with collaboration among producers, consumers, IT and operations

Metadata - Precise Definition - for all front-to-back applications, for all business processes and for all derived formulas

Metadata - Documentation and Metadata - names, definitions, aliases, business rules, provisioning points, authorized data sources, source of data, transformation processes, logical-to-physical mapping, etc.

Data Lineage (vs Data Flow) - End-to-End Lineage - may be required to complete data forensics required to root cause fix of poor quality data (capturing all transformations and calculations across the full business lifecycle)

Data Quality - Fit-for-Purpose - quality measurements, quality thresholds, defect management, root cause analysis and remediation

Appendix

Glossary

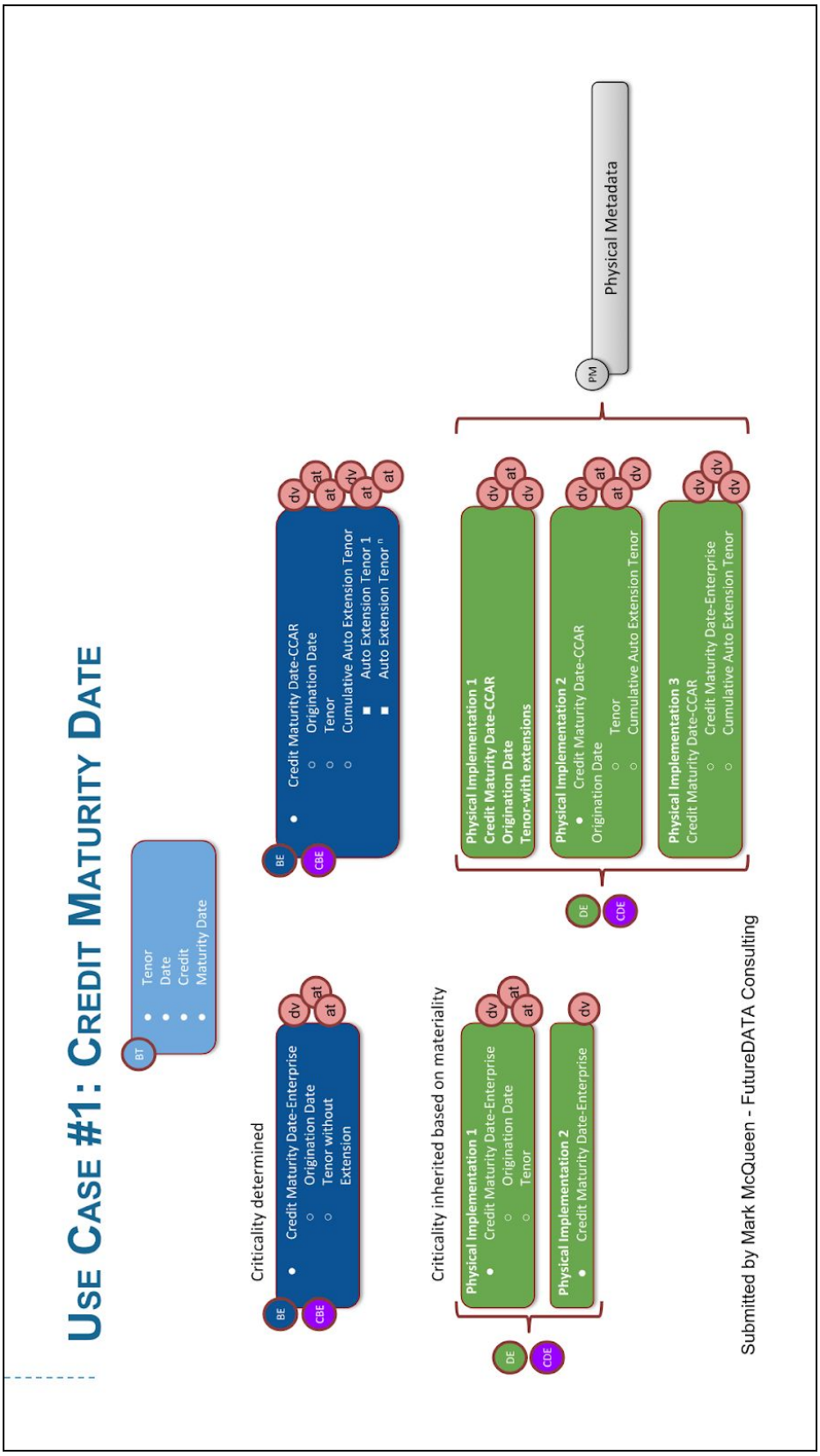
The source of these term names and definitions is the EDM Council Data Management Business Glossary[8].

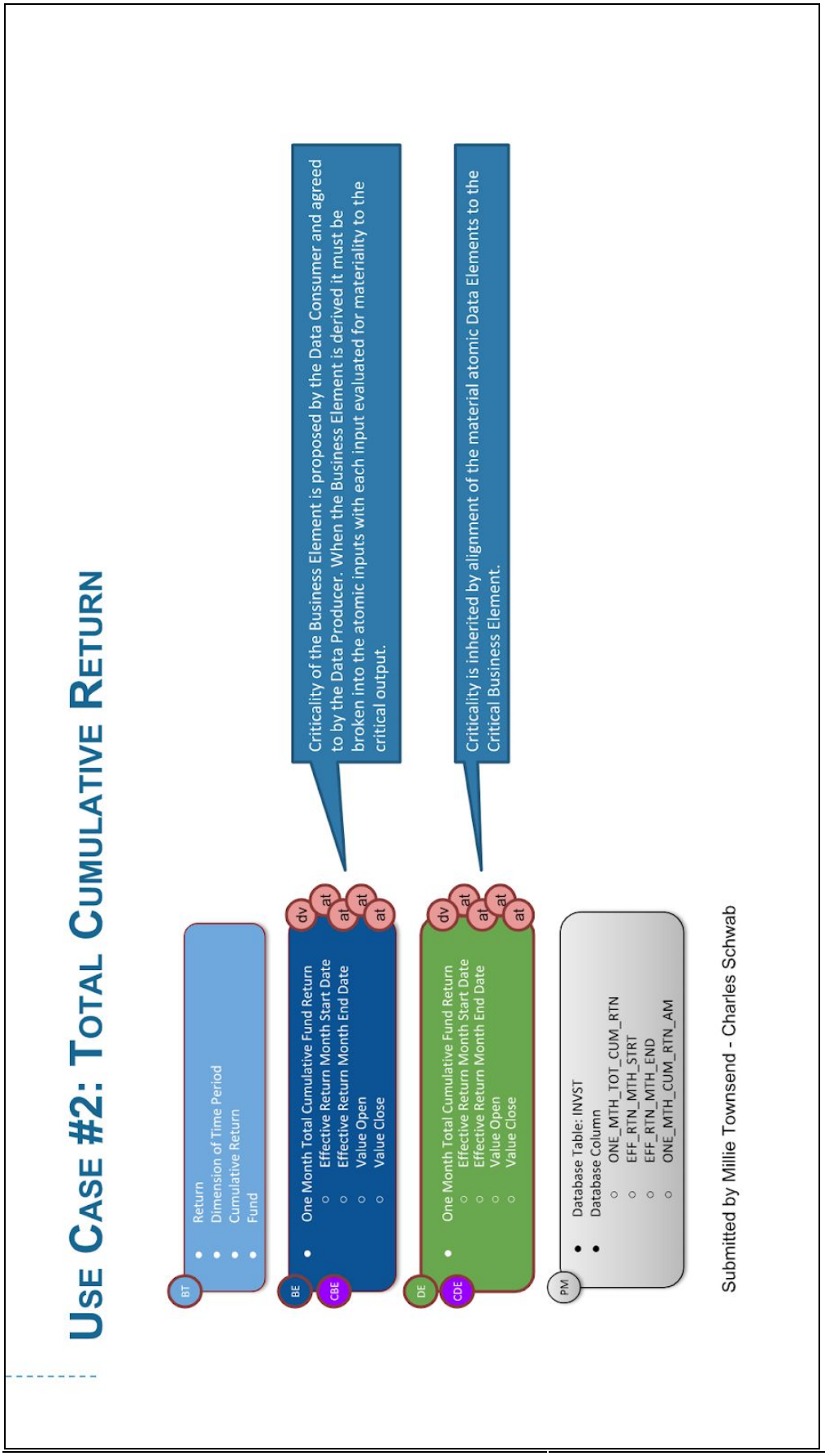
Term	Definition
Atomic	The lowest level of detail, factual meaning. (e.g. Interest Rate)
Authoritative Provisioning Point	A Provisioning Point that has been designated by the relevant data management governing body as providing data from an Authoritative Data Domain.
Business Element	A unit of information that has a specific meaning in the context of a business process or collection of processes within a domain.
Business Glossary	A collection of term names and definitions from the perspective of the business process.
Business Metadata	Provides context about the data from the perspective of the business process.
Business Term	The name(s) and meaning of common business language.
Critical Business Element	A Business Element that is deemed materially important to one or more business processes.
Critical Data Element	A Data Element that is aligned with a Critical Business Element and is deemed materially important.
Data Architect	The function that defines and implements the data content strategy for a given subset of data.
Data Consumer	A process, application or stakeholder that receives or uses data from a Data Producer.
Data Domain	A logical representation of a category of data that has been designated and named.
Data Element	A unit of data that is considered in context to be indivisible. [ISO 2382-4:1999]
Data Flow	A flow of data from one point to another, without involving any intermediaries at a specific level of granularity; to transport data.
Data Lineage	Documentation of the sequence of movement and/or transformation of data as it flows between the consumer and the source(s).
Data Producer	A process, application or stakeholder that provisions data to one or more Data Consumers
Data Sharing Agreement (DSA)	An agreement that sets out a common set of rules to be adopted by the various organizations involved in a data sharing operation.
Data Traceability	The ability to track a data construct back to the construct it was derived from as a more concrete instantiation.
Derived Data	Data that are created from other data or calculated.
Determined	Data elements that are subjective thereby including an element of opinion or human interpretation. (Subjective e.g.. Gold Customer - alias: Interpreted)
Financial Industry Business Ontology (FIBO)	An open standards business conceptual model developed by EDM Council members for how all financial instruments, business entities, and processes work in the financial industry.

8 https://edmcouncil.org/global_engine/download.aspx?fileid=8539E913-09A5-44EB-92E3-B6AC995F88F7&ext=pdf

Materiality	The degree to which the use of a data element in the business process could result in a substantive impact to the financial, operational or reputational position of the organization.
Physical Metadata	Metadata that describes the physical location of data.
Service Level Agreement (SLA)	An agreement between a service provider and a service consumer, minimally covering quality, availability, responsibilities.
System of Record	The Authoritative Data Source for the specified Data Element after it has been remediated and validated.
Technical Metadata	Used to describe the creation, organization, movement, change, and storage of the data from the perspective of the physical implementation.

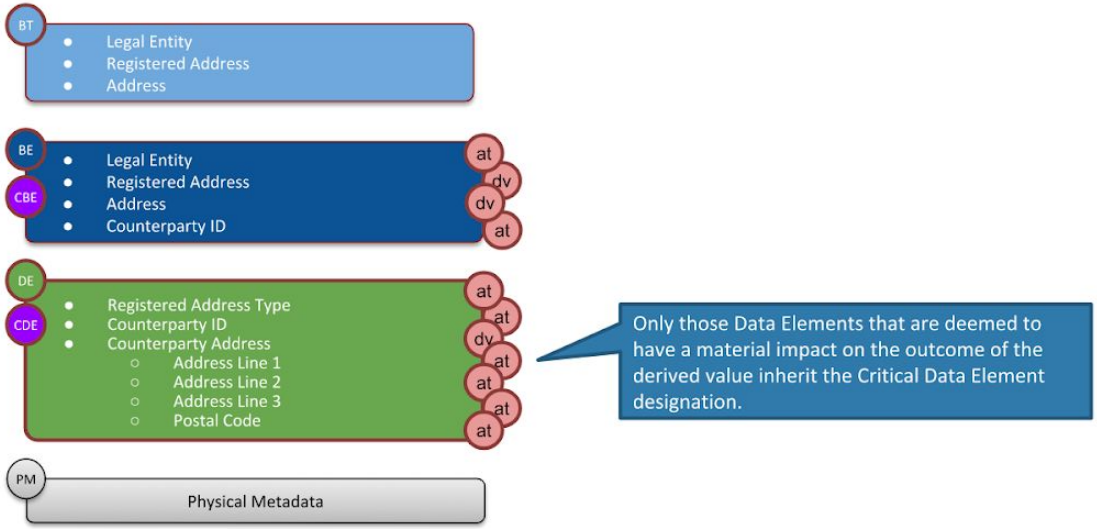
Business Element / Data Element Use Case Validation





USE CASE #3: REGISTERED ADDRESS

The business has identified the "Registered Address" of a legal entity as being critical. The business requirement is that "all counterparties must have a valid registered address".



Submitted by Kathryn Klaentschi - Deutsche Bank

USE CASE #4: RISK FX VEGA (1/3)

FX Vega – (FR Y-14Q: F.5 FX Vega - FR_Y-14Q_Trading_template.pdf : page 7)
FX Vega by Tenor values are what financial institutions often use as an internal Risk Metric, and regulators also request this dataset in regulatory submissions.
Vega - The expected change in the value of an option when the option's implied volatility increases by 1%, i.e. goes from 25% to 26%. When not specified otherwise, vega denotes lognormal vega as opposed to normal vega.
Thresholds: Enter all currency pairs for which the absolute value of the vega at any tenor (or in total) exceeds $1 mm / +1 vol point; pairs with smaller vegas may be omitted.
Tenors: In the term structure section, replace the tenor points shown in green with those the firm has available. Insert additional term structure columns as needed. Unused columns should be left blank
MDRM **CTRDH065** – FX VEGA: CURRENCY 1
MDRM **CTRDH063** – FX VEGA: CURRENCY 2
MDRM **CTRDH064** – FX VEGA: MATURITY
Note more complex examples exist, this is just illustrative.

Trading, PE & Other Fair Value Assets Schedule
FX Vega

Firm Name

Effective Date:
Submission Date:

FX Lognormal Vega ($K / +1 vol pt)

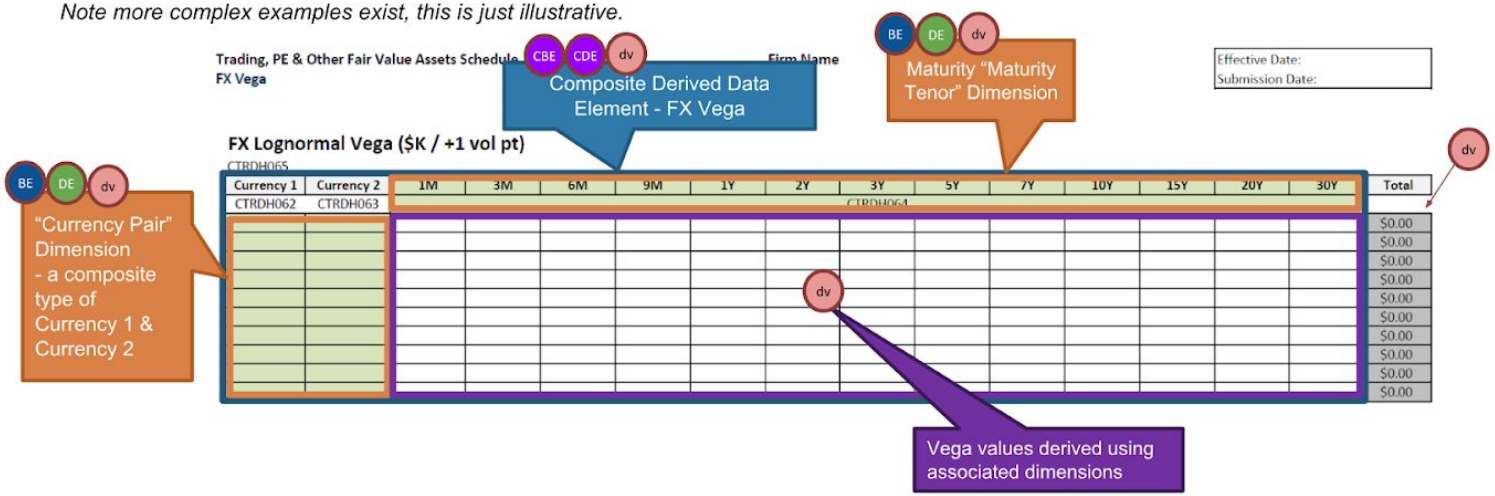
CTRDH065

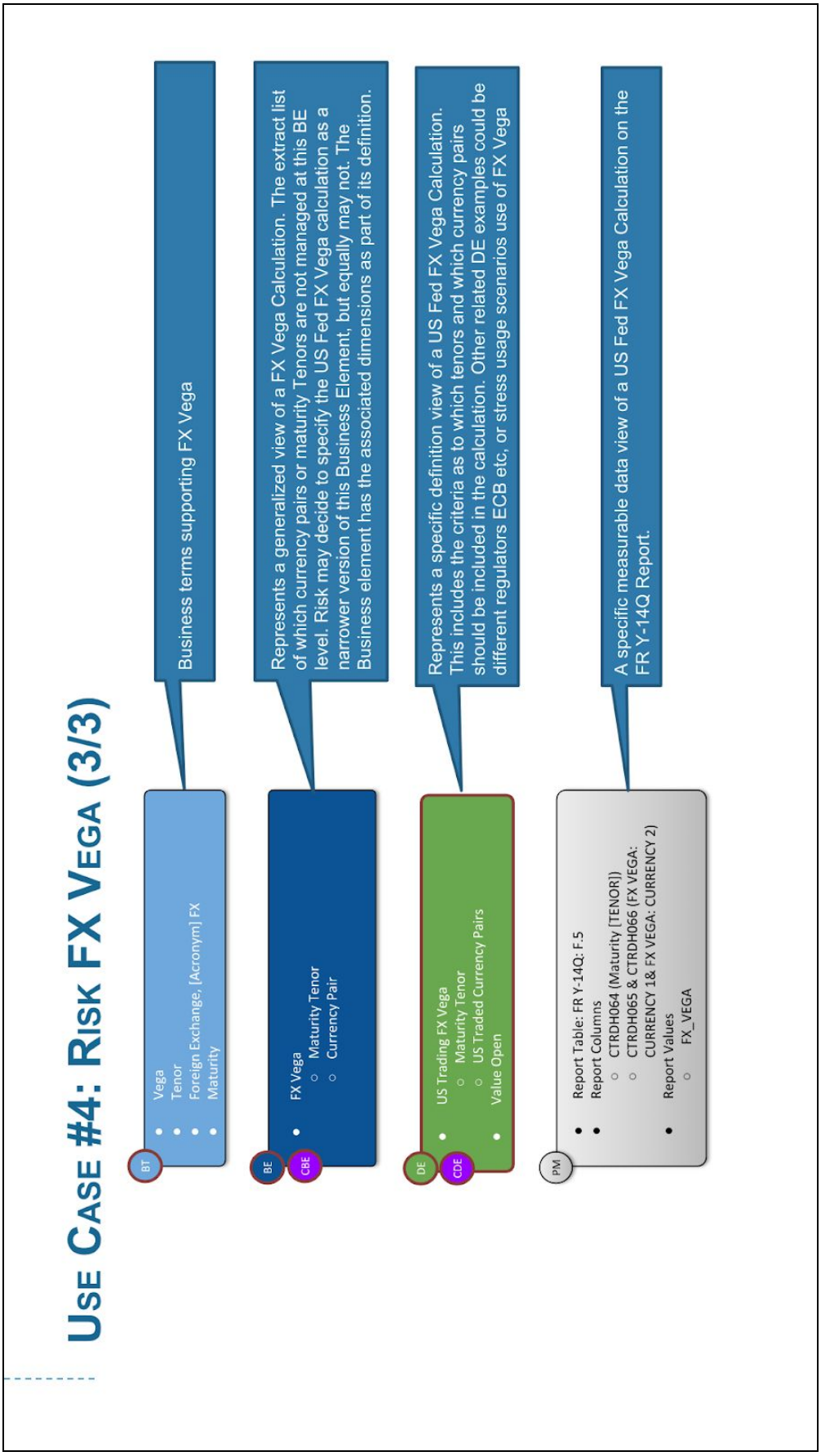
Currency 1	Currency 2	1M	3M	6M	9M	1Y	2Y	3Y	5Y	7Y	10Y	15Y	20Y	30Y	Total
CTRDH062	CTRDH063	CTRDH064													
															$0.00
															$0.00
															$0.00
															$0.00
															$0.00
															$0.00
															$0.00
															$0.00
															$0.00
															$0.00

Submitted by Gareth Isaac - Ortecha

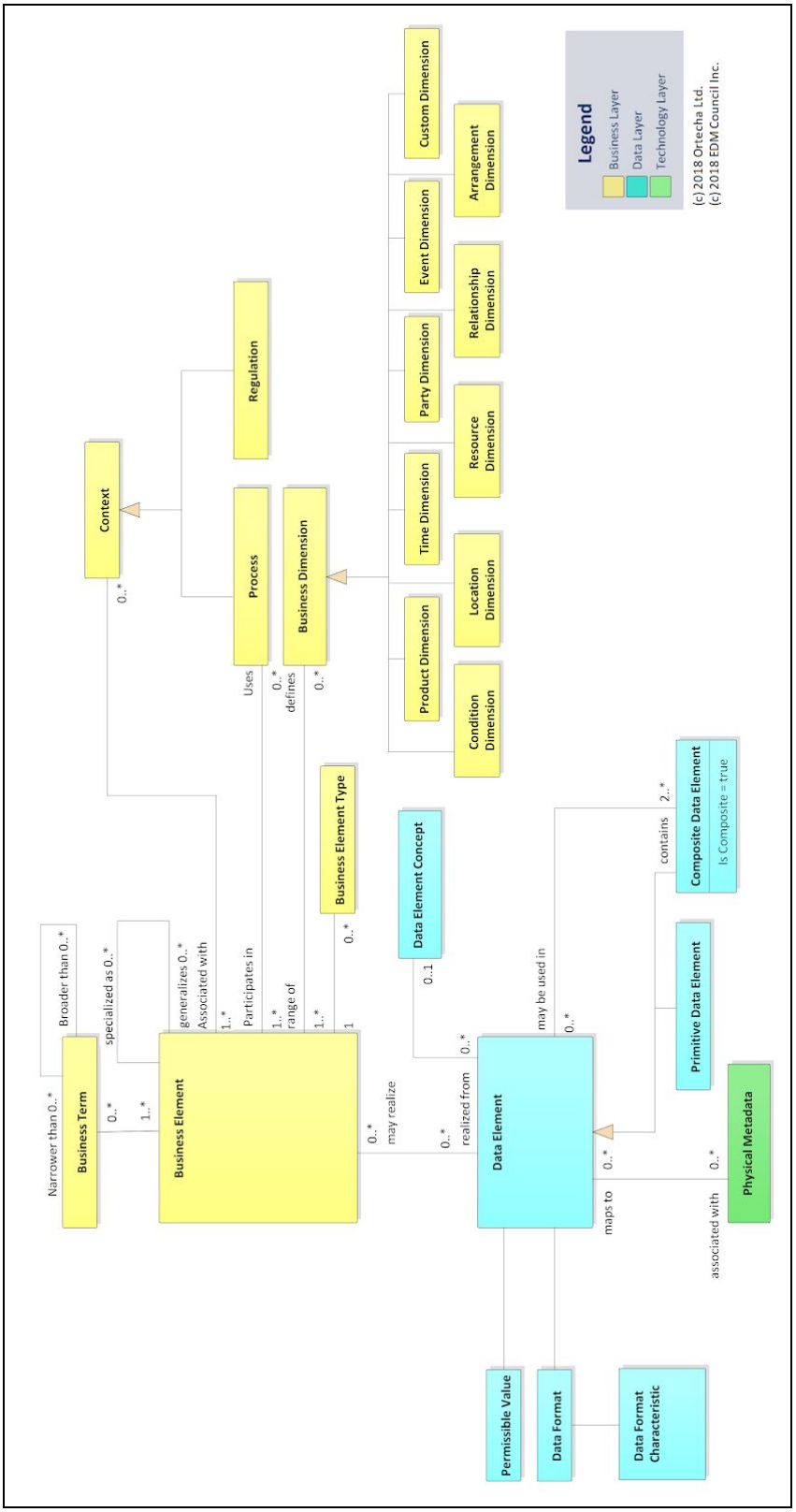
USE CASE #4: RISK FX VEGA (2/3)

Vega - The expected change in the value of an option when the option's implied volatility increases by 1%, i.e. goes from 25% to 26%. When not specified otherwise, vega denotes lognormal vega as opposed to normal vega.
Thresholds: Enter all currency pairs for which the absolute value of the vega at any tenor (or in total) exceeds $1 mm / +1 vol point; pairs with smaller vegas may be omitted.
Tenors: In the term structure section, replace the tenor points shown in green with those the firm has available. Insert additional term structure columns as needed. Unused columns should be left blank
MDRM **CTRDH065** – FX VEGA: CURRENCY 1
MDRM **CTRDH063** – FX VEGA: CURRENCY 2 (BE)
MDRM **CTRDH064** – FX VEGA: MATURITY
Note more complex examples exist, this is just illustrative.





Alignment to Data Architecture & Modeling Analysis



Epilogue

About the EDM Council & Best Practice Program

The EDM Council is a global organization, with member organizations from the US, Canada, UK, Europe, South Africa, Japan, Asia, Singapore, and Australia. Over 200 organizations and 7,000 data management professionals are members of the EDM Council.

The EDM Council provides a venue for data professionals to interact, communicate, and collaborate on the challenges and advances in data management as a critical organizational function. The Council provides research, education and exposure to how data, as an asset, is being curated today, and a vision of how it must be managed in the future.

EDM Council members work collaboratively to define and publish best practices for effective Data Management. All Best Practice work is grounded in the ***WHAT*** - essential principles found in the Data Management Capabilities Assessment Model (DCAM™). The Best Practice Program objective is to develop the ***HOW*** - documenting the experiences of data management practitioners to support the development and refinement of standard Data Management processes and tools across the full range of capabilities.

The Council also conducts a biennial benchmarking study as a baseline for evaluating progress, publishes a glossary of data management concepts to support stakeholder communication and engages with global regulators to promote more effective public/private partnerships.

About the Critical Data Element (CDE) Work Group

One of the most significant regulatory directives since the 2008 financial crisis has been the introduction of the “Principles for Effective Risk Data Aggregation and Risk Reporting” or BCBS 239. The Principles outlined in this directive require banks to establish sound information infrastructures to support their risk and risk reporting functions. As part of creating the required control environment, a common practice in the financial services industry is the establishment of CDEs or “critical data elements”.

In the 2017 Industry Benchmark Study, the management of CDEs was identified as a top challenge universally across the industry. Members report that there is uncertainty regarding the exact definition of a CDE, how is it designated, or how should it be used to satisfy the control requirement.

In August of 2017, the Council held a CDE webinar briefing for all members to propose a work effort to develop a best practice recommendation for identifying and managing CDEs. The forum was an open invitation for representatives from member organizations to join a Work Group. The Work Group was then formed and today contains approximately 60 members representing all aspects of the industry (GSIBs, SIFIs, buy side, sell side, geographic, consultants, vendors). See Epilogue: Work Group Members for a complete list of participating members.

The project objective was to create an agreed upon understanding of the purpose and definition of a CDE. Then, based on that purpose and definition develop a best practice process, procedures, and tools for the identification of CDEs and for managing the implications of criticality. The execution of the process, procedures and tools will be aligned with the DCAM Framework and the Data Management capabilities it defines. The output of this effort will be shared with banks and regulatory bodies alike.

The project was structured into three phases;

1. Define the "things" in the neighborhood of a CDE in order to understand the purpose and definition of a CDE.
2. Design the process and tools for identifying criticality.
3. Establish the implications of criticality and how to manage the implications across the critical set of data.

About the Authors

Mark McQueen is the Senior Advisor, Best Practice and Process Management for the EDM Council. He joined the Council in 2016 and now leads the Best Practice Program to develop Data Management industry standard processes for executing the DCAM™ Framework. Mark has over 20 years with a Fortune 25 GSIB where he was the business Data Management Executive for the Wholesale Bank. In addition to Best Practice Program facilitation, he provides training and EDMC Advisory Services related to adoption and execution of the DCAM™ Framework in member organizations.

Mark is DCAM™ Framework accredited, Six Sigma Black Belt Certified, and Strategic Foresight accredited - University of Houston.

Mark is Founder and Principal Consultant of FutureDATA Consulting.

mmcqueen@edmcouncil.org
+1 615.308.6465

Gareth Isaac is a Principal Consultant in Ortecha. He is a professional Data practitioner who works with stakeholders - both leadership and subject matter experts – to understand the complex challenges involved with improving processes and data throughout the end to end information lifecycle. Gareth has worked with multiple GSIBs over the years to help improve their data management practices, specializing in data lineage, control frameworks and governance functions.

gareth.isaac@ortecha.com
+44 20 3239 3823

Work Group Members

Arzaga, Raymund	Scotiabank
Atkin, Mike	EDMC
Bala, Sathya	Deutsche Bank
Bersie, Bret*	US Bank
Bland, Karen*	Moody's Corporation
Brophy, Doris	Societe Generale
Deligiannis, Greg	S&P Global Ratings
Dewsbury, Jeff	DTCC
Dimitrion, Genevey	State Street
Doyle, Martin*	DQ Global
Farenci, Susan	MUFG Union Bank
Finnen, Michael	Mitsubishi UFJ Financial Group
Fruhstuck, Mary	BNY Mellon | Pershing
Giardin, Christopher	IBM Hybrid Cloud
Gordon, Andrew	Deutsche Bank
Hawkins, Matthew*	Goldman Sachs
Isaac, Gareth*	Ortecha
Jeffries, Denise	
Keslick, Rob	BMO
Klaentschi, Kathryn	
Lawson, Andrew	Brickendon
Liu, Irene	PWC
McAdams, Curtis	
McQueen, Mark*	EDMC / FutureDATA
Nham, Annie	Macquarie Group Limited
Pandya, Hiten*	HSBC Bank
Robeen, Erica	Mastercard
Rolles, Daniel	EXL Service Holdings , Inc.
Roper, Michael	
Sondhi, Alok	DTCC
Tang, Alec	ADIA
Townsend, Millie	Charles Schwab
Zlat, Olga	Vanguard

* Data Architecture Subgroup Member