مركز الأنظمة الإلكترونية والمعلومات
SYSTEMS & INFORMATION CENTRE

ABU DHABI GOVERNMENT

DATA MANAGEMENT STANDARDS

VERSION 1.0

Contents

Document Configuration Control

Version	Release Date	Summary of Changes	Release Approval
1.0		**Initial Publication Release**	**Abu Dhabi Systems & Information Centre**

A review and update of this document will take place when changes require revising the Data Management Standards and associated Data Management Policy. Such modifications may relate to changes in roles and responsibilities, release of new legislation or technical guidance, or the identification of a new policy area.

The document should be distributed to:

Title	Format
Heads of all Abu Dhabi Government Entities	**Electronic copy; hard copy**

The document should be stored in the following locations:

Location	Format	Owner
Abu Dhabi Portal	**Electronic copy**	**ADSIC**
ADSIC website	**Electronic copy**	**ADSIC**
ADSIC office	**Hard copy**	**ADSIC**

This document affects the following parties:

Group

All Abu Dhabi Government Entity personnel, contractors, and third party individuals directly or indirectly involved in the provision of government services.

1. Executive Summary

Data is an essential resource for organisations. The success of an organisation is affected by the quality of the data used within its business processes. Effective data management is the key to maximising the quality of data, and allowing the organisation to deliver high quality services.

In recognition of this, the Abu Dhabi Government has developed a government-wide data management programme to be implemented by all Abu Dhabi Government Entities ('Entities'). The goal of the Abu Dhabi Government Data Management Programme is first to acknowledge that data is a key asset of the Abu Dhabi Government, and then to improve both the data management functions and the data stored within the Abu Dhabi Government. Owning and using high quality data is acknowledged as a strategic enabler for the Abu Dhabi Government in its journey to become a world-class administration.

The ability of Entities to share and consume valuable data within a managed framework opens up many opportunities to identify and deliver new or enhanced services to stakeholders, and to establish a working culture that leads to continuous improvement in the way these services operate.

World-class data management must be directed and supported from the highest levels of an organisation, with vision, direction, guidance and resources necessary to implement consistent policy and standards across and throughout the organisational structure. With these objectives being of primary importance, the Abu Dhabi Government has developed a core set of standards for data management based on the following principles:

1. Data shall be **owned**: all information used to enable the Entity's business must have a designated owner who is accountable for its proper custody.
2. Data shall be **described**: all data must be appropriately described to allow its content – and its purpose within the organisation – to be properly understood.
3. Data shall be of known good **quality**: all data must be of the appropriate quality for its use within the organisation.
4. Data shall be **accessible**: all data must be accessible to those who have a legitimate reason to use it. Data must be securely protected against loss, damage or misuse.
5. Data shall be **used and shared**: all data must be available to share easily with any legitimate party, and its use appropriately managed.
6. Data management shall be **implemented**: appropriate management of all data must be implemented through initiatives designed to introduce or strengthen particular data management capabilities.

The executive management teams of all Abu Dhabi Government Entities are requested to acknowledge that their vision, leadership, and commitment will ultimately decide how effectively their organisations embrace the aims of these Standards, and that this will determine whether they achieve effective management of the data given into their trust. The stewardship of government services is a significant and privileged responsibility. It is a responsibility that can be effectively realised when executives, staff and suppliers are committed to data management best practice.

2. Introduction

2.1 Overview

Successful data management has a profound influence on the effectiveness of any organisation. For the Abu Dhabi Government, a consistent approach will enable the smooth flow of data across Abu Dhabi Government Entities. This can be achieved by creating a common set of standards, and a governance platform upon which each Entity can develop an understanding of all of the data assets available across the government as a whole.

The Abu Dhabi Government Data Management Model (figure 1) represents the landscape of data management concepts within a hierarchy of dependent principles.

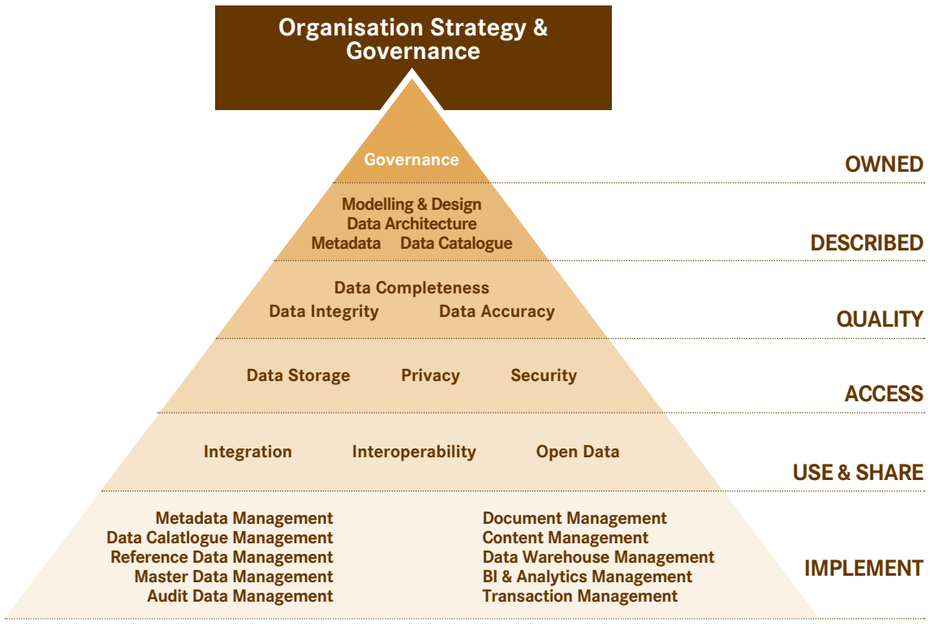

Figure 1: The Abu Dhabi Government Data Management Model

The principles are shown towards the right-hand side of the diagram. Under the overarching organisational strategy and programme governance, the model is read top down, with each principle providing a framework for the principles below.

Data **ownership** is of primary importance for governing the effective management of all data created, curated and used within each Entity.

Having established ownership, the model next indicates the need for Entities to develop and maintain a **description** of the data they own. The resulting catalogue of information about data is published and made widely available in a consistent form, and serves to communicate a common understanding of all the data owned by and maintained within the government.

The next principle in the model relates to all aspects of data **quality**. Entities are required to ensure that all the data they own is of sufficient quality appropriate to support its intended use.

The principle of **access** determines that data needs to be accessible to those who have a legitimate reason to use it, with the legitimate access enabled through proper security, privacy, storage, lifecycle and disaster recovery controls.

All data should be available to be **used and shared** by any legitimate party. Entities are required to ensure that data is readily shareable and re-usable, and that interoperability follows a consistent approach. This will lead to data services exposed via an enterprise integration platform. Legitimate parties to receive and use shared data could also be external stakeholders including those outside of government (eg citizens and other individuals, commercial companies and other organisations, other nations etc). Data and recipients shall be considered through the 'Open Data' controls.

Once the core principles of data management have been addressed, initiatives for managing and using data can be **implemented**. Such initiatives are at the level that most discussions about data take place – encapsulating subjects such as master data management, document and content management, data warehousing, business intelligence (BI) and analytics etc.

2.2 Purpose

The Abu Dhabi Government Data Management Standards document is intended to direct Entities and other stakeholders in areas requiring focus for the application of data management controls. Adherence to the Control Standards means that data management controls are being deployed consistently across Abu Dhabi Government Entities.

The Control Standards contained within this document represent the government's expectations for data management. The Control Standards are expressed in 13 domains of data management that are interrelated and mutually supportive. Entities and business partners handling government data have the responsibility to understand the Control Standards defined within this document, and to effectively apply these Standards in the context of all data assets they own.

The Standards – and assessments made against them – are instruments intended to support the significant goals of:

- Informed and responsible data ownership and usage;
- Protecting government data assets to a level appropriate to their value and the risks posed to them;
- Engendering and maintaining stakeholder confidence in the capability of government to deliver sufficiently secure and reliable services to the Emirate of Abu Dhabi;
- Protecting and enhancing the reputation of Abu Dhabi, at home and abroad; and
- Maximising the return on investment in information assets and systems, through the enhanced support afforded to their availability, confidentiality and integrity as part of a broader contribution to service quality.

Accompanying guidance documentation and checklists supports the Control Standards (see Section 7 Related Documents for an overview of these items). The Standards should be read in conjunction with these supporting materials.

2.3 Scope

The Abu Dhabi Government Data Management Standards provide definition of both management and technically-oriented control standards across 13 data management domains (Figure 2):

Figure 2: Abu Dhabi Data Management Domains

Domain	Definition
Data Governance	Provides planning and control over the implementation of the Data Management Programme, together with the governance checkpoint processes to show continued monitoring of compliance
Metadata Management	Planning, implementation, and control activities to enable easy access to high quality integrated metadata
Data Catalogue	Activities required of Entities in terms of creating, managing and contributing information about their datasets to the entitie's catalogue
Data Modelling and Design	Activities required of ADGEs in terms of designing data to meet the strategic requirements of the organisation
Data Architecture	Activities required for the ADGE in terms of defining the data needs of the enterprise, and designing the master blueprints to meet those needs
Data Quality	Planning, implementation and control activities that apply quality management techniques to measure, assess, improve and ensure the fitness of data for use
Data Security	Planning, development and execution of security policies to provide proper authentication, authorisation, access, and auditing of data and information
Data Storage	Requirements related to the management of structured and unstructured physical data assets at rest
Data Integration and Interoperability	Managing data in motion, discovering and intergrating data within the Entity and between Entities through a strategic integration platform
Open Data	Activities required of ADGEs to ensure the correct data is publicly available to appropriate quality standards, in appropriate formats, and with appropriate descriptions
Reference and Master Data Management	Planning, implementation and control activities to ensure consistency with a golden version of contextual data values
Documents and Content	The required activities relating to the lifecycle of content and documents outside structural databases
Data Warehouse, Business Intelligence and Analytics	Planning, implementation and control processes to provide decision support data, and support for knowledge workers engaged in reporting, query and analysis.

The functional scope of this document extends beyond information technology in order to address the broader scope of data management. The disciplines shown above are interrelated and interdependent; however, there is an implied hierarchy within the Standards. Each box shown in figure 3 acts as an enabling wrapper for the boxes contained within, for example, Governance controls establish the governance checkpoint process used by all subsequent data management domains.

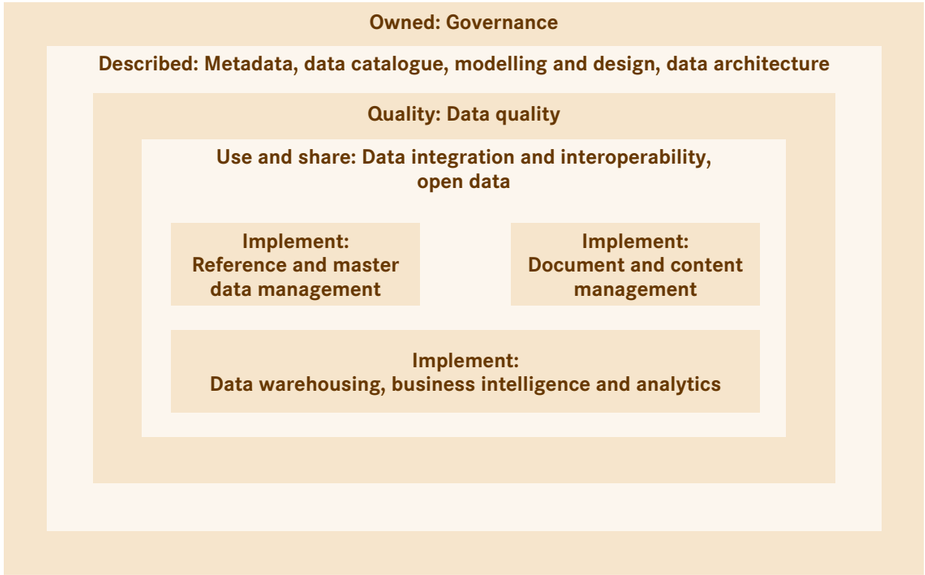

Figure 3: Structure of the Data Management Standards

Implementation of the Government Data Management Programme is required of all Entities, across all 13 domains. Entities shall gather evidence from across their business and technology functions in order to show compliance with these Standards from all data users. Entities shall use the data management domains to direct the implementation of all programmes that contain a data management element.

2.4 Applicability

Control Standards defined within this document must be applied by Abu Dhabi Government personnel, contractors and – wherever possible – other third party organisations (eg federal bodies) with responsibility for the creation, handling, storage, management transmission and destruction of Abu Dhabi Government data assets (including information systems and other equipment).

These Control Standards apply to all programmes of work that have an aspect of data management. This includes line-of-business information systems, whether new, changed, bespoke or commercial off-the-shelf. Some controls are applicable to the data management programme as a whole, such as the development of the data governance function, while other controls apply to each information system, data source or other information under the Entity's control (see section 5 – Data Management Framework for an overview). This shall include assets that are provided by – or managed for – the Entity by third-party organisations.

Entities have the responsibility for the rollout of a data management programme of work ensuring that controls are deployed in sufficient depth and range, applying the Control Standards effectively across the scope of the Entity's information assets.

3. Data Management Principles

Over the course of the Entity's Data Management Programme, initiatives will be established to develop capabilities within each of these domains, and this will involve changes affecting people, process and technology. The intention is to raise the maturity level for every Entity in each of these domains. As Entities individually increase aspects of their data management maturity, this will result in a respective increase in maturity for the Abu Dhabi Government overall.

The 13 data management domains are grouped together as 'data principles'. These principles assist in the understanding of the overall data management landscape and provide a natural grouping, hierarchy and sequencing with each principle providing the framework for the next.

Principle	Definition	Domains
Owned	All data must have an owner, and data management responsibilities must be assigned to an individual who is accountable for the management of the data within the scope of their role. Ownership shall be governed through the formation of a Data Governance Board.	• Data Governance
Described	All data must be described. Processes and tools must be in place to support the appropriate level of description of all data used and managed by the Entity. The breadth and depth of this information across the government promotes: • Standardised and simplified data sharing • Increased consistency and quality of data • Maximum discoverability and reuse of data • Wider use of data, both by people and also information and knowledge based systems • Greater opportunity for machine based 'understanding' of the meaning (ie semantics) of data, and therefore the development of automated 'intelligent agents' that are capable of responding to complex human requests based on this understanding	• Metadata Management • Data Catalogue • Data Modelling and Design • Data Architecture
Quality	Quality must be measured, monitored and managed in order to ensure sufficient data quality appropriate to support its intended use. Data quality must be defined and measured in order to provide the background understanding that allows business users of the data rely upon it to inform their decision making. Once data quality is known, a programme of data cleansing and monitoring can be introduced to improve the quality of the data in line with Entity's definitions of data quality. Practices shall be developed to ensure that data quality continuously improves.	• Data Quality
Access	Data must be stored in a format suitable to its use, and must be available to those who have an authorised need to access the data. This principle includes consideration of protecting the privacy of information relating to individuals, and the Entity shall be required to inform those individuals about whom data is captured of their privacy rights. Secure use of data ensures that all data access and data operations performed can be audited, monitored and traced back to individual users. Entities must ensure that data and information systems are stored/hosted in environments that are secure, robust and resilient. This is best served by adopting a consistent approach towards data server hosting, and exploiting the benefits of a centrally managed and virtualised private 'cloud'. This will require each Entity to undertake an audit of their existing and projected data centre utilisation and storage capacity, leading to the development and execution of a plan to migrate data and information systems into the best-suited environment. The lifecycle for all data should also be taken into account when considering data access, with particular emphasis on when data should be archived and/or destroyed. Entities also need to provide continuity of access, ensuring data is protected by an adequate backup schedule, and can be restored from backups. Entities will also need to establish provision for disaster recovery to ensure service disruption is minimised in the event of a prolonged system outage.	• Data Security and Privacy • Data Storage
Use and Share	Data should be created and managed using as few processes and systems as possible. Data should be shared between information systems and processes within the boundaries of the Entity, but also with third parties where relevant. Entities should review the current use and purpose of their data, only capturing data that is reasonable, necessary and proportionate to the tasks involved. Data services that are made available for data sharing and reuse is encouraged. For example, Entities should strive to design data services that allow functionality to be as generally applicable as possible, rather than simply meeting the needs of a specific and limited use case. This will lead to data services exposed via an strategic integration platform across the Entity and the wider government. Entities will also need to consider how to address the prospect of publishing information as 'Open Data', so that it can be shared with and used by stakeholders including those outside of government (eg citizens and other individuals, commercial companies and other organisations, other nations etc).	• Open Data • Data Integration and Interoperability
Implement	Data that is properly managed enables the Entity to implement information systems that take advantage of well-controlled data. Master and Reference Data , Document and Content management, data warehousing, business intelligence (BI) and analytics are frequently established without due attention to the core data principles, and this usually leads to delays and failures. The application of best practice, from industry and government, provides the greatest factors for success.	• Master and Reference Data Management • Documents and Content Management • Data Warehouse, Business Intelligence and Analytics

4. Entity Data Management Programme

The Abu Dhabi Data Management Standards are intended to support government Entities in implementing and embedding a Data Management Framework (see section 5). The breadth of the scope of the data management framework will require each Entity to develop a programme that is suitable to meet the requirements for compliance with the Standards, while meeting the continuing requirements of the Entity.

The principles of the Government Data Management Model (and its associated Controls and Specifications) have been developed so that required changes can be applied – where they exist – through established information systems programmes and projects.

Each Entity will need to mobilise a Data Management Programme to address the core principles of the Government Data Management Model.

Figure 4 illustrates the distribution of effort across the Government Data Management Model for the Data Management Programme and the projects that follow. The Entity will need to begin at the top of the model and focus on implementing the necessary elements of the 'Owned' principle. This activity will encompass elements to support all of the subordinate principles, providing the operational framework that will ensure that future projects and programmes require less additional effort.

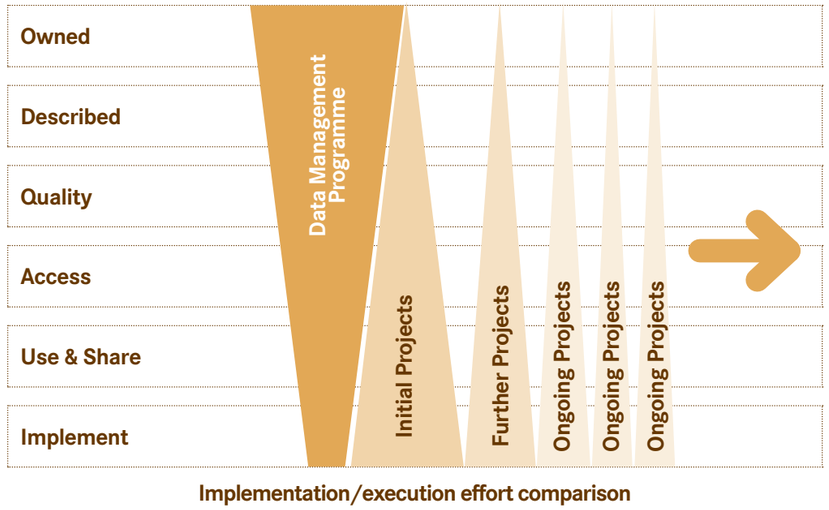

Figure 4: Distribution of Effort in the Government Data Management Model

As the Programme progresses to address each of the data principles in turn, there is less foundation work required from subsequent information system projects. It is important to establish the organisation, processes and tools that support the data principles as soon as possible, to allow business-focused initiatives within the Entity to align with the Control Standards, in order to realise the benefits that the Data Management Programme attracts.

The adoption of the Data Management Standards across the data domains should be considered on a case-by-case basis. Each Entity will have programmes and projects that are already in progress or planned to start, and each of these projects will touch various datasets across the business domains. It is recommended that these initial projects apply the Data Management Standards to the datasets within their scope.

5. Data Management Framework

The Government Data Management Model provides a framework to shape the structure of the Standards within this document. Each of the data management domains represented within the model have controls and specifications that are applicable across different levels within the Entity's own programme for data management.

The three levels of programme applicability are:

Programme Applicability	Description
Data Management Programme	Controls that provide structure, governance and process for the Entity's Data Management Programme eg data governance, managing Entity metadata, enterprise data modelling, and developing an Entity-wide data architecture roadmap
Enterprise Data Capabilities	Controls that deliver data capabilities across the Entity's business functions eg data cleansing, master and reference data management, and business intelligence capabilities
Application Data Management	Controls that manage data within line of business information systems eg data security, data architecture, and data modelling

These three levels of applicability provide the Entity with a framework (figure 5) for implementing the Data Management Standards.

Entities can begin the implementation of the Control Standards almost immediately by focusing initially on the Data Management Programme-level controls. This covers the development of policies, governance processes, the identification and cataloguing of data owned by the Entity, and establishing a data architecture roadmap to assist in planning and implementing both the Enterprise Data Capabilities and the Application Data Management capabilities.

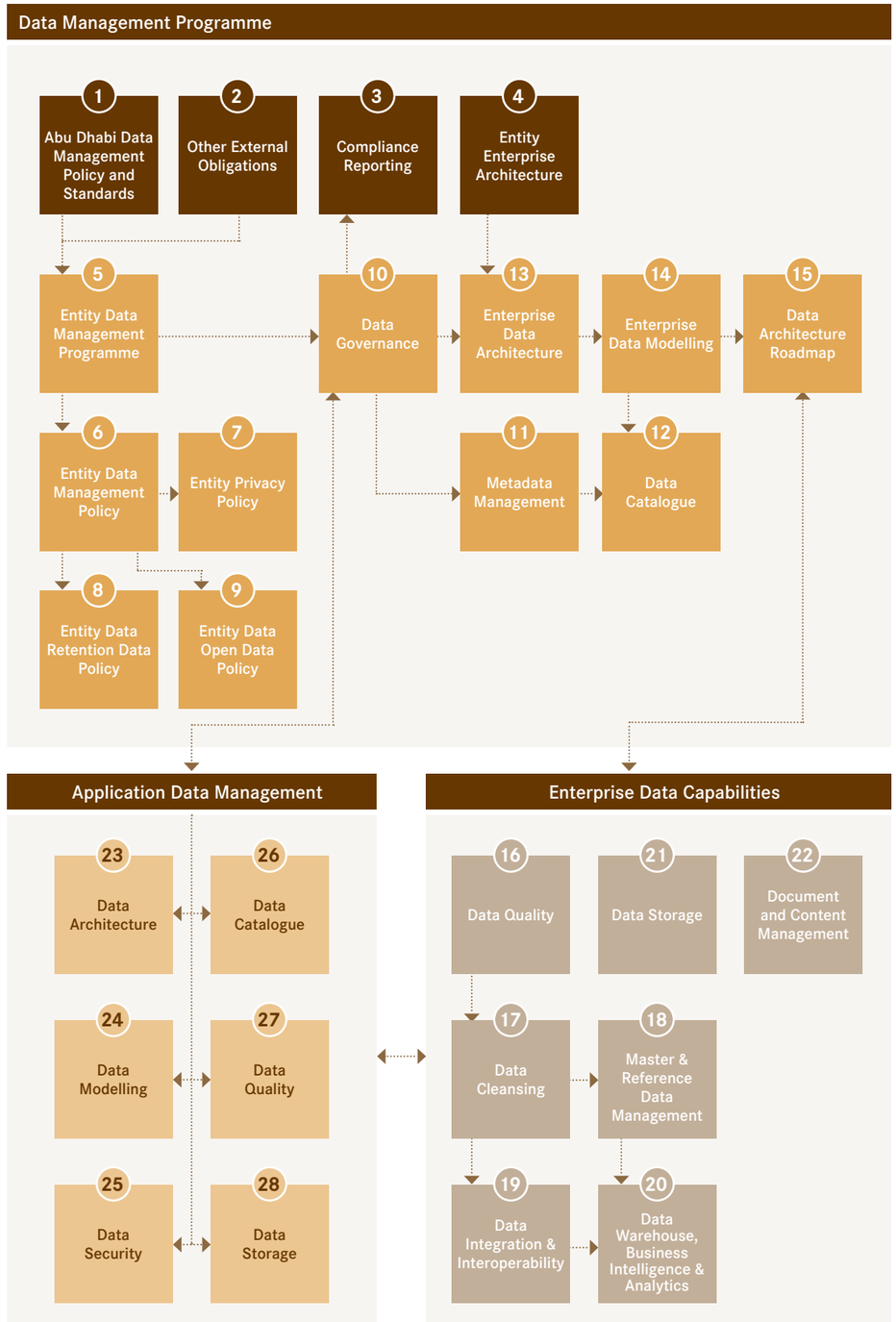

Figure 5: Abu Dhabi Government Data Management Framework

Each of the elements of the Data Management Framework are described in the following table:

Item No	Element	Description	Primary Related Control Standard(s)
Data Management Programme			
1	**Abu Dhabi Government Data Management Standards**	This document: provides definition of Data Management Control Standards that an Abu Dhabi Government Entity (ADGE) is expected to follow	All
2	**Other External Obligations**	Other external obligations such as government technology standards, including UAE National Information Assurance Standards, and the Metadata and Standards described in the Abu Dhabi Government Interoperability Framework (eGIF)	
3	**Compliance Reporting**	Gathering evidence and reporting standards compliance to the Abu Dhabi Government Data Governance Committee	
4	**Entity Enterprise Architecture**	The business processes and supporting technology that enable the Entity's service delivery	DA.1
5	**Entity Data Management Programme**	The Entity's programme to implement these standards	DG.3
6	**Entity Data Management Policy**	The Entity's internal documented policies for managing each of the 13 data domains	DG.2
7	**Entity Privacy Policy**	The Entity's public Privacy Policy, describing the Entity's obligations and the rights of its service users	DSP.2
8	**Entity Data Retention Policy**	The Entity's internal documented policy for data retention, describing how long data will be kept and the circumstances that will lead to data archival and destruction	DG.2
9	**Entity Open Data Policy**	The Entity's public Open Data policy, describing the requirements, circumstances and licence under which data shall be published to the public	DG.1
10	**Data Governance**	The Entity's Data Governance Board, and the Governance Checkpoint Process used to evaluate evidence of compliance from enterprise and application level programmes	DG.1, DG.2, DG.3
11	**Metadata Management**	Defining the names, values and definitions of data that shall be managed from across the Entity's business functions	MD.2
12	**Data Catalogue**	Capturing metadata in the form of master profiles, data models, data structures, both at a business and technical level	DC.3, DC.4
13	**Enterprise Data Architecture**	Developing the baseline and target data architectures from across the Entity's business functions	DA.2, DA.3, DIO.2, DWBA.2

Item No	Element	Description	Primary Related Control Standard(s)
14	**Enterprise Data Modelling**	Modelling the master profiles that cross system boundaries that support the Entity's business functions; this is a deliverable of the Enterprise Data Architecture, and helps populate the Data Catalogue	DM.2, DM.6, DWBA.3
15	**Data Architecture Roadmap**	The plan to fill the data capability gaps between the Entity's baseline and target data architectures	DA.4
Enterprise Data Capabilities			
16	**Data Quality**	Enterprise-wide data quality management and monitoring	DQ.1, DQ.2
17	**Data Cleansing**	Provision of data cleansing tools and processes and skills for the Entity's master profiles	DQ.3
18	**Master and Reference Data Management**	Managing versioned reference data across the Entity, and ensuring the single 'golden view' of the Entity's master profiles through matching and merging techniques	RM.1, RM.5
19	**Data Integration and Interoperability**	Providing the ability to consistently share high-quality data both within the Entity and between Government Entities	DIO.1
20	**Data Warehouse, Business Intelligence and Analytics**	Providing coordinated data warehousing, business intelligence and analytics capabilities through a defined set of tooling across the Entity's business subject areas	DWBA.1, DWBA.6, DWBA.7
21	**Data Storage**	Centralised Entity data storage provision	DS.3, DS.4
22	**Document and Content Management**	Managing the classification, traceability and workflows of documents and content across the Entity	DCM.2
Application Data Management			
23	**Data Architecture**	The development of baseline and target data architecture for line-of-business applications in order to fulfil the requirements of the enterprise-wide data architecture roadmap	DA.1
24	**Data Modelling**	Performing data modelling for the appropriate audiences within line of business applications	DM.1
25	**Data Security**	Alignment with the Information Security Standards and providing tooling support for data access monitoring, data loss prevention, data masking, and monitoring data privacy issues	DSP.1, DSP.3, DSP.5
26	**Data Catalogue**	Populating data sets with their ownership, quality, security and access endpoints as metadata within the Data Catalogue to enable data reuse across the Entity	DC.4
27	**Data Quality**	Addressing Data Quality at the source of data through data validation and user awareness	DQ.2, DQ.3
28	**Data Storage**	Utilising centralised data storage and managing data lifecycle	DS.7

6. Compliance and Enforcement

All Abu Dhabi Government Entities are expected to adhere to these Standards. Conformance with Control Standards should be prioritised, with Entities themselves determining which Standards should be addressed first. The Entity should consider its own risk profile, and its available resources when deciding upon prioritisation.

The Entity should maintain its own self-assessment capabilities to determine if compliance is being maintained. It is anticipated that this capability will be achieved through a Governance Checkpoint Process, allowing evidence and justifications to be presented to the Data Governance Board at specific programme and project milestones. This shall be overseen by the Entity's Data Manager, who shall provide compliance evidence to the Abu Dhabi Systems and Information Centre (ADSIC)as required, which has the primary and definitive responsibility for determining if compliance to these Standards has been achieved.

Entities and individual staff members found to be non-compliant with these Standards may have their access to information systems and data revoked.

Information systems found to be non-compliant with these Standards may be restricted from processing government data and from connecting to government networks.

Abu Dhabi Government Entities are responsible for ensuring that third party suppliers engaged on their behalf are acquainted with – and contractually committed to – adhering to relevant elements of these Standards and the Entity's Data Management Programme.

7. Related Documents

7.1 Alignment with Related Government Standards

The Abu Dhabi Data Management Programme is one of a number of initiatives sponsored by the Executive Council of Abu Dhabi.

These Standards are intended to provide a coherent perspective on multiple disciplines relevant to the management of data by Abu Dhabi Government Entities. These Standards are not intended to replace or replicate other government standards.

Where government-wide policies and standards exist in related areas, then these should be regarded as the authoritative reference, and any contradictions should be resolved in favour of the government standards and policies for their specific areas. Examples of potential government-wide standards include:

- Enterprise Risk Management
- Audit Management
- Incident Management
- Business Continuity Management

Where there are no government-wide standards in any associated areas, then Entities may reasonably assume that these Data Management Standards serve as the primary reference until other such materials are approved and published.

The Data Management Standards are aligned to, and support compliance with, the following standards:

- Approved Information Security Standards in the Abu Dhabi Government
- Abu Dhabi Government Interoperability Framework, including:
    - Technical Standards Catalogue
    - Metadata Management Standards and Profile Bindings
    - Namespace Policy
- Statistics Centre Abu Dhabi (SCAD) Data Management, Metadata and Data Quality standards
    - SCAD “160913 Statistical Quality Checklist”
    - SCAD Dataset and Variable Elements Standard
    - Generic Statistical Business Process Model (GSBPM)
    - SCAD Data Management Policy

8. Implementation priorities – When and How to Apply Controls

8.1 When to Apply Controls

Government Entities are expected to exercise discretion and good judgment in determining what Data Management controls to implement, and where, how and when to implement the controls.

The decision-making process will be influenced by:

- The mandate and business objectives of the Entity
- The business processes that the Entity transacts
- The value and sensitivity of the government data assets within the Entity’s custody
- The complexity of the Entity’s supply chain (eg the extent to which its business process is dependent upon third parties)
- The range, depth and potential impact of risks faced by the Entity
- The resources on hand for building, implementing and managing data management-related controls
- The knowledge, skills and experience of Entity personnel in relation to the data management domains
- The legacy of controls that have already been deployed

Additionally, the Entity will be guided by two elements from these Standards that will help determine an appropriate sequence of control implementation, these being:

Suggested Priority

Three priorities have been allocated, and are applicable within the context of the Government Data Management Model:

Priority 1: The essential first steps that should be taken by any organisation to provide a base level of process and governance controls.

Priority 2: Controls that represent an expansion of data management maturity across the Entity’s data management programme.

Priority 3: Controls that provide additional support for building data management capability.

Each of these priority allocations exist in the context of each principle through the Government Data Management Model. Thus, the Priority 1 controls within the “Ownership” principle should be addressed before the Priority 1 controls within the “Described” principle, and so forth.

These priorities are meant only to guide the Entity – they are not intended to be prescriptive. Due to its own unique circumstances, the Entity may determine that a different priority sequence is warranted.

The highest priority controls have the underlying themes of:

1. Setting clear management direction for what is expected of the Entity’s data management capabilities.
2. Deploying a foundation of planning, process and governance controls to provide an organisational maturity with which to deliver improved data management practices.
3. Implementing improved data management practices across the data in the custody of the Entity, starting with the data already in the scope of active or planned programmes of work.

Control Specification Applicability
Section 9 defines the levels of Control Specification Applicability relevant to a given control (ie 'Mandatory' or 'Recommended'). The interrelationship between control priority and control specification applicability may be summed up as: Control specification applicability confirms the expected level of control application, ie what must and what should be done. Control prioritisation provides an indication of how quickly a given Control Standard might be addressed. It is preferable to maintain a balance in the Entity's data management control set, and for controls to be mutually supportive. In this context, an Entity seek to implement a range of control specifications from across the domains rather than all of the Priority 1 Controls (including 'Recommended' items).

8.2 How to Apply Controls

These Standards impose compliance obligations upon Entities. However, discretion and good judgement are required as to what resources are applied, and in what configuration, in order to achieve those obligations, and to implement any additional controls judged necessary by the Entity.

Entities need to determine what organisational structure best suits achievement of its own Data Management Programme Plan. Examples of where decisions are required include:

- Whether the mandate of the Data Governance Board should be addressed by a free-standing committee or incorporated into a body that already exists
- Whether the role of Data Manager should be full or part time
- Whether the role Data Manager should also function as the Chair of the Data Governance Board
- Whether the level of risk, programme goals and level of activity provide justification for additional data management-related resources
- What weighting should be applied to data management roles (ie technical vs managerial)
- What minimum level of experience, competence and qualifications post-holders require to successfully achieve the goals of the Entity's Data Management Programme

A one-size-fits-all approach is not practical, given the diversity of Abu Dhabi Government Entities in terms of their remit, structure, risk profile and resources.

In the above context, data management domains described within these Standards should not be taken to be equivalent to specific organisational roles or units. For example, obligations for reference or master data management may be undertaken as a central capability or be split across applications, depending on the demands and structure of the Entity.

Within the Standards, terms such as 'significant' and 'appropriate' have been used. These require a subjective decision to be made on the part of the Entity, an example being:

"The Data Governance Board shall develop guidance appropriate to its departments and stakeholders."
(From DM2.2)

For such control specifications, the Entity is obligated to determine for itself what constitutes 'appropriate' in the context of its own business processes, risks, and deployed technologies. It is neither practical nor advisable for these Standards to specify absolutes across all areas of an Entity's delivery of data management. For areas requiring subjective decision making, the Entity should be able to demonstrate, during assessment, that the judgement applied was thoughtful and took advantage of all necessary and available information.

9. Mandatory vs. Recommended Control Specifications

The Control Standards described within this document show two levels of expected applicability in relation to control specification:

- Mandatory
- Recommended

The level of Control Specification application is expanded upon in the table below.

Applicability Level	Mandatory (M)
Description	
'Mandatory' Control Specifications are expected to be complied with in full by the Entity, from the time that the given Control Standard is implemented. Due to constraints of finite time and resources, it is recognised that an Entity will not be able to achieve compliance with all 'Mandatory' components from the outset of its own programme for data management. The Entity's Data Management Programme Plan should demonstrate the prioritisation for control implementation, mapped to the relevant Control Standards within this document. Suggested priorities have been proposed against each Control Standard within this document, but Entities are expected to apply management discretion, based upon their business priorities and identified areas of weakness.	
Impact Upon the Entity's Risk Management Activities	
Mandatory control elements need to be implemented, irrespective of the results of the Entity's risk management activities. They represent core areas of capability in the given discipline of data management.	

Applicability Level	Recommended (R)
Description	
Recommended Control Specifications are those that ADSIC assessment teams would typically expect to see in place. However, there is the understanding that circumstances specific and unique to the Entity may mean that the given Control Specification is either not applied at all, or not applied in full. However, such exemptions would need to be on the basis of defined criteria that can be justified by the Entity. (It should not be interpreted that 'Recommended' Control Specification elements are merely advisable to implement.) For any Control Specification not designated as 'Mandatory', there is a degree of discretion and judgement that needs to be applied by the Entity's management.	
Impact Upon the Entity's Risk Management Activities	
Risk analysis will help determine if the Entity's unique circumstances make the given control type applicable or not applicable in the specific setting being analysed. Risk management can provide the Entity with informed and coherent justification for the de-scoping of Recommended Control Specifications, where appropriate.	

Entities should recognise that the Abu Dhabi Data Management Standards provide a common base of data management definition that provides a platform to increase the value of data assets across government.

The Standards are not an end in themselves, and achieving the minimum necessary compliance with the Standards should not be regarded as a primary goal. In the above context, Entities have the primary responsibility for ensuring that they have the appropriate depth and range of data management controls deployed. In some circumstances, the Entity may determine that the control definition required exceeds what is found in these Standards.

10. Common vs Tailored Data Management Controls

Government Entities should take the opportunity to review how their obligations to these Standards can be met. In the implementation of any control set, there is the need to balance time, cost and quality constraints effectively. Entities should seek opportunities that allow them to implement the right data management controls at the right time, and in the right way.

Common data management controls have the greatest potential to help the Entity balance expenditure on Data Management versus effectiveness of the controls deployed.

However, for common controls to be effective, their range of potential uses needs to be carefully evaluated. A control that is ideally suited for Service A may be less appropriately optimised for Service B when it is introduced a year from now.

Examples of common controls that multiple information systems and services could potentially leverage include:

- Standardised integration design patterns and formats
- A standardised breadth and depth for metadata detail captured, providing consistency of coverage based on the category of data
- Processes for review and consideration of best practices for data management implementations
- Organisational clarity of the assignment of accountability and responsibility for data management activities
- Implementation of data management tools and platforms to support a broad range of requirements across the Entity's data portfolio

The application of common controls will depend on the risk context and the business need of the Entity. There will be circumstances where a tailored data management control (ie one that is specific to an individual service or system) is necessary, justified and preferable.

The Entity has the obligation to understand its own data management needs, opportunities and weaknesses, and to tailor its control set appropriately. The Abu Dhabi Data Management Standards are intended as a starting point for informed engagement within the Entity.

'Tailored' controls will be ones that are specific and unique to the target data asset. They will be utilised where no common control is available, or where the available common control is not fit for a specific purpose. Tailored controls do not necessarily indicate that the control has been heavily customised. Such a control might be a standard off-the-shelf type from a vendor, but which has been acquired specifically in reference to a target information system. Equally, a version or copy of an existing common control may be adapted or configured in a way that makes it unique to a specific control requirement.

Examples of tailored controls:

- An application system might come supplied with an embedded metadata feature that describes its data structures
- An application system might come supplied with embedded data integration features and design patterns/ formats that differ from the common controls
- The stringency of review and approval processes might be varied depending on the nature of the data in scope for the review

11. Alignment to Standards

The development of these Standards has been informed by reference to – and use of – international best practice from government, industry and academia. The following references have served as the primary sources:

- Asset Description Metadata Schema (ADMS) (W3C, 2013)
- Common Warehouse Metamodel (OMG, 2003)
- Data Management Body of Knowledge (Mosley and Brackett, 2010)
- Data Catalogue Vocabulary (DCAT) (W3.org, 2014)
- Dublin Core® Metadata Initiative (DCMI) (Dublincore.org, 2014), (Standardised in ISO 15836:2009)
- IBM Data Governance Unified Process (Soars, 2010)
- ISO 8000 Data Quality
- ISO11179 Metadata Registries
- ISO 15489-1:2001 Information and documentation
- ISO 22301 Business Continuity Management Systems
- ISO 27017 Cloud Security Standards
- ISO 27018 Handling of Personally Identifiable Information
- Telecommunications Infrastructure Standard for Data Centers, (Telecommunications Industry Association, 2005)

12. External dependencies

The Control Standards described in this document have no external dependencies other than those described in Section 8 Related Documents. The Entity may find that it is necessary, however, to consider the impact of additional external data management guidelines as they emerge.

13. Control Structure

The key shown below describes guidance on the individual elements of the control structure.

XX.5 (1)	Control Name (2)		**Version** (3)	1
			Suggested Priority (4)	1
Control Standards (5)	Control Standards definition			
Control Type (6)	Directive ☑	Preventive ☐	Detective ☑	Corrective ☐
Control Specification				**M/R**
XX.5.1 (7)	Control Specification definition			M
XX.5.2	Control Specification definition (8)			R
Control Version History (9)				
V1.0 (10)	Control Version History			
Control Dependencies	List of Data Management Controls that this control depends upon			
References (11)	List of related references that are used and/or related to this control			

Key	Element	Description
1	**Control numbering**	The numbering format is: DOMAIN.CONTROL STANDARD NUMBER An example being: DG.1 This means that this is the first control in the Data Governance section of the standards. A Control Specification within a Control Standard inherits its numbering from its parent control standard. So: DG.1.2 means that this is the second element of Control Specification applicable to the DG.1 Control Standard.
2	**Control name**	The title of the control standard
3	**Version**	The current iteration of the control
4	**Suggested Priority**	A suggested priority has been offered for determining the order in which control standards should be addressed (see section 8.1)
5	**Control Standards**	The data management outcomes needing to be realised in order to achieve Standards compliance and to ensure adequate security

6	**Control Type**	Directive Controls: Express management expectations of behaviours and activities to support compliance with the data management programme Preventative Controls: Provide a framework for the implementation of best practice processes in order to avoid data management risk Detective Controls: Identify data management issues to allow early remediation Corrective Controls: Targeted data management techniques to improve managed data
7	**Control Specification**	One of more elements of control implementation specifying how a given control standard shall be met. Each control specification has a unique reference. Compliance with each control specification will support the improvement of the Entity's data management practice. Control specifications should be introduced into the Entity's business processes as appropriate.
8	**Compliance Requirement**	As described in section 9, there are Mandatory (M) and Recommended (R) control specifications. The Entity should articulate a rationale for why a recommended control specification does not apply in each specific case concerned.
9	**Control Version History**	The version history allows recording control version changes following this release of the document. In version 1, this field is left empty.
10	**Control Dependencies**	Other Control Standards upon which a given Control Standard has a direct dependency. Dependencies may be pre-requisite dependencies that must be complied with to ensure that this control is effective or a functional dependency where this control shall use the techniques described in order to comply.
11	**References**	External best practice references beyond the content of this document, from other government bodies, industry best practice and academia.

14. Data Management Standards

14.1 OWNED: Data Governance

DG.1	**Organisational Structure**			**Version**	1
				Suggested Priority	1
Control Standards	The Entity shall develop an organisational capability to support data governance				
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐	
Control Specification					**M/R**
DG.1.1	The Entity shall establish an organisational structure to support the Data Management Programme. • The organisation shall be positioned in the Entity with sufficient authority such that it is empowered to do its job effectively • The organisation will take responsibility and accountability for Data Management • The organisation will be based on the Roles and Responsibilities described in this control. An illustrative example of an appropriate RACI matrix is provided in the appendix				M
DG.1.2	The Entity shall convene the Data Governance Board to manage delegated authority and responsibility within the Entity. The Board will be the final arbiter within the Entity for all matters relating to data management. • This Board should have representatives from each area affected by data management initiatives, with the Data Manager responsible for the execution of the Boards actions through the programme management function of the Entity • The Data Governance Board shall meet regularly (weekly, initially) to provide independent oversight and support for the Data Management initiatives being undertaken by the Entity				M
DG.1.3	The Entity shall appoint a Data Manager. The Data Manager shall have delegated authority from the Data Governance Board. The Data Manager shall: • Oversee the implementation of change • Ensure compliance with governance, policy and standards • Ensure the coordinated training and awareness programmes are executed within the Entity • Share best practice with other Entities				M

DG.1.4	The Entity shall identify and appoint Data Architects to support the Data Manager. The Data Architects shall: • Work with the Data Manager and the Data Governance Board to ensure the implementation of the Data Management Standards in all designs across the Entity • Establish a clearly defined target state for all data sources • Establish a clearly defined roadmap to achieve the target state for all data sources • Be responsible for developing and maintaining a formal description of the data and data structures within the Entity, including: 1. Data designs and design artefacts 2. Dataset metadata definitions 3. Data flows throughout the Entity	M
DG.1.5	The Entity shall identify and appoint Data Stewards to support the Data Manager in both the business and technical areas of the organisation. • The Data Stewards will take responsibility for the lifecycle of the data as it passes through information systems and ownership boundaries • The Data Stewards will take responsibility for the quality of the data under their stewardship, and cleanse the data as necessary	M
DG.1.6	The Entity shall identify and appoint Data Owners (who are responsible for a particular dataset) to support the Data Stewards. Data Owners will be drawn from both the business and technical areas of the organisation. • The Data Owners will take responsibility for a particular dataset throughout the lifecycle across systems • The Data Owners will ensure the quality standards for their dataset are met • The Data Owners will liaise between the business and technical stakeholders to ensure that their dataset is maintained to the highest standards possible	M
DG.1.7	The Entity shall regularly undertake monitoring and compliance checking to ensure that information systems and data related processes are implemented in accordance with established policy, standards and best practices. Such reviews should include coverage of: • Performance of the domain processes • User satisfaction	M
Control Version History		
1.0		
Control Dependencies		
References	Data Governance (Ladley, 2012) DMBOK (Mosley and Brackett, 2010) Four Critical Principles of Data Governance Success (Griffin, 2010) IBM Data Governance Unified Process (Soars, 2010)	

DG.2	**Data Management Policy**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop their data management policy		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DG.2.1	The Entity's Data Management Policy shall address the scope of its data management systems, roles, responsibilities, management commitment, coordination among organisational functions, and compliance obligations.		M
DG.2.2	The policy document shall be approved by the Entity's Data Management Board, Data Manager and the Entity's executive management, and shall be published and communicated to all employees and relevant stakeholders.		M
DG.2.3	The policy shall contain a definition of data management; its overall objectives and scope, and the importance of data management as a pillar of upholding high standards of data quality.		M
DG.2.4	The policy shall be applicable to all business functions of the organisation and should be supplemented by supporting instructions and guidance where appropriate for specific areas of activity.		M
DG.2.5	The Entity shall establish its Data Management Policy (through implementing this control), describing how data will be managed across the Entity. The Data Management Policy shall be supported by the production of an internal Document Retention Policy – describing the Entity's policy for retaining, archiving and destroying documents (See Document and Content controls).		M
DG.2.6	In support of the Data Management Policy, the Entity shall establish policies for public consumption where there are external stakeholders. The following policies should be made publicly available: • Privacy Policy – the Entity's statement of public individuals rights over their data, and the Entity's obligations to those individuals (See Data Security and Privacy controls) • Open Data Policy – describing the process and rationale under which data shall be published (See Open Data controls)		M
DG.2.7	The policy shall cover the end-to-end data management lifecycle.		M
DG.2.8	The policy shall include a clear statement of management intent, showing support for the principles of data management, and reinforcing its importance in alignment with government strategy.		M
DG.2.9	The policy shall underline management expectations of teams and individuals when handling data, and highlight the importance of maintaining high levels of data quality at all points within the organisation's operations.		M

DG.2.10	The Entity shall include governance metrics and process checkpoints within their policy, describing how they will measure the effectiveness of data management throughout the Entity's information systems and processes on a continuous basis. • Measures and metrics should be maintained continuously • Measures and metrics should be tracked to reveal trends • Measures and metrics should be available for audit purposes at all times	M
DG.2.11	The policy shall describe the mechanism allowing business and technical users to raise data related issues, including a clear escalation plan to ensure such issues are appropriately handled and resolved.	M
DG.2.12	The policy shall describe the change management process. This shall include how it applies to the Data Management Programme and its initiatives.	M
DG.2.13	The policy shall be regularly reviewed and updated (annually at a minimum). The Data Management Board shall ensure the policy's continued relevance, adequacy, and effectiveness. Policy reviews should become more frequent if significant business or regulatory changes occur.	M
DG.2.14	The Entity shall ensure that all policy developments are aligned with all relevant legislation.	M
DG.2.15	The Entity shall collect and maintain evidence of compliance with their policies, and with the Control Specifications within these standards.	M
DG.2.16	The policy shall be quantifiable and traceable back to the Control Standards of this document; the Entity should be able to demonstrate how each control will contribute to achieving a given policy requirement.	M
DG.2.17	The Entity shall ensure that all personnel and stakeholders (internal, external, contractors etc) confirm in writing that they have read, understood, and will comply with the obligations articulated within the Policy. A formal signed written record from all individuals asserting understanding and compliance with the policy should retained on file for future reference.	M
Control Version History		
1.0		
Control Dependencies	DG.1 Organisational Structure	
References	Building Effective Data Governance Models, Policies, and Agreements in a Hi Tech world (Indiana Health Information Exchange, 2012) Data Governance (Ladley, 2012)	

DG.3	**Data Management Programme**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop and execute a plan for implementing its data management programme.		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DG.3.1	The Entity shall agree and maintain specific, measurable and scheduled goals in support of its Data Management Programme. Goals shall reflect the programme's obligation to support: • Business strategy and priorities • The Entity's management of its data related risks • Compliance obligations to data management policy and these Standards, and other relevant laws and regulations • The promotion of an organisational culture within the Entity that is aware of data management concerns and responsibilities		M
DG.3.2	The Plan shall be made available to ADSIC for review.		M
DG.3.3	The Plan shall: • Provide a clear roadmap for data management initiatives, their priorities and dependencies • Demonstrate clear alignment with the Entity's strategic plan and objectives • Be reviewed annually to ensure it remains effective and aligned with evolving priorities • Include key performance indicators for analysis to track progress on a continual basis. • Provide a clear indication of internal budget requirements for delivering the planned initiatives		M
DG.3.4	The Entity shall ensure that robust version control of all Data Management Programme artefacts is detailed within the plan		M
DG.3.5	The Entity's Data Management Programme shall be approved by the Entity executive with responsibility and accountability for the risk being incurred to organisational operations		M
DG.3.6	In support of its Data Management Programme, the Entity shall develop supporting plans to build out specific capabilities in defined areas. These subsidiary plans may include (but are not limited to): • Data Governance (including the Governance Checkpoint Process) • Organisational Awareness and Training (See DG.4) • Disaster Recovery (See Data Storage controls) • Document and Content Management • Data Architecture Management • Inter-Entity Data Integration • Reference and Master Data Management Subsidiary plans may be rendered as either freestanding documents or as appendices to the Entity's Data Management Programme Plan.		M

DG.3.7	The Entity shall ensure that the principles and structure of the Government Data Management Model (Owned, Described, Quality, Access, Implemented) are adhered to within the Data Management Programme, and that these principles are built into subsidiary plans and business processes introduced through the rollout of the Data Management Programme.	M
Control Version History		
1.0		
Control Dependencies	DG.1 Organisational Structure DG.2 Data Management Policy	
References	Abu Dhabi Information Security Standards Data Governance (Ladley, 2012)	

DG.4	**Change Management**		**Version**	1
			Suggested Priority	1
Control Standards	The Entity shall develop and maintain its change management processes for the Data Management Programme as a whole, and domain-level processes developed within the Data Management Programme			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification				**M/R**
DG.4.1	The Entity's Data Governance Board should approve all changes to the Data Management Programme (eg Plan or Policy).			M
DG.4.2	The Entity shall integrate its existing change management processes into each of the data management domains, or create a new change management process if none already exists.			M
DG.4.3	The Entity should establish a baseline for its Data Management Programme Plan, with proposed changes to the plan being analysed for impact			M
DG.4.4	Changes to the Data Management Programme Plan should be coordinated with the organisation-wide Change Management capabilities of the Entity to ensure on-going alignment between Data Management and other organisation initiatives.			M
DG.4.5	Where compliance with these Standards requires a change to existing business process, the Entity shall perform an impact assessment to identify relevant stakeholders and other impacted processes in order to properly coordinate and communicate the change.			M
DG.4.6	As Business Processes are identified to be in compliance with these Standards, the Entity shall establish a baseline for each process to allow the Data Governance Board to assess and ensure that future business process change remains compliant with these Standards.			M
Control Version History				
1.0				
Control Dependencies	DG.1 Organisational Structure DG.3 Data Management Programme			
References	Data Governance (Ladley, 2012) DMBOK (Mosley and Brackett, 2010)			

DG.5	**Organisational Awareness**		**Version**	1
			Suggested Priority	2
Control Standards	The Entity shall develop and execute organisation-wide awareness programmes for the required data domains			
Control Type	Directive ☑	Preventive ☑	Detective ☐	Corrective ☐
Control Specification				**M/R**
DG.5.1	The Entity shall establish, maintain – and review an ongoing awareness and training programme for – data management, including but not limited to: • Training required for specific individuals or roles • The legal and regulatory framework within which the Entity's data is managed • Information systems and processes that impact data management			M
DG.5.2	Training records shall be retained, and refresher training carried out at regular intervals (annually should be considered as the minimum interval or else as determined by the requirements of the training content for a specific domain or other topic). New training shall be provided when there new requirements (eg new policy, standards or projects).			M
DG.5.3	For those responsible for creating, manipulating, interpreting, managing or disposing of data, training shall include (but not be limited to): • The scope and purpose of the Entity's Data Management Programme and policy • The role and benefit of these Standards • Key roles, responsibilities and processes supporting the Data Management Programme, with contact information provided for relevant post-holders • The Data Catalogue and importance of capturing accurate Metadata • Data Security responsibilities to ensure the confidentialiy, integrity and availablilty of data • Data Quality impact to ensure that data is captured and maintained correctly • The Entity-wide requirement for common data architecture and known data quality • The identification of data for release under the Open Data policy • The requirements on the Entity to facilitate data sharing with other Entities • Their individual responsibilities under the Data Management Programme			M
DG.5.4	All personnel with defined responsibilities within the Data Management Programme shall be provided with training tailored to their role type, with appropriately tailored content, length and frequency as required by specific roles.			M
DG.5.5	The Entity shall determine in advance the learning outcomes and desired capabilities in order to provide focussed and structured training. The Data Governance Board should verify that training is being delivered in a manner consistent with the requirements of the Data Management Programme.			M

DG.5.6	The Entity shall implement a general awareness programme to raise the profile of the user responsibilities and programme benefits within Data Management Programme, with particular attention to Data Quality, Data Security and data and document lifecycles.	M
DG.5.7	The Entity shall develop a communications approach in order to manage and track the rollout of data management awareness across the Entity's users. The communications approach shall confirm the requirements of different categories of users and the specific messages, delivery channels and frequencies of communication. The Entity shall monitor the effectiveness of the communications approach.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DG.4 Change Management	
References	Abu Dhabi Information Security Standards (2013) UAE Information Assurance Standards Data Governance (Ladley, 2012) DMBOK (Mosley and Brackett, 2010)	

DG.6	**Capability Audit**		**Version**	1
			Suggested Priority	1
Control Standards	The Entity shall perform an audit of its capabilities and/or current state for each data domain			
Control Type	Directive ☑	Preventive ☐	Detective ☑	Corrective ☐
Control Specification				**M/R**
DG.6.1	The Entity shall develop a Data Management Audit Framework to ensure compliance with the Data Management Policy and Standards. The Audit Framework shall address • The Scope of the Entity's Data Management Programme • Roles and Responsibilities within the Data Management Programme • Management commitment and coordination across the various departmental levels within the Entity Data Management Audit activities should be supportive of the Entity's existing Internal Audit Framework and the Information Security Framework. Alignment should be achieved with the Entity's Internal Audit Plan.			M
DG.6.2	The Data Governance Board shall facilitate development and implementation of Data Management audits. Implementation of Data Management audits should be approved by an overseeing function independent of the Entity's Data Governance Board.			M
DG.6.3	Data Management auditors should be independent of the function/ process being audited to ensure the opportunity for an objective assessment to be undertaken. The reporting line for Data Management auditors should be via the overseeing function referenced in DG.6.2			M
DG.6.4	The Entity shall facilitate external audits by ADSIC or approved third parties on an annual and ad hoc basis. External auditors should be competent to undertake Data Management audit, with an appropriate level of skills, experience and qualifications in each domain as required. The overseeing function should ensure that auditor profiles are relevant to the target audit (eg relevant technical skills appropriate to the data domain under assessment).			M
DG.6.5	The Entity shall regularly undertake monitoring and compliance checking to ensure that information systems, data related processes and data sharing practices are implemented in accordance with established policy and standards. Such reviews should include coverage of: • Performance of the data management domain processes • User satisfaction			M
DG.6.6	Audit results shall be supported by evidence and divided into 'Findings' (verified non-compliance with these Standards and/or the Entity's own security policy and procedures), and 'Recommendations' (suggested areas for Data Management enhancement or improvement. Findings should reference the specific clause(s) of the target publication where non-compliance has been identified Audit results and supporting evidence shall be stored for a period of no less than three years.			M
DG.6.7	Audit results shall confirm the potential risks that could be manifested due to an identified finding not being addressed			M
DG.6.8	Audit results shall be classified and protected to a level at least equivalent to the Information Security classification of the highest security data source being audited			M
DG.6.9	Data Management audit activities should be coordinated with other audit activities within the Entity, to ensure effective reporting on performance and compliance while also minimising the business impact of audit			M
DG.6.10	The Entity shall maintain and update their Data Management Programme Plan and Policy in response to the relevant audit findings in each data domain			M
Control Version History				
1.0				
Control Dependencies	DG.1 Organisational Structure DG.3 Data Management Programme DG.4 Change Management			
References	DMBOK (Mosley and Brackett, 2010) IBM Data Governance Unified Process (Soars, 2010) UAE Information Assurance Standards			

DG.7	Performance Management	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop, report against and analyse key performance indicators relating to its Data Management Programme		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			M/R
DG.7.1	Data management performance reporting shall be against specific, measurable, achievable, realistic and timetabled goals articulated by the Entity's Data Governance Board and the Abu Dhabi Data Management Programme. Goals should encompass the Entity's business needs as well as legal and regulatory obligations.		M
DG.7.2	The Entity shall develop outcome-based performance metrics to measure the effectiveness and efficiency of its Data Management Programme and implementation of these Standards in support of the programme. The Data Governance Board shall serve as the authorising and overseeing body for Data Management performance metrics. The board shall: • Oversee the setting of performance metrics aligned to the Entity's Data Management Programme plan and its compliance obligations to these Standards • Receive and analyse performance data from the Data Manager (supplied by Data Owners and others responsible for compliance) with each domain within the Data Management Programme • Report performance of the Data Management Programme to ADSIC and other relevant stakeholders at a frequency and in a format specified by those stakeholders		M
DG.7.3	The Entity's Data Management performance metrics shall be aligned to the performance indicators of the Abu Dhabi Government Data Management Programme, and should support the Entity in reporting timely and accurate Data Management status to ADSIC and other relevant stakeholders.		M
DG.7.4	Data Management performance data shall be verified by a competent and independent party that is not directly connected with the work that is the subject of measurement.		M
DG.7.5	Data Management performance reporting shall consider multiple dimensions of data management performance. These should include (but are not limited to): • Compliant technology business processes • Compliant line of business processes • Level of maintenance of data architecture artefacts • Production and completeness of Entity-level data models and architectures • Level of maintenance of system-level data models and architectures • Documented master profiles across the Entity's line of business systems • Data quality milestones • Active master and reference data management achievements • Information and document lifecycles		M
DG.7.6	The Entity shall implement continuous improvement mechanisms that are informed by performance data and the analysis associated with the metrics. The Data Governance Board shall monitor the cost, benefit and status of proposed and implemented improvements		
Control Version History			
1.0			
Control Dependencies	DG.1 Organisational Structure DG.3 Data Management Programme		
References	DMBOK (Mosley and Brackett, 2010)		

14.2 DESCRIBED: Metadata Management

MD.1	Metadata Standards Conformance	Version	1
		Suggested Priority	1
Control Standards	The Entity shall conform with existing metadata standards		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			M/R
MD.1.1	The Entity shall conform to applicable Abu Dhabi Government Metadata Standards (such as the eGIF, SCAD standards and geospatial metadata standards).		M
MD.1.2	The Entity shall ensure that metadata management tools adhere to ISO/IEC:11179 Metadata Registry Standards.		M
MD.1.3	The Entity shall comply with the requirements and recommendations in ISO/IEC:11179 Part 4 'Formulation of Data Definitions' when defining data. This Standard presents the steps required to develop unambiguous data definitions. This applies to the definitions that make up the Entity's business glossary and data dictionary, but also wherever metadata definition and capture are required in other data management domains.		M
MD.1.4	The Entity shall comply with the principles documented in ISO/IEC:11179 Part 5 'Naming and identification principles'. This standard presents principles to be followed to develop names and identifiers (eg Emirates ID) that have meaning to people, or only have meaning within a particular data context (such as synthetic keys). Names and identifiers that have meaning to people are typically related to the data item's definition.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme		
References	Abu Dhabi Government eGIF ISO/IEC:11179 Metadata Registries (ISO/IEC, 2004)		

MD.2	Metadata Management Programme	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop and execute a metadata management initiative, ensuring processes exist to make metadata defined, captured and accessible		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
MD.2.1	The Entity shall develop and execute a metadata initiative. Metadata management describes the processes and practices of the Entity in order to effectively gather, store and use metadata. Activities within a metadata management initiative include, but are not limited to: • Assessment of existing metadata sources and repositories • Stakeholder interviews to develop initial knowledge about the range of data held • Gathering requirements for business and technical metadata • Development of metadata architecture • Establishment of data stewardship functions to gather and maintain, and to promote metadata usage • Production of a metadata management rollout plan	M
MD.2.2	The Entity shall utilise Abu Dhabi government and international standards when developing their metadata (eg eGIF, SCAD, Geospatial, ADMS) to accommodate the needs of its particular operational context. In alignment with the Abu Dhabi Government eGIF Metadata Standard, the specialised standards will contain the metadata Elements, Refinements and Encoding Schemes to represent the values necessary to be captured in the Entity's particular context. The development of Metadata Elements, Refinements and Encoding Schemes shall take account of metadata defined and captured in other data management domains (eg Data Security, Data Quality etc).	M
MD.2.3	The Entity shall manage metadata using both automated and manual techniques. Automated scanning of information systems using data discovery tools, metadata capture tools and other proprietary methods, shall be used to maintain the accuracy of metadata according to a schedule defined by the metadata management programme. Data Stewards shall manage all metadata that has been captured via automated processes, and shall be responsible for maintaining additional business and technical metadata (where this is not captured automatically). Data Stewards are responsible for the quality of the metadata (Ref: MD.4.4).	M
MD.2.4	The Data Governance Board shall be responsible for arbitrating any conflicts relating to the definition and quality of metadata that cannot be resolved by Data Stewards. For example, such situations may emerge where metadata names, definitions, or values cross-departmental boundaries.	M
MD.2.5	The Entity shall ensure that all metadata is accessible via the Data Catalogue (see Data Catalogue Standards), which shall be used as the user access point end for the repository of metadata, data dictionary, business glossary, and associated modelling and architectural deliverables.	M
MD.2.6	The Data Catalogue shall support indexing, search, and retrieval of metadata appropriate to the given user's role.	M
MD.2.7	The Entity shall ensure that all aspects of metadata definitions (including Elements, Refinements and Encoding Schemes) are version controlled, and that all metadata values identify the version they were captured against.	M

Control Version History	
1.0	
Control Dependencies	DG.6 Capability Audit MD.1 Standards Conformance
References	DMBOK (Mosley and Brackett, 2010) Enabling Interoperability of Government Data Catalogues (Maali, Cyganiak and Peristeras, 2010) Overview of Government Metadata Standards (Alasem, 2009)

MD.3	Metadata Architecture	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop its metadata architecture to support the requirements of its metadata management programme		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
MD.3.1	The Entity shall document the metadata architecture according to the requirements of the Data Architecture standards (see DA Standards). Metadata architecture shall be a component of the Enterprise Data Architecture.	M
MD.3.2	The Entity shall evaluate the most appropriate metadata architecture that meets the business requirements while maintaining alignment with any emerging central standards. Justification for the architectural approach shall be submitted to the Data Governance Board for approval. Possible architectural approaches for metadata systems include: • Centralised: A central metadata repository, storing all data required by the data catalogue, data modelling, data dictionary and business glossary • De-centralised: Separate physical metadata components delivered through a single access point. Automatically scanned metadata remains in the source systems and repositories, with access made available • Hybrid: Separate physical components delivered through a single access point; however, automatically scanned metadata is pulled in from source systems and managed, maintained and refreshed centrally	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme MD.2 Metadata Management Programme
References	Building Semantic Interoperability in Europe (European Commission, 2012) Digialiser.dk semantic asset repository - Case Study (European Commission, 2012a) XRepository semantic asset repository - Case Study (European Commission, 2012b)

MD.4	Metadata Monitoring	Version	1
		Suggested Priority	1
Control Standards	The Entity shall implement metadata monitoring		
Control Type	Directive ☐	Preventive ☐	Detective ☑	Corrective ☐
Control Specification			**M/R**
MD.4.1	The Entity shall define measurements for the quality of metadata names and definitions according to the Data Quality standards. This may include the encoding of subjective business experience, user surveys and so forth to aid understanding of the effectiveness of metadata capture, discovery and use.		M
MD.4.2	The Entity shall monitor and report on metadata quality according to the measurements defined.		M
MD.4.3	The Entity shall monitor metadata coverage across the Entity's business functions, in terms of: • Metadata definition coverage – how many of the Entity's business functions are covered by metadata definition • Metadata capture coverage – how many of the Entity's business functions have metadata values captured, and to what depth are they captured • Metadata usage coverage – how many of the Entity's business functions are making use of captured metadata; of particular concern should be metadata captured across business function boundaries		M
MD.4.4	The Entity shall monitor the effectiveness of metadata stewardship across the organisation through the use of workflow monitoring, issue tracking, and training and awareness programmes.		R
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme MD.3 Metadata Architecture		
References	DMBOK (Mosley and Brackett, 2010)		

14.3 DESCRIBED: Data Catalogue

DC.1	Data Catalogue Requirements	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop a Data Catalogue that fulfils the Abu Dhabi Government Data Catalogue core requirements		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DC.1.1	The Entity shall align its Data Catalogue with mandatory standards to facilitate Data Catalogue interoperability. The following standards are mandatory: • Abu Dhabi Government eGIF Schema Generation • DCAT – Data Catalogue Vocabulary to describe data sets • XSD – XML Schema Definition, used to describe dataset structure		M
DC.1.2	The Entity should align its Data Catalogue with the recommended standards, as follows: • ADMS – Asset Description Metadata Schema, used to describe assets, schemas, data models and reference data • RDF – Resource Description Framework, used to describe the semantic relationships between data assets Where a Data Catalogue does not align with a given standard (eg due to lack of vendor support), the Entity shall document and submit justification for non-alignment to the Data Governance Board		R
DC.1.3	The Entity shall develop a Data Catalogue capability that includes the following features: • Metadata repository – to store or otherwise provide access to the Entity's metadata (see MD3.2 for description of acceptable metadata repository architectures) • Publishing portal – to provide controlled access to metadata, definitions, data models, and reference datasets • Workflow management tool – to facilitate the management of Data Catalogue entries across their lifecycle • Business glossary – allowing business-level profiles, attributes, definitions and rules to be stored and accessed • Data dictionary – allowing technical-level profiles, attributes, definitions and rules to be stored and accessed • Data model repository – to store application specific and enterprise data model assets • Version control – versioning of metadata definitions, captured metadata, reference data, and other stored assets		M
DC.1.4	The Entity shall align their data catalogue requirements with government-wide data catalogue requirements as they emerge.		M
Control Version History			
1.0			
Control Dependencies	DG.6 Capability Audit MD.1 Standards Conformance MD.2 Metadata Management Programme MD.3 Metadata Architecture		

References	Asset Description Metadata Schema (ADMS) (W3C, 2013) Data Catalogue Vocabulary (W3.org, 2014) DMBOK (Mosley and Brackett, 2010) Resource Description Framework (RDF) (W3C, 2014)

DC.2	**Data Catalogue Principles**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall implement and manage a Data Catalogue according to cataloguing principles		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		**M/R**
DC.2.1	The Entity shall develop its Data Catalogue in alignment with each of the following principles: • Usability – make pragmatic design decisions about the Data Catalogue with the end user in mind • Common usage – use a standard vocabulary that meets the understanding of the end user • Representation – names and descriptions should be based upon real-world concepts where possible • Accuracy – the captured data should accurately describe its real-world representation • Sufficiency and necessity – elements should only be included that are required to fulfil user tasks or to uniquely identify an entry • Economy – the least cost or simplest approach should be taken • Consistency – entries in the Data Catalogue should be of a consistent depth and breadth • Integration – names and descriptions describing the data captured should be integrated and consistent across the Entity's business functions Alignment shall be shown through the Governance Checkpoint Process. Where principles conflict, the Entity shall develop a pragmatic solution, and submit a justification for approval by the Data Governance Board.	
DC.2.2	The Data Catalogue shall act as a single point of access for all users (both internal and external) of the description of the Entity's data assets. Though specific data assets (such as datasets, metadata, data models, etc) will continue to reside in a multitude of separate systems, the Data Catalogue should provide a central resource that allows users to find and determine information about any asset.	

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DC.1 Data Catalogue Requirements
References	DMBOK (Mosley and Brackett, 2010)

DC.3	**Data Catalogue Population**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop and execute a plan to populate the Data Catalogue across the Entity's business and technical functions		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		**M/R**
DC.3.1	The Entity shall identify datasets for inclusion in the Data Catalogue. Such datasets shall include, but are not limited to: • Transactional data within application systems • Reference datasets • Datasets containing master data profiles • Statistical data • Geospatial data Consideration shall be given to the size of the potential numbers of users of that data, the likelihood of re-use, and the breadth, depth and complexity of the data.	M
DC.3.2	The Entity shall employ suitable methods to discover datasets that should be populated within the Data Catalogue. Such discovery is likely to involve both human interactions, and assistance by technical tooling designed for the purpose. Specialised technical components can be used to scan a network for data sources and datasets within an organisation. Human interactions might include holding interviews and developing awareness programmes targeted at the individuals that produce, manage, or disseminate data that could be worthy of inclusion in the Catalogue.	M
DC.3.3	The Entity shall identify priorities for including data in the Data Catalogue. In particular, this should take account of previous demand for data from both internal and external users. Particular consideration shall be given to the sequence in which metadata is captured; typically business-level metadata should be captured first, followed by technical, and then semantic metadata. The Data Manager shall produce a roadmap for populating the Data Catalogue, which shall be submitted to the Data Governance Board for approval.	M
DC.3.4	The Entity shall produce and store data models for the data captured in the Data Catalogue (see Data Modelling standards). Data models for data within the Data Catalogue shall captured at the following levels: • Business – describes data in business terms, to aid understanding of business requirements • Technical – describes data in technical and physical implementation-specific terms, to assist technical development activities and operational management of data	M
DC.3.5	The Entity should develop semantic data models for the data captured. Semantic models describe the relationships within data using a defined vocabulary that is machine-readable.	R

DC.3.6	The Entity shall define appropriate metadata for the data capture using the techniques described in the metadata standards. This includes developing or re-using Elements, Refinements and Encoding Schemes, and creating standard names and definitions. Re-use should be preferred. The metadata requirements of the Abu Dhabi Government eGIF, and the metadata requirements for the other domains within these Standards, shall be observed and included on the Data Catalogue Population Roadmap.	M
DC.3.7	The Entity shall capture and populate metadata into the Data Catalogue. The approach shall be documented within the Data Catalogue Population Roadmap for each dataset to be captured. Metadata captured shall include (but is not limited to): • Ownership, publisher and contact information • Security classification (See the approved Information Security Standards in the Abu Dhabi Government)Data quality definitions and ratings • Validity period and refresh dates • Version information	M
DC.3.8	The Entity shall ensure that metadata is appropriately maintained within the Data Catalogue. The primary mechanism shall be through the Governance Checkpoint Process; however, the Data Catalogue Population Roadmap shall specify minimum metadata refresh periods for each dataset captured.	M
DC.3.9	The Entity shall classify their data assets according to the following data classification hierarchy: • Metadata – Metadata is essential for capturing descriptions about data. As the name suggests, metadata is also data in its own right, and is often characterised as 'data about data'. • Reference Data – Reference data comprises constrained lists of values that classify other information. Typically, the data that appears within a dropdown list on a website will constitute reference data (though it is not a requirement for reference data values to be published in this form). A list of countries is an example of reference data. • Master Data – Master data contributes to a single view of key business data profiles, though the elements of that view may be distributed across multiple systems. A customer name or address is an example of master data that forms part of the 'customer' profile. • Transactional Data – Transactional data is used within a business process. This type of data is typically created at the start of a process, modified during the life of the process, and is then stored as outcome of the process. • Audit and Log Data – Audit and log data is generated by systems to provide a history of all steps involved in a process. The data classes towards the top of the hierarchy are more important, because data in the lower classes depends upon data in the upper levels. The volume of data within the higher classes is less, but increases for data towards the bottom. Data in the higher classes is relatively static and has a longer lifecycle than data towards the bottom (which is more likely to change frequently but have a shorter useful life).	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme MD.3 Metadata Architecture DC.1 Data Catalogue Requirements DC.2 Data Catalogue Principles
References	Abu Dhabi Government Information Security Standards (2013) DMBOK (Mosley and Brackett, 2010)

DC.4	**Data Catalogue Usage**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop internal guidance and monitoring for usage of data published through the Data Catalogue		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		**M/R**
DC.4.1	The Entity shall develop and publish a licensing model for data sharing, which shall be made available through the data catalogue.	M
DC.4.2	The Entity shall plan and execute an awareness programme to publicise the information available within the Data Catalogue to its business and technical stakeholders. The awareness programme shall highlight the benefits to project teams of re-using data, and describe the datasets available for re-use.	R
DC.4.3	The Entity shall ensure that the System Development Lifecycle (SDLC) of information systems includes consideration for re-use of the datasets captured within the Data Catalogue. Consideration for data re-use shall be monitored through the Governance Checkpoint Process for approval by the Data Governance Board.	M
DC.4.4	The Entity shall encourage submissions for innovative use of data from across business and technical functions, which shall be evaluated for merit by the Data Governance Board. The Data Governance Board, through the Data Manager, shall socialise data innovation resulting from Data Catalogue usage.	M
DC.4.5	The Entity shall allow consumers of datasets to register their data usage in the Data Catalogue. Registered consumers of data published through the Data Catalogue shall be informed of changes within the dataset, such as significant data refreshes, data model changes, and data purges. A consumer is defined as an individual, an application system representative, or business function representative.	M
DC.4.6	The Entity shall classify registered consumers of datasets published through the Data Catalogue with a status of Formal or Informal. Formal registered consumers shall be identified by the provision of service level (or other agreements) between the data producer and consumer. Informal consumers receive no such agreement outside of the bounds of the published licence and policy.	M

DC.4.7	The Entity shall monitor and report on the effectiveness of the Data Catalogue according to the following minimum metrics: • Coverage of dataset represented in the Data Catalogue from across business functions • Registered datasets consumers • Completeness of metadata entries for datasets The Entity shall report the effectiveness of the data coverage annually to the Data Governance Board.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme MD.4 Metadata Monitoring DC.2 Data Catalogue Principles DC.3 Data Catalogue Population	
References	DMBOK (Mosley and Brackett, 2010)	

14.4 DESCRIBED: Data Modelling and Design

DM.1	**Implement Tools and Methods**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop and execute a plan for introducing and standardising data modelling tools and techniques		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DM.1.1	The Entity shall ensure that data models for information systems within the software development lifecycle are reviewed by the Data Governance Board as part of its Governance Checkpoint Process. Data models shall form a core deliverable of any system built, purchased, or commissioned by an Entity as part of developing its data architectures in support of business and technology requirements.		M
DM.1.2	The Entity shall implement data modelling tools with the following minimum capabilities: • The creation of UML2.x-compliant models • Support for UML model interchange using the XMI Interchange Format • Modelling and reverse engineering structured datasets • Modelling unstructured datasets (see DM.10) • Use of the Common Warehouse Metamodel (CWM) for modelling data warehouse systems • Associating metadata to models to facilitate and promote re-use • Model versioning and traceability		M
	Where the Entity already has data modelling tools, it shall certify that any existing toolset meets the minimum capabilities. Evidence should be captured and be available upon request to support any specification and development of centralised tooling. If the Entity's toolset does not meet the requirements, the Entity shall begin an initiative to fill the requirement gaps, whether that be through the purchase of new tooling or through other development or negotiation with suppliers.		
DM.1.3	The Entity shall provide appropriate training and education programmes for developing data models in order to promote awareness, and increase its value for business and technical users. This training shall be delivered as appropriate to the user's levels of engagement with information systems. For example, business users should understand conceptual data models in order to discuss high-level concepts, whereas database administrators require deep understanding of the development and maintenance of physical data models in order to properly support production systems.		M
DM.1.4	The Entity shall develop data models at the conceptual, logical and physical level. A typical journey to document the as-is data model of the Entity is as follows: 1. Develop conceptual data models (see DM.5) to document high-level ideas and ensure understanding. This will need input from business users who are familiar with the processes and functions within the Entity, and business analyst expertise to conduct interviews and produce the documentation. Profiles identified in conceptual data modelling are ideal candidates for the Entity's master profiles (see DM.7). 2. Develop logical data models (see DM.8) that map concepts to specific business units, functions and processes, independent of physical system implementations, linking the logical data models to the conceptual data models. This will need business analysts, business users and systems analysts to collaborate in order to document the idealised, system independent view of the data. 3. Develop physical data models (see DM.9) that document the specific implemented information systems, referencing the logical data models where appropriate. These will require systems analysts and database designers to model the structure and data types within the data stores themselves. Enterