



هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission



Data Governance Maturity Guideline

for Telecommunication and
Information Technology Sector

Version 3

Table of Contents

Introduction	3
Framework Structure	5
Governance Domains	9
GD.3-1 Data Aspiration	9
GD.3-2 Technology and Data Architecture	12
GD.3-3 Data Operating Model	14
GD.3-4 Culture and Risk	18
Glossary	21
Appendix	22

Introduction

Based on the Communications and Information Technology Act issued by Royal Decree No. (M/106) dated 02/11/1443 AH, and its Bylaw, and based on the regulatory tasks assigned to CST under its Ordinance, CST prepared this document titled “Data Governance Maturity Guideline for Service Providers Regulated by CST”.

This framework is a self-assessment framework for service providers regulated by CST in order for them to improve their data governance practices and digital capabilities, as well as increasing their data protection standards and reducing data related risks. This framework contains a maturity assessment model which consists of nineteen subdomains, each with multiple levels of maturity defined and best practices explained for each sub-domain.

This framework is limited to the data governance and management topics such as data storage, data classification, data strategy, data security, data infrastructure, etc. which are enablers to the effective usage of data in an organization, often managed by either the Chief Data Officer’s (or equivalent) team and it does not aim to provide any guidance outside of this defined scope.

1-1 Purpose of this Framework

This Framework is a non-binding self-assessment framework for services providers in sectors regulated by CST to assess their data governance maturity based on 19 identified data governance sub-domains ranging from data management vision and strategy to data ethics. It is meant to provide guidance to service providers by:

providing examples of best-in-class approaches to data governance sub-domains, calculating a data governance maturity score to gain an overall perspective, identifying data governance sub-domains for improvement.

1-2 Review, Updates and Maintenance

CST shall update this framework in the future when changes are deemed necessary either due to changing regulatory environments, adapting to changes in technologies, or changes in best practices.

1-3 How to use this Framework

This framework shall be used by service providers to self-assess the data governance maturity along 19 sub-domains. The service provider may assign a team of professionals with relevant experience in either data governance, data management, or other related functions to oversee the implementation of this assessment by following the following steps:

Comprehend the Framework by carefully reading this document to understand the various data governance sub-domains and the maturity levels for each of them, understanding the purpose of this exercise and how it will lead to benefits for the organization.

Understand Requirements through interviews with senior leadership, department heads, IT specialists, etc. as well as conducting technical reviews of relevant data systems to assess level of maturity for each sub-domain.

Determine Maturity level by using the templates provided in the appendix by filling in the maturity level for each sub-domain for each domain then multiplying with the modifier to calculate the maturity score for each domain and then use the domain scores to calculate the final overall maturity score.

Communicate Results of the self-assessment to senior leadership in the form of a report highlighting current strengths and opportunities for improvement along the different sub-domains with specific actions and recommendations based on the interviews conducted as well as the best practices given in the document.

Capture Value from the assessment by implementing the actions and recommendations communicated in the report in step 4. After implementing these actions, it is recommended to conduct the self-assessment again on a regular basis using the latest version of this Data Governance Maturity Framework.

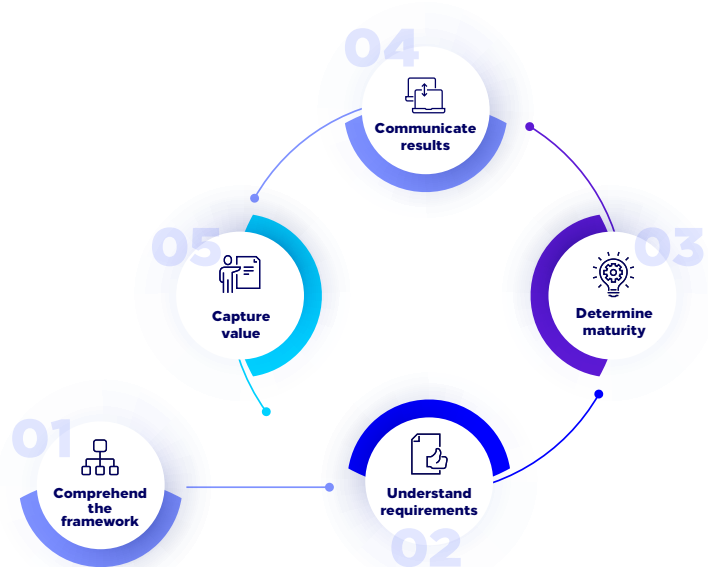


Figure 1: How to use this framework in four steps

Framework Structure

2-1 Data Governance Maturity Model

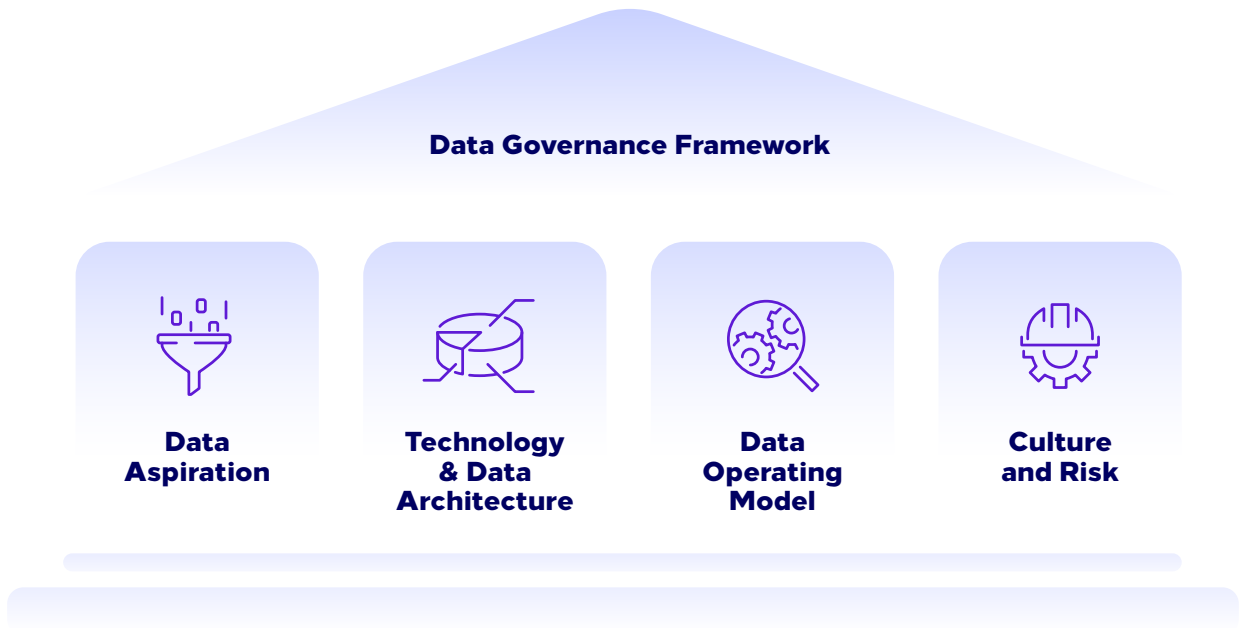
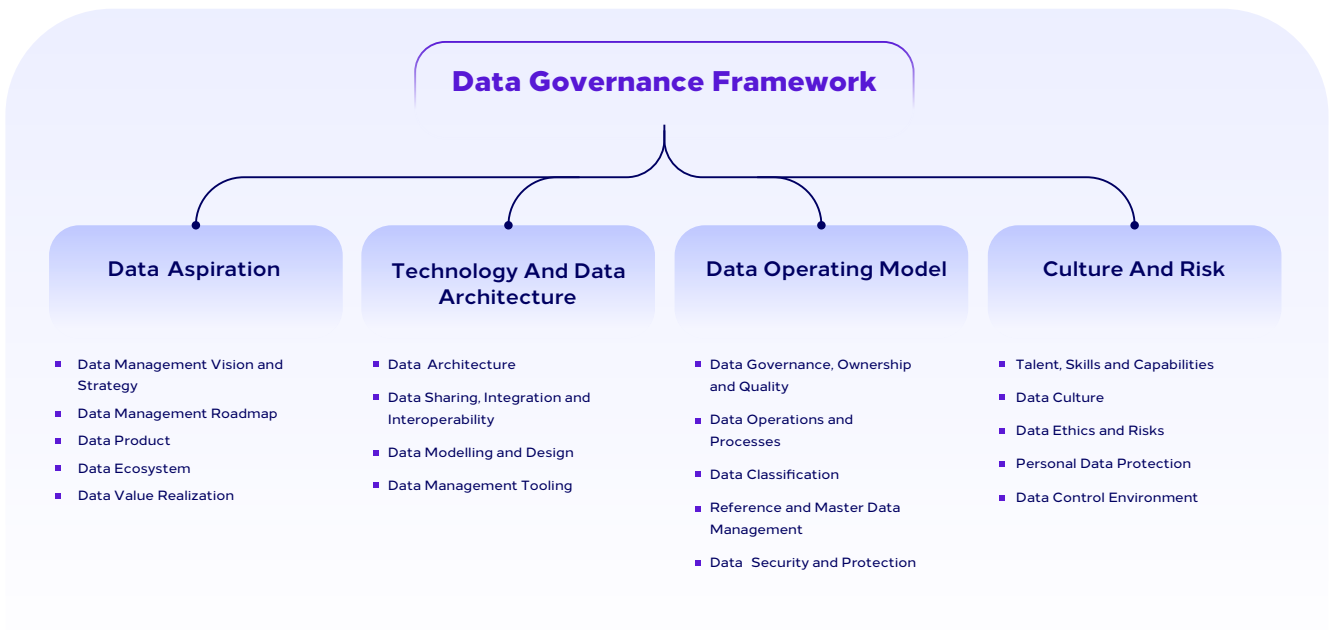


Figure 2: Data Governance Framework

The Data Governance Maturity Framework with its four domains - Data Aspiration, Technology and Data Architecture, Data Operating Model and Culture and Risk - forms the basis for all service providers to assess their data governance maturity.



The Data Aspiration domain contains five sub-domains, the Technology and Data Architecture domain has four sub-domains, Data Operating Model is split into five sub-domains and Culture and Risk has five sub-domains.

The data governance maturity model has five maturity levels from 1 to 5 for each sub-domain under each domain detailed in the next section. In order to achieve a higher maturity level, the service provider must first meet the requirements of all preceding levels.

Broadly, any service provider can interpret the maturity levels for each sub-domain as given below.



Data Governance Maturity Levels

Maturity Level	Value for Calculation	Description
Nascent	1	Service provider has not taken any action yet for this sub-domain and can be considered to be nascent; it may or may not plan to take action for this sub-domain at the moment
Experimenting	2	Service provider has taken a few actions for this sub-domain but it is not considered a fundamental part of the service provider's business strategy; benefits from the actions taken have not been realized at this point
Maturing	3	Service provider has taken several actions for this sub-domain and is slowly becoming a fundamental part of the service provider's business strategy; benefits from actions taken may or may not have been realized and the service provider is planning to scale up these actions
Mature	4	Service provider is implementing best practices for this sub-domain and it is a fundamental part of the business strategy; these best practices have led to benefits at scale and has led to an overall improvement in the service provider's abilities
Leader	5	Service provider is using best practices and is innovating in this sub-domain to be ahead of its peers; the service provider may be testing new technologies, processes, approaches and is generally considered as the benchmark for best-in-class in this particular sub-domain in its sector. Overall, the service provider follows an integrated and consistent approach across the whole organisation.

Table 1: Data governance maturity levels

2-2 Structure

The key shown below explains how to interpret the tables that contains information provided each sub-domain and domain in the next section.

2-3 Governance Domain Structure

Option #1

Domain Code	GD.X	Governance Domain	XX
Domain Description	XXXX		
Sub-Domain Code	Sub-Domain		
GD.X.1	XXXX		
GD.X.2	XXXX		
GD.X.3	XXXX		
...	...		

Table 2: Template for data governance domain cards

Key	Element	Description
1	Domain Code	The numbering format for the domain is GD.X where GD stands for 'Governance Domain' e.g., the first domain will be labelled GD.1
2	Governance Domain	Title of the Governance Domain
3	Domain Description	Short introduction to the Governance Domain including an explanation as to why it is necessary for service providers to look at this domain
4	Sub-Domain Code	The numbering format for the sub-domain is GD.X.X where the first number indicates the domain number the second number indicates the sub-domain number e.g., the second sub-domain for first domain will be labelled GD.1.2
5	Sub-Domain	Title of Governance Sub-domain

Table 3: Legend for data governance domain card template

3-3 Sub-Domain Structure

GD.X	Governance Domain	XXXX	Version
GD.X.X	Sub-Domain	XXXX	
Sub-Domain Description	XXXX		
Sub-Domain Best-in-class Practices	XXXX		
Maturity Level	Maturity Level Description		
1	XXXX		
2	XXXX		
3	XXXX		
...	...		

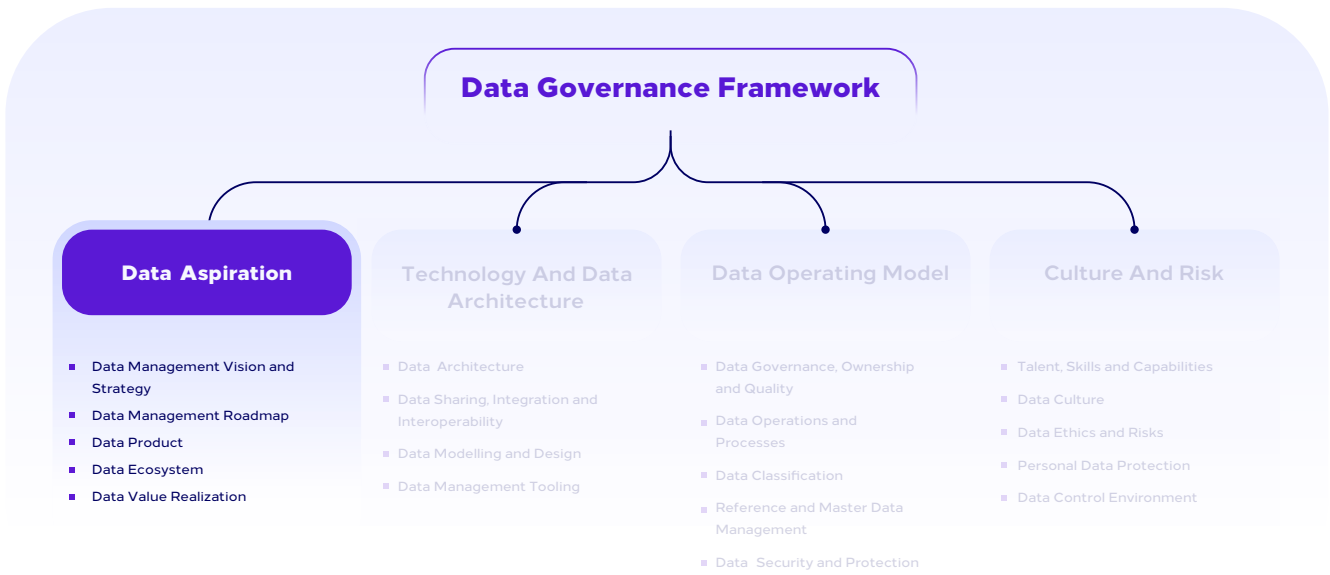
Table 4: Template for data governance sub-domain cards

Key	Element	Description
1	Domain Code	The numbering format for the domain is GD.X where GD stands for 'Governance Domain' e.g., the first domain will be labelled GD.1
2	Governance Domain	Title of the Governance Domain
3	Sub-Domain Code	The numbering format for the sub-domain is GD.X.X where the first number indicates the domain number the second number indicates the sub-domain number e.g., the second sub-domain for the first domain will be labelled GD.1.2
4	Sub-Domain	Title of Governance Sub-domain
5	Version	Current version of the sub-domain and maturity level definitions
6	Sub-Domain Description	Short introduction to the Governance Sub-domain
	Sub-Domain Best-in-class Practices	Explanation of the best practices that service providers can follow
7	Maturity Level	Maturity levels ranging from level 1 to 5
8	Maturity Level Description	Description of the maturity level for the sub-domain including activities being conducted by the service provider in order to be classified as having obtained that particular level of opportunity

Table 5: Legend for data governance sub-domain card template

Governance Domains

GD.3-1 Data Aspiration



Domain Code	GD.3-1	Governance Domain	Data Aspiration
Governance Domain Description	<p>Service providers that intend to use data in their operations and business strategy should define a cohesive, organization-wide approach to data governance and management in order to successfully realize the benefits from the time and effort spent in developing the data architecture, operating model, culture and governance capabilities traditionally associated with a data-mature organization.</p> <p>This domain covers the strategic activities that shape the overall data governance and management strategy of the service provider, including the business model of potential services, products and alliances that a service provider might build as well as actions it can take to ensure effective implementation of its strategies.</p>		
Sub-Domain Code	Sub-Domain		
GD.3-1-1	Data Management Vision and Strategy		
GD.3-1-2	Data Management Roadmap		
GD.3-1-3	Data Product		
GD.3-1-4	Data Ecosystem		
GD.3-1-5	Data Value Realization		

3-1-1 Data Management Vision and Strategy

GD.3-1	Governance Domain	Data Aspiration	Version	1
GD.3-1-1	Sub-Domain	Data Management Vision and Strategy		
Sub-Domain Description	<p>Service providers should operationalize their data aspirations by having a data governance and management strategy in place which would require establishing internal initiatives such as identifying use cases, monitoring data usage, establishing data governance standards, implementing necessary data infrastructure etc.</p>			
Sub-Domain Best-in-class Practices	<p>Having a well-defined data governance and management strategy with identified initiatives tied to business goals and planned benefits, designated initiative owners and a robust mechanism to review the benefits, and plan new initiatives when necessary, with the ultimate goal to integrate the results from this strategy into the service provider's operations and realize benefits from it.</p>			
Maturity Level	Maturity Level Description			
1	<p>Service provider does not have a clearly defined data management vision and strategy, hence has not started implementing a data governance and management vision and strategy and may not have a plan in place to implement such a vision/ strategy</p>			
2	<p>Service provider has started implementing a few scattered initiatives which benefit the overall business strategy of the organization but does not have a complete and clear data governance and management vision and strategy in place; these activities could include hiring data scientists, onboarding data vendors, etc.</p>			

3	Service provider is implementing a set of initiatives which are part of the data governance and management vision and strategy such as defining policies, standards, delegating responsibilities, etc. but has not yet experienced the benefits from it
4	Service provider is implementing a significant set of initiatives as part of a wider data management vision and strategy and outcomes from these initiatives are resulting in some early benefits that are helping the service provider to improve its data-related goals
5	Service provider has delivered a significant batch of initiatives as part of a defined and incorporated data management vision and strategy, reviews initiative impacts and iteratively implements new initiatives when required by the broader data aspirations of the organization

3-1-2 Data Management Roadmap

GD.3-1	Governance Domain	Data Aspiration	Version	1
GD.3-1-2	Sub-Domain	Data Management Roadmap		
Sub-Domain Description	A data management roadmap is the mechanism for operationalizing the data management and governance strategy in an enterprise which includes activities such as alignment of stakeholders, proper internal communications, education programs, engagement models, regular checks and operational routines that are established to implement the service provider's data management strategy.			
Sub-Domain Best-in-class Practices	Having a well-defined multi-year roadmap for the rollout of initiatives with a robust dashboard that tracks KPIs regarding the implementation of these initiatives, clear and effective communication of the data governance and management strategy to leadership as well as employees, identifying potential risks and preparing mitigation techniques to ensure the success of the data governance and management program.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a data governance and management strategy in place and hence does not have a roadmap for its operationalization, any data-related initiatives are owned by a comparably small teams with limited cross-division visibility or coherent strategy			
2	Service provider has a high-level roadmap for its data governance and management in place which is aligned with senior stakeholders and there are only a couple of high-level KPIs in place to track progress on the operationalization of the strategy			
3	Service provider has a well-defined roadmap but does not incorporate all the planned data initiatives that may be in place or planned at the division-level also the company has a few KPIs to track progress on a project-by-project basis and the strategy has been communicated to senior and mid-level stakeholders who are responsible for the implementation of some of these initiatives			
4	Service provider has a well-defined roadmap that encompasses the planned data initiatives in most divisions as well as extensive KPIs to measure progress on their operationalization, clear communication to initiative stakeholders of all seniority levels			
5	Service provider has a well-defined roadmap that encompasses the planned data initiatives in all divisions as well as extensive KPIs to measure progress on their operationalization, clear internal communications with feedback from stakeholders to fine-tune the roadmap, and has prepared mechanisms that would mitigate any identified risks to the operationalization of the strategy			

3-1-3 Data Product

GD.3-1	Governance Domain	Data Aspiration	Version	1
GD.3-1-3	Sub-Domain	Data Product		
Sub-Domain Description	Data products refer to data-related offerings that can be useful as a service or product provided to either internal or external customers. These products consist of usually autonomous, self-sufficient and well-labelled datasets that can be useful for a specific purpose and may be purpose built to solve a specific problem for customers.			
Sub-Domain Best-in-class Practices	Having a well-defined value proposition and strategy around the creation of data products with a dedicated team of data specialists, such as data engineers, analysts, or stewards, steered by data owners responsible for conducting monitoring and technical follow-up of the data lifecycle, maintaining dashboards and other tools to ensure the successful deployment of data products to internal and external stakeholders.			
Maturity Level	Maturity Level Description			
1	Service provider is not aware of data products or has not implemented it			
2	Service provider has started exploring the creation of data products but does not have a specific launch plan; internal testing and development of data products may be in place but without dedicated owners			
3	Service provider is in the process of developing data products that have a launch date planned within the next year with identified owners responsible for the deployment and development			
4	Service provider has deployed several data products with clear ownership roles but is not tracking individual profit and loss and does not have a strategic roadmap for the enhancement of current and development of new data products			
5	Service provider has deployed several data products with a well-defined value proposition, monitors their profit and loss, has defined ownership roles for each data product, and has a strategic roadmap for the enhancement of current data products and development of future data products			

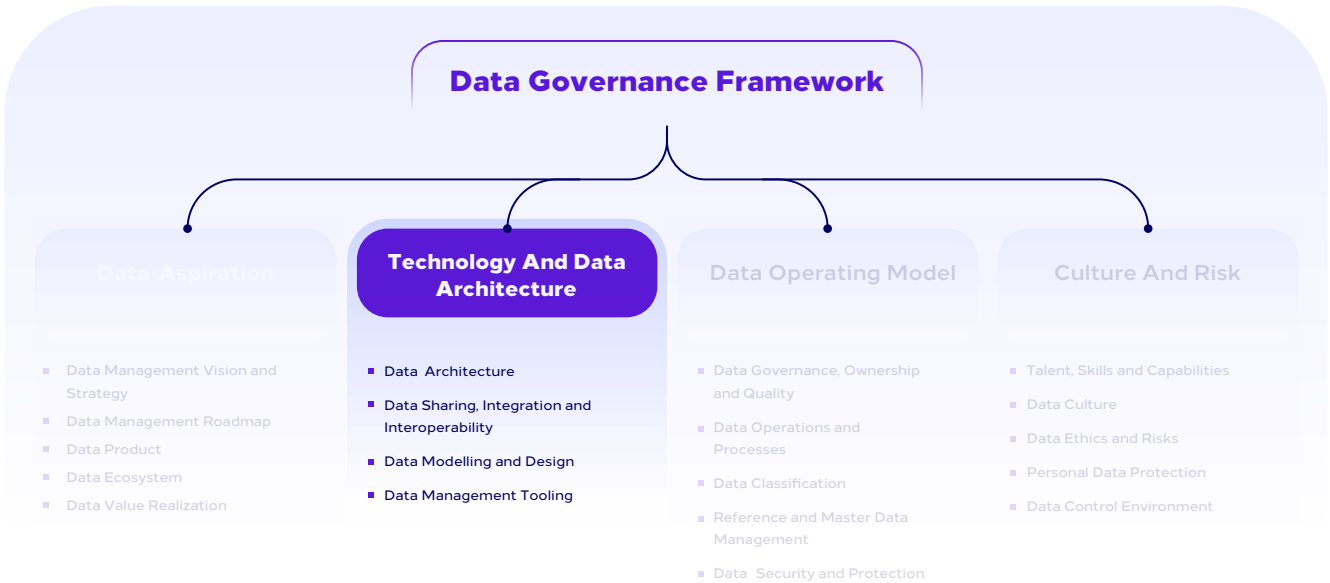
3-1-4 Data Ecosystem

GD.3-1	Governance Domain	Data Aspiration	Version	1
GD.3-1-4	Sub-Domain	Data Ecosystem		
Sub-Domain Description	Data ecosystems are platforms that combine data from numerous providers and build value for all entities who have access to the data on that platform. Data platforms allow organizations access to resources that traditionally they would not have been able to use, hence allowing them to create new data-enabled products and services. Often, associations of organizations as well as government authorities can help in the creation of these ecosystems.			
Sub-Domain Best-in-class Practices	Having strategic partnerships with multiple players, well-defined infrastructure for data sharing and common standards for data in place.			
Maturity Level	Maturity Level Description			
1	Service provider is not aware of data ecosystems and has not participated in one			
2	Service provider has started exploring options such as the creation of or participation in data ecosystems but without a definite plan in place			
3	Service provider is planning to either launch or join a data ecosystem in the next 12 months and is in the process of shortlisting its options			
4	Service provider has identified specific data ecosystems or stakeholder that it wants to build an ecosystem with and are currently in the course of joining it			
5	Service provider has already been leveraging data ecosystems in collaboration with other stakeholders and has realized the benefits from it, e.g., access to new data from another stakeholder has led to improvements in the service provider's existing products or services			

3-1 Data Value Realization

GD.3-1	Governance Domain	Data Aspiration	Version	1
GD.3-1-5	Sub-Domain	Data Value Realization		
Sub-Domain Description	Data value realization involves the continuous evaluation of data assets for potential data driven use cases that generate revenue or reduce operating costs for the service provider. By understanding the value of data, often by building hypothetical use cases and sizing the value of these use cases, service providers can effectively build business cases using data and identify the technical and organizational target state necessary to achieve desired outcomes.			
Sub-Domain Best-in-class Practices	Having a close collaboration between teams from the business and analytics departments in order to scope, build, deploy and maintain impactful data-enabled use cases, with identified profit and loss scenarios and a robust governance mechanism in place to intervene if use cases do not perform as expected according to critical KPIs.			
Maturity Level	Maturity Level Description			
1	Service provider does not see data as a value-generating asset and mostly uses it for reporting and operational purposes			
2	Service provider has started viewing data as a strategic asset and the first initiatives have been identified and owners assigned			
3	Service provider is implementing data-enabled use cases across business divisions with proper owners identified and their return on investments calculated			
4	Service provider has implemented several data-enabled use cases which are regularly tracked for their performance including profit, loss, malfunctions etc. and internal use cases now support several business decisions but manual intervention is often required			
5	Service provider has implemented several data-enabled use cases whose value generated is constantly tracked with proper governance in place if interventions are required and business decisions are now driven by mature and effective internal use cases that rarely require manual inputs			

GD.3-2 Technology and Data Architecture



Domain Code	GD.3-2	Governance Domain	Technology and Data Architecture
Governance Domain Description	<p>Service providers need to ensure that proper tools, technologies, systems and standards are in place in order to store, analyze and transform data to realize value from it. Investing in the right technologies means that service providers can manage their data more efficiently, build more accurate advanced analytics-enabled models, provide the latest tools to employees so they can work efficiently with data and make it easier to integrate with external resources with proper interoperability standards baked in.</p>		
Sub-Domain Code	Sub-Domain		
GD.3-2-1	Data Architecture		
GD.3-2-2	Data Sharing, Integration and Interoperability		
GD.3-2-3	Data Modelling and Design		
GD.3-2-4	Data Management Tooling		

3-2-1 Data Architecture

GD 3-2	Governance Domain	Technology and Data Architecture	Version	1
GD.3-2-1	Sub-Domain	Data Architecture		
Sub-Domain Description	<p>The Data Architecture of an organization or service provider describes how data is stored, managed and integrated with different systems through specific rules, systems and models to support the business strategy. A well-designed data architecture makes it easier for data users to build data pipelines, conduct transformations or identify data lineage for any data products or use cases they would like to build.</p>			
Sub-Domain Best-in-class Practices	<p>Having an end-to-end consistency, covering all layers of data transformation that most data owned by an enterprise would go through from its source to aggregation, cleaning, storage to the end user or products.</p>			
Maturity Level	Maturity Level Description			
1	Service provider has not yet defined a data architecture			
2	Service provider has defined a data architecture for certain processes or business units			
3	Service provider has defined a data architecture for almost all relevant processes but the architecture does not cover all layers of transformation (sourcing, storage, aggregation, manipulation, presentation, etc.) and does not provide a view on data flows and data lineage			
4	Service provider has defined a data architecture for all relevant processes but the architecture does not cover all layers of transformation (sourcing, storage, aggregation, manipulation, presentation etc.) and provides an incomplete view on data flows and data lineage			
5	Service provider has defined a data architecture for all relevant processes which covers all layers of transformation (sourcing, storage, aggregation, manipulation, presentation etc.) and provides detailed information on the data flows, data lineage and the service provider regularly assesses its data architecture for gaps and improvements			

3-2-2 Data Sharing, Integration and Interoperability

GD.3-2	Governance Domain	Technology and Data Architecture	Version	1
GD.3-2-2	Sub-Domain	Data Sharing, Integration and Interoperability		
Sub-Domain Description	This sub-domain covers the collection of data from different sources and consists of integration solutions fostering a harmonious internal and external communication between various IT components that allows flexible movement of data from one system to another to enable products and users to use multiple types of data within the same solution.			
Sub-Domain Best-in-class Practices	Having common data standards as well as technologies for interoperability within the organization/ service provider or externally, widespread use of Application Programming Interfaces (APIs) for easier transfer of data internally and externally, incorporating data sharing techniques in all systems that are part of the data flow, etc.			
Maturity Level	Maturity Level Description			
1	Service provider does not consider data sharing as an important aspect when developing solutions and data is often siloed off and not exposed to external systems or consumers			
2	Service provider has planned the adoption of relevant technologies and practices that enable data sharing but has not yet implemented it and has also identified the integration requirements necessary to integrate the IT components including cost, resources required, etc.			
3	Service provider has started implementing systems and standards internally for better data sharing and interoperability, documents ETL, data flow and transformation instructions to improve integration between future IT components			
4	Service provider often builds solutions that support data sharing and interoperability internally and only enables external integration in exceptional circumstances, does not participate in data sharing ecosystems or marketplaces, and regularly verifies the correctness of data flows between integrated IT components			
5	Service provider builds technical solutions that are designed to support integration of both internal and external systems by default, enabling seamless integration of external data sources such as open data, different APIs, proprietary systems, etc., and also participates in data ecosystems or marketplaces			

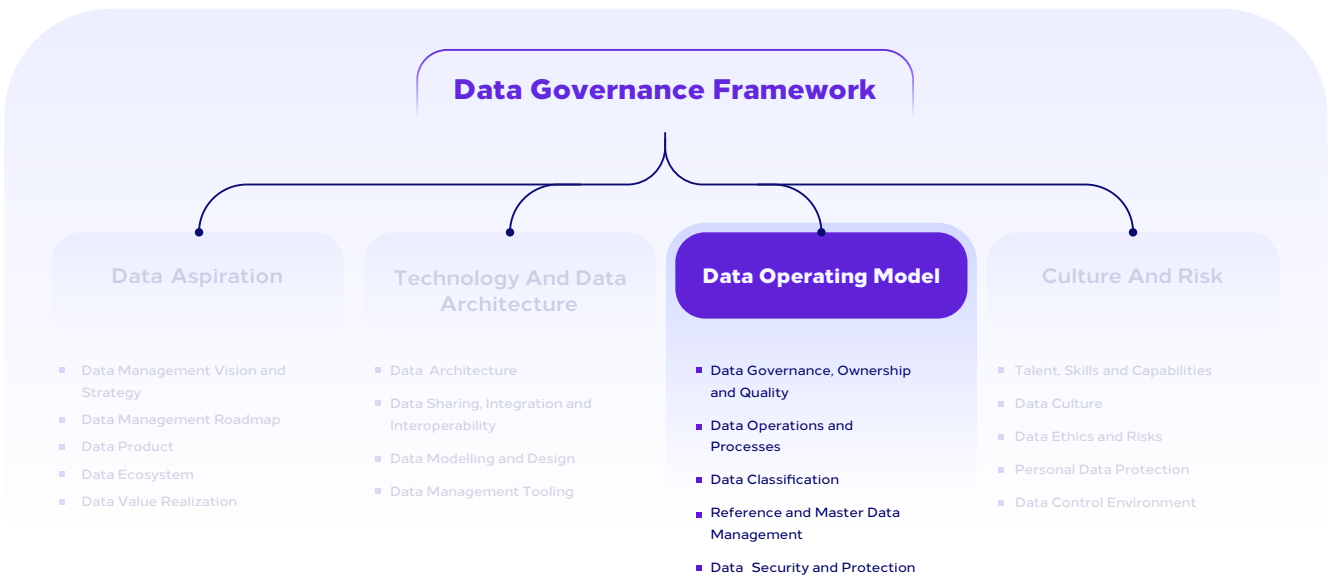
3-2-3 Data Modelling and Design

GD.3-2	Governance Domain	Technology and Data Architecture	Version	1
GD.3-2-3	Sub-Domain	Data Modelling and Design		
Sub-Domain Description	Data Modeling is the process of discovering, analyzing, representing, and communicating data requirements in a precise form so that it is easy for data users to quickly interpret data and start using it. Without data models, problems might arise such as conflicting standards and definitions, difficulty in locating data, lack of contextual awareness while using certain data, etc.			
Sub-Domain Best-in-class Practices	Having an Enterprise Data Model (EDM) in place with comprehensive data aggregation covering most types of data relevant to the service provider, ideally covering data at the conceptual, logical and physical levels. The EDM should also be regularly updated and flexible to accommodate new types of data.			
Maturity Level	Maturity Level Description			
1	Service provider does not aggregate their data and do not plan to aggregate their data to achieve a granular view			
2	Service provider is aggregating limited amounts of data albeit on a high level without a sufficiently granular view of the data			
3	Service provider is aggregating limited amounts of data and the model has a sufficiently granular view for most complex use cases			
4	Service provider has aggregated almost all relevant data, although the aggregation is not flexible and not to the required granularity for complex use cases			
5	Service provider has defined a clear source of truth for most data elements and has aggregated almost all relevant data in a flexible Enterprise Data Model which has sufficient granularity for nearly all use cases excluding a few exceptional use cases where off-the-shelf software would be required to make sure data is appropriately represented			

3-2-4 Data Management Tooling

GD.3-2	Governance Domain	Technology and Data Architecture	Version	1
GD.3-2-4	Sub-Domain	Data Management Tooling		
Sub-Domain Description	This sub-domain describes how effectively a service provider captures, stores, accesses, and uses data by leveraging data management tools such as database management tools, ERPs, data analytics and BI tools, data lineage tools, data catalogue tools, etc.			
Sub-Domain Best-in-class Practices	Identifying a technology stack that is easy to use, sufficiently covers all needs of data users, is interoperable and harmonious with existing systems.			
Maturity Level	Maturity Level Description			
1	Service provider does not have specialized data management tools or has a bare minimum that is only accessible by an IT department. No training is provided on using these tools.			
2	Service provider allows its IT department to enable users to access data management tools on ad-hoc basis as per their requirements which usually takes more than two to three days			
3	Service provider has a list of up-to-date data management tools that are validated for use by employees and users can gain access to them usually within the same day of submitting a request to the IT department			
4	Service provider allows users to access most of the latest data management tools seamlessly, e.g. registering via enterprise-supported single sign-on (SSO) barring certain tools which require special requests, and ensures that broad compatibility with a variety of systems is a prioritized characteristic in the choice of tools			
5	Service provider allows users to access most of the latest data management tools seamlessly, e.g. registering via enterprise-supported single sign-on (SSO) barring certain tools which require special requests, and also provides training and guides for new users. Data management tools usage policies and guidelines are aligned with service provider's business objectives and this alignment is regularly communicated to data users.			

GD.3-3 Data Operating Model



Domain Code	GD.3-3	Governance Domain	Data Operating Model
Governance Domain Description	<p>A data operating model is a critical element in the overall data management strategy of a service provider as it links the organizational practices to the data operations necessary to take advantage of data as an asset.</p> <p>An effective data operating model ensures that service providers would be able to take advantage of investments in data related technologies through senior stakeholder alignment, proper data management policies, governance and quality standards in order to make data easily usable by data and analytics teams to build value-generating data use cases.</p>		
Sub-Domain Code	Sub-Domain		
GD.3-3-1	Data Governance, Ownership and Quality		
GD.3-3-2	Data Operations and Processes		
GD.3-3-3	Data Classification		
GD.3-3-4	Reference and Master Data Management		
GD.3-3-5	Data Security and Protection		

3-3-1 Data Governance, Ownership and Quality

GD.3-3	Governance Domain	Data Operating Model	Version	1
GD.3-3-1	Sub-Domain	Data Governance, Ownership And Quality		
Sub-Domain Description	This sub-domain describes the controls over the planning and implementation of an service provider's data management practices by ensuring there is clear ownership of data domains and proper implementation of data standards and quality. Improvements in data governance, ownership, and quality will reduce time to value for any data use cases envisioned by data users at the service provider.			
Sub-Domain Best-in-class Practices	Having an effective dedicated data governance department led by a Chief Data Officer and well-defined data domains for most relevant data with clear ownership and regular assessments of data against reference data sources to ensure high data quality standards that reduce time to value for users of data.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a clear leadership structure for its data and analytics functions and has not established data governance and quality standards; hence data is most often not tagged to a particular data domain and is often of low quality with unclear ownership of data			
2	Service provider has a data governance team embedded with IT/Risk, has started establishing centralized data governance and quality standards, has mapped some data to a few domains with plans to map data to additional domains, and is conducting spot checks for data quality issues for some data			
3	Service provider has a Chief Data Officer responsible for coordinating data management activities across the organization, has an effective centralized data governance structure with clear ownership with some high-level data domains being very well-defined but inconsistently followed, and conducts regular data quality checks of complete datasets which have identified several errors			
4	Service provider has a Chief Data Officer empowered by a robust central governance organization which has identified several clearly defined data domains although adherence to these domains is not perfect and data quality is comprehensively assessed regularly on various dimensions (e.g., completeness, accuracy, timeliness, uniqueness, validity, etc.) and is usually found to be adequate			
5	Service provider has a Chief Data Officer, on the board of directors, empowered by a strong central governance organization consisting of dedicated councils and committees which have identified several clearly defined and well adopted data domains that span the entire organization of the service provider; Service provider also comprehensively monitors data quality on various dimensions (e.g., completeness, accuracy, timeliness, uniqueness, validity, etc.) with reporting and interventions in place in case any data quality issues are identified, and data is fully checked against reference data sources with few deviations if any			

3-3-2 Data Operations and Processes

GD.3-3	Governance Domain	Data Operating Model	Version	1
GD.3-3-2	Sub-Domain	Data Operations and Processes		
Sub-Domain Description	This sub-domain covers the processes surrounding the design, implementation, and data storage and management to maximize the value of data throughout its lifecycle from creation/acquisition to disposal as well as the involvement of leadership in these processes.			
Sub-Domain Best-in-class Practices	Having leadership involvement in the decision-making regarding data operations, and a well-defined operations plan which would require a service provider to perform activities such as forecasting storage requirements, database monitoring, establish access controls etc.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a data operations plan in place			
2	Service provider is creating a data operations plan that includes data operations such as forecasting data storage requirements, prioritization of information systems for business criticality, processes for selection of database management systems etc.			
3	Service provider has a data operations plan in place but does not cover technical operations such as data lifecycle management, database monitoring, access controls etc.			
4	Service provider has a comprehensive data operations plan in place that exhaustively covers all technical and business-specific operations and process linked with data storage management			
5	Service provider has a comprehensive data operations plan in place that is frequently reviewed by leadership in order to take strategic decisions on the data storage management practices			

3-3-3 Data Classification

GD.3-3	Governance Domain	Data Operating Model	Version	1
GD.3-3-3	Sub-Domain	Data Classification		
Sub-Domain Description	Data in any service provider organization should be classified on the basis of how critical it is to the success in a business area, as well as how sensitive that data is to security and privacy in order for teams to prioritize which data to use, secure and track issues for.			
Sub-Domain Best-in-class Practices	Regularly tracking any data issues that may exist, ensuring high level of adherence to data classification guidelines and well-defined data classification levels for all if not most types of data used by a service provider (e.g., 'Low Impact', 'High Impact', 'Public', 'Confidential', etc.), access management to restrict access of sensitive or critical data to only those users with a legitimate reason to access it, and enforcing classification standards by integrating it across systems such as email gateways, web gateways and data loss prevention solutions.			
Maturity Level	Maturity Level Description			
1	Service provider does not classify data, any classifications may happen independently by business units or analytics teams			
2	Service provider classifies some types of data but does not actively enforce classification guidelines across the organization			
3	Service provider classifies most types of data and enforces classification guidelines for some critical types of data elements (e.g., personal data, finance data, internal emails etc.)			
4	Service provider classifies most types of data and enforces classification guidelines for all types of data elements across the organization based on the level of risk associated with the data (e.g. Public, Internal, Confidential and Protected) and its importance to business areas or functions			
5	Service provider classifies all types of data and enforces effective classification guidelines with high degree of adherence, data issues are regularly tracked and fixed by a dedicated team of specialists			

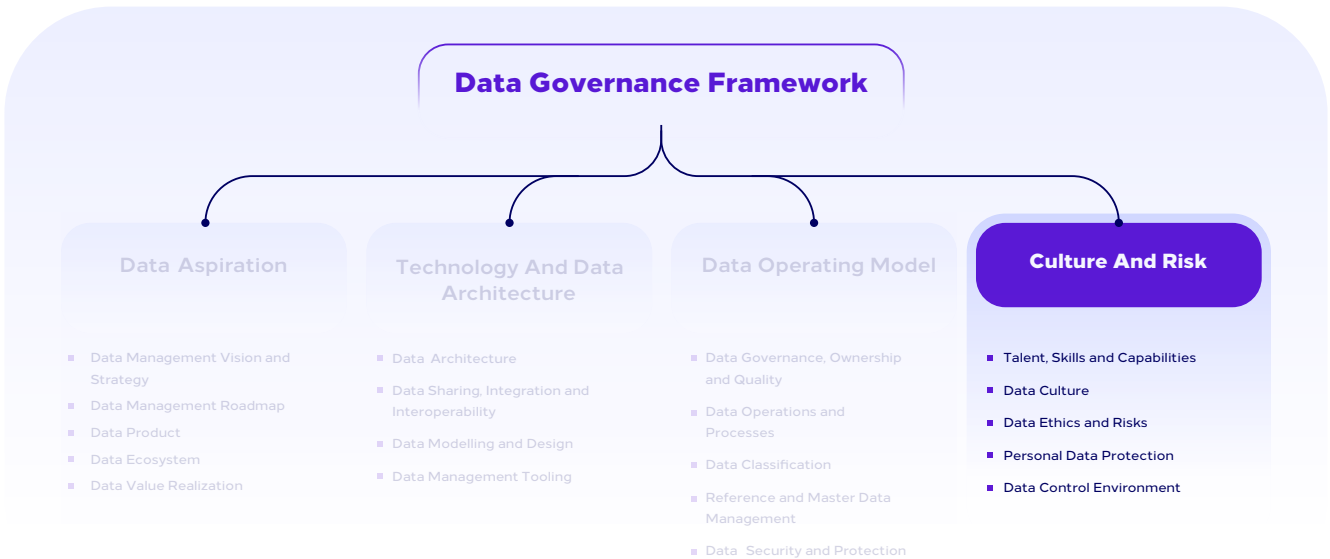
3-3-4 Reference and Master Data Management

GD.3-3	Governance Domain	Data Operating Model	Version	1
GD.3-3-4	Sub-Domain	Reference And Master Data Management		
Sub-Domain Description	This sub-domain allows linking of all critical data used by a service provider to a single reference and master data architecture, making it easier for data users to find, use, and understand the data owned by the service provider. Master Data Management solutions provide context to the data owned by a service provider and help to automate the process of classifying and managing the data. Master Data Management relies in part on the Metadata to meet compliance requirements and minimize risk exposure.			
Sub-Domain Best-in-class Practices	Establishing clear policies and standards for categorization of data elements, designing and documenting an effective architecture for a Reference and Master Data Environment, assigning data stewards to Reference and Master Data etc.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a reference and master data strategy and does not conduct any activities that may potentially be covered under it			
2	Service provider conducts activities such as classifying and identifying data objects used by the service provider but does not conduct them as part of a reference and master data strategy in place			
3	Service provider is in the process of implementing a reference and master data strategy which stipulates the mapping of the data used by a service provider by identifying master data objects, sources, prioritization of objects for inclusion, categorization of data objects, etc.			
4	Service provider has a well-defined strategy on reference and master data and has successfully identified, classified and mapped most of the data used by it and is now selecting a master data hub design to manage the reference and master data objects			
5	Service provider has successfully implemented a clear strategy on reference and master data which has led to benefits such as improvement in data quality, improved data compliance, etc. and continues to innovate and adapt to the best practices, architectures, and tools available globally			

3-3-5 Data Security and Protection

GD.3-3	Governance Domain	Data Operating Model	Version	1
GD.3-3-5	Sub-Domain	Data Security and Protection		
Sub-Domain Description	This sub-domain includes processes, people, and technology designed to protect the entity's data by defining the main data risks, restricting access to sensitive data assets and improving the cybersecurity infrastructure of an organization and following specific controls and guidelines set out by a corresponding regulatory authority.			
Sub-Domain Best-in-class Practices	Establishing an information security governance plan, having a dedicated team responsible for implementing information security practices, designing an information security architecture, keeping information security in mind while developing systems, having a robust identity and access management, etc.			
Maturity Level	Maturity Level Description			
1	Service provider does not have an organization-wide information security governance strategy, and has not restricted access to data resulting in a broader audience for sensitive data than intended with no identity and access management solutions in place			
2	Service provider has implemented identity and access management solutions and is in the process of creating an information security governance strategy and information security architecture but does not consider information security as a priority while developing systems			
3	Service provider effectively restricts access to most of their sensitive data while information security architecture, identity and access management, incident management, and other security tools are being implemented as part of the information security governance strategy			
4	Service provider has automated access approval systems for sensitive data, has implemented information security architecture, identity and access management, incident management, etc. as part of the information security governance strategy and prioritizes information security capabilities in any technical solutions it builds			
5	Service provider follows all recommendations by relevant information security guidelines set out by relevant regulatory authorities and takes steps above and beyond what is specified, continues to innovate and improve its data security and protection practices, and has successfully prevented data breaches through its effective information security practices			

GD.3-4 Culture and Risk



Domain Code	GD.3-4	Governance Domain	Culture and Risk
Governance Domain Description	Service providers that hire appropriate talent , incentivize adherence to data standards, promote ethical use of data and minimize risks to customers through data protection practices will be able to sustainably create a culture that embraces the use of data as a strategically important asset to increase operational efficiency, develop new products, improve existing products and services through innovative applications of data.		
Sub-Domain Code	Sub-Domain		
GD.3-4-1	Talent, Skills and Capabilities		
GD.3-4-2	Data Culture		
GD.3-4-3	Data Ethics and Risks		
GD.3-4-4	Personal Data Protection		
GD.3-4-5	Data Control Environment		

3-4-1 Talent, Skills and Capabilities

GD.3-4	Governance Domain	Culture and Risk	Version	1
GD.3-4-1	Sub-Domain	Talent, Skills and Capabilities		
Sub-Domain Description	This sub-domain refers to the management of the data and analytics talent and capabilities value chain (attraction, acquisition, development, retention etc.) which is critical to the data and analytics strategy of any service provider.			
Sub-Domain Best-in-class Practices	Creating well-defined career paths for both data-focused and data-adjacent roles, identifying talent requirements well in advance, ensuring skilled talent is retained, ensuring effective data management and data analytics training is provided to all employees interested in learning these skills, and fostering talent through events such as hackathons			
Maturity Level	Maturity Level Description			
1	Service provider does not have a comprehensive data and analytics talent management strategy, instead it allows business units to independently hire required talent or engage the services of outside-in experts for bespoke data and analytics projects			
2	Service provider is building a comprehensive data and analytics talent management strategy including well-defined roles, pay structures, job descriptions and is identifying the requirements for such talent at the enterprise, business unit, product or chapter level.			
3	Service provider is implementing a comprehensive data and analytics talent management strategy including data and analytics training for current employees, a well-defined talent acquisition strategy across all levels but has not focused on talent retention so far.			
4	Service provider has a comprehensive data and analytics talent management strategy in place with regular events to spur innovation and interest among employees such as hackathons, spotlights and workshops.			
5	Service provider has a comprehensive data and analytics talent management strategy in place covering acquisition, development, attraction as well as retention through industry leading benefits and employee experiences leading to highly skilled data scientists, analysts, stewards, engineers etc. being embedded across several teams creating value for the service provider through effective and innovative use of data. Service provider uses automation tools for planning and assessment of data talent, skills and competencies to ensure sustainable levels of attraction and retention throughout the organization.			

3-4-2 Data Culture

GD.3-4	Governance Domain	Culture and Risk	Version	1
GD.3-4-2	Sub-Domain	Data Culture		
Sub-Domain Description	This sub-domain describes how well a service provider can drive cultural change amongst employees to change their approach to treating data as an asset in order to bring about self-driven innovation to build new use cases from data and encourage self-discipline regarding adherence to data standards.			
Sub-Domain Best-in-class Practices	Best-in-class practices would differ from one service provider to another depending on the current maturity, ideal target state and planned scope for this transformation. Activities can include conducting trainings, tracking performance on data KPIs, conducting interviews to understand challenges, reward better performance etc.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a data culture strategy			
2	Service provider is in the process of creating a data culture strategy and is currently trying to understand the mindsets, behaviors and pain points of employees			
3	Service provider is rolling out some elements of a data culture strategy for a few select business units such as training and awareness programs, tracking relevant KPIs and sharing objectives of the strategy with employees			
4	Service provider has an enterprise-wide data culture strategy including training and awareness programs, tracking relevant KPIs, sharing target state, incentivizing adherence to data standards but the strategy has not yet led to self-driven data innovation use cases			
5	Service provider has implemented a well-defined enterprise-wide data culture strategy which has led to significantly higher data-driven innovation across roles at all levels, overall improvement in usability of data and an understanding of the benefits brought on by best data practices by most employees.			

3-4-3 Data Ethics And Risks

GD.3-4	Governance Domain	Culture and Risk	Version	1
GD.3-4-3	Sub-Domain	Data Ethics and Risks		
Sub-Domain Description	This sub-domain refers to the ethical usage of data and analytics models in order to protect the rights of individuals who may be influenced or impacted by products developed by the service providers as well as the management of the associated risk with using data that, if compromised or misused, may cause financial, legal, security, reputational or other types of risks.			
Sub-Domain Best-in-class Practices	Having well-defined practices regarding the ethical use of data and practices to mitigate potential data risks, taking decisions on the risk appetite supported by senior management, having a governance structure to monitor adherence to these practices and an intervention mechanism to ensure unethical data practices and actions that may cause risks are prevented from taking place.			
Maturity Level	Maturity Level Description			
1	Service provider does not look at data ethics and risk as part of its data strategy			
2	Service provider is building a data ethics and risk strategy , including defining a set of ethical data practices and identifying potential risks that might arise from data owned or used by the service provider			
3	Service provider has a data ethics and risk strategy in place which educates employees of ethical data practices, instructs employees on how to mitigate data risks that they might encounter and is also setting up a council or committee to monitor adherence to the data ethics and risks			
4	Service provider has a data ethics and risk strategy in place . A functioning council or committee regularly monitors if data users are compliant with ethical data practices defined by the organization as well as the measures to mitigate data risk			
5	Service provider has a comprehensive data ethics and risk strategy in place which has successfully identified and intervened whenever potential unethical data practices were being used or data was being used without considerations to risks, the service provider is also continuously improving its capabilities and is collaborating with its partners and suppliers to follow similar guidelines			

3-4-4 Personal Data Protection

GD.3-4	Governance Domain	Culture and Risk	Version	1
GD.3-4-4	Sub-Domain	Personal Data Protection		
Sub-Domain Description	As service providers collect and gather more data than ever before, it is critical that the personal data of customers, and employees are protected. Service providers must ensure that data breaches are avoided and that proper safeguards are put in place to ensure the proper handling and non-disclosure of personal information.			
Sub-Domain Best-in-class Practices	Conducting regular assessments of the data protection policies of the service provider, conducting training, having robust policies and processes to manage data breaches, having well-defined privacy policies, etc.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a personal data protection plan in place and has not conducted an assessment of its personal data protection environment (i.e., the rules, tools, techniques, procedures, etc. that are in place to protect personal data)			
2	Service provider is creating a personal data protection plan that is expected to be implemented in the next twelve months and has not yet conducted an assessment of its personal data protection environment (i.e., the rules, tools, techniques, procedures, etc. that are in place to protect personal data)			
3	Service provider has a personal data protection plan in place or is in the process of conducting an assessment of its personal data protection environment (i.e., the rules, tools, techniques, procedures, etc. that are in place to protect personal data)			
4	Service provider has a personal data protection plan in place and has conducted an assessment of its personal data protection environment (i.e., the rules, tools, procedures, etc. that are in place to protect personal data); the service provider also has processes in place to notify authorities and customers in case of data breaches and provides clear communication to customers and other data subjects of their personal data protection rights; service provider is fully compliant with all relevant regulations on personal data protection			
5	Service provider regularly reviews and revamps its data protection practices to account for new risks that might emerge, has adopted the best-in-class practices for personal data protection, has a consistent record of ensuring personal data is not compromised, and innovates in this space by testing new technologies, techniques and practices in personal data protection			

3-4-5 Data Control Environment

GD.3-4	Governance Domain	Culture and Risk	Version	1
GD.3-4-5	Sub-Domain	Data Control Environment		
Sub-Domain Description	Data Control Environment consists of policies and procedures that are used to manage and protect data, as well as the people, and processes involved in the data lifecycle. An effective data control environment helps a service provider to implement privacy and security policies as well as ensure data is effectively used to make informed decisions.			
Sub-Domain Best-in-class Practices	Having clear policies and procedures on how data should be collected, stored, processed, and used while ensuring transparency, collaboration, and alignment between data users, data owners, and the data management office across the data lifecycle with proper audits in place when necessary.			
Maturity Level	Maturity Level Description			
1	Service provider does not have a data control environment in place and data may be collected and stored in an ad hoc manner, without any formal processes or controls in place			
2	Service provider is currently building a formal data control environment to align cross-organizational data management capabilities, employees are being made aware of their responsibilities and some basic policies and technologies may be used to support these processes			
3	Service provider has a defined formal data control environment which has been adopted by most of the organization with a comprehensive set of policies and processes applicable on several teams but most the technologies to support the data control environment is still manual and not automated			
4	Service provider has a defined formal data control environment that is widely adopted, understood and followed by stakeholders to align data management capabilities, policies and standards across most business units, a well-established culture of adherence to data management policies, and a gradual adoption of automation techniques in the processes and auditing of the enforcement of these policies and procedures			
5	Service provider has a defined formal data control environment and it is a well-established part of the business as usual with most business units having successfully aligned their data management capabilities, policies and standards and has also automated several of the repetitive tasks in the processes and auditing of the enforcement of the policies and procedures that are part of the data control environment			

Glossary

Access Management

Access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users.

Data Management

The process of developing and executing plans, policies, initiatives, and practices to enable entities to manage and govern their data and achieve the aspired value, with data considered an organizational asset.

Cybersecurity

Protection of networks, systems, operations and their components of hardware and software, provided services, and contained data from any unauthorized access or disruption or misuse. The concept of cybersecurity includes information security and digital security.

Key Performance Indicator (KPI)

A type of performance measurement that evaluate the success of an organization or of a particular activity in which it engages; numerical threshold(s) are typically used to categorize performance.

Data

A collection of facts in a raw or unorganized form such as numbers, characters, images, video, voice recordings, or symbols.

Personal Data

Any element of data, alone or in connection with other available data, that would enable the identification of a Saudi citizen.

Data Classification

Setting the sensitivity level of data and information that results in security controls for each level of classification. Data and information security levels are set according to predefined categories where data and information is created, modified, improved, stored or transmitted. The classification level is an indication of the value or importance of the data and information of the organization.

Privacy

Freedom from unauthorized interference or disclosure of personal information about an individual.

Risk Appetite

The amount and type of risk that an organization is willing to take in order to meet their strategic objectives.

Service Provider

The service provider of under CST laws and regulations.

Data Stewardship

Data stewardship is a collection of functions that ensure all data assets of an organization are accessible, usable, safe, and trusted.

Appendix

GD.3-1 Data Aspiration Maturity Assessment Template

Column A	Column B	Column C	Column D	Column E
Sub-Domain Code	Sub-Domain	Maturity Level (1-5)	Modifier %	Sub-Domain Score $E = (C * D)$
GD.3-1-1	Data Management Vision and Strategy		20%	
GD.3-1-2	Data Management Roadmap		20%	
GD.3-1-3	Data Product		20%	
GD.3-1-4	Data Ecosystem		20%	
GD.3-1-5	Data Value Realization		20%	
Maturity Score for GD.1 Data Aspiration				[SUM of Column E]

GD.3-2 Technology and Data Architecture Maturity Assessment Template

Column A	Column B	Column C	Column D	Column E
Sub-Domain Code	Sub-Domain	Maturity Level (1-5)	Modifier %	Sub-Domain Score $E = (C * D)$
GD.3-2-1	Data Architecture		25%	
GD.3-2-2	Data Sharing, Integration and Interoperability		25%	
GD.3-2-3	Data Modelling and Design		25%	
GD.3-2-4	Data Management Tooling		25%	
Maturity Score for GD.2 Technology and Data Architecture				[SUM of Column E]

GD.3-3 Data Operating Model Maturity Assessment Template

Column A	Column B	Column C	Column D	Column E
Sub-Domain Code	Sub-Domain	Maturity Level (1-5)	Modifier %	Sub-Domain Score $E = (C * D)$
GD.3-3-1	Data Governance, Ownership and Quality		20%	
GD.3-3-2	Data Operations and Processes		20%	
GD.3-3-3	Data Classification		20%	
GD.3-3-4	Reference and Master Data Management		20%	
GD.3-3-5	Data Security and Protection		20%	
Maturity Score for GD.3 Data Operating Model				[SUM of Column E]

GD.3-4 Culture and Risk Maturity Assessment Template

Column A	Column B	Column C	Column D	Column E
Sub-Domain Code	Sub-Domain	Maturity Level (1-5)	Modifier %	Sub-Domain Score $E = (C * D)$
GD.3-4-1	Talent, Skills and Capabilities		20%	
GD.3-4-2	Data Culture		20%	
GD.3-4-3	Data Ethics and Risks		20%	
GD.3-4-4	Personal Data Protection		20%	
GD.3-4-5	Data Control Environment		20%	
Maturity Score for GD.4 Culture and Risk				[SUM of Column E]

Overall Data Governance Maturity Assessment Template

Column A	Column B	Column C	Column D	Column E
Domain Code	Domain	Maturity Score	Modifier %	Partial Score $E = (C * D)$
GD.3-1	Data Aspiration		25%	
GD.3-2	Technology and Data Architecture		25%	
GD.3-3	Data Operating Model		25%	
GD.3-4	Culture and Risk		25%	
Overall Data Governance Maturity Score for Service Provider				[SUM of Column E]



هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission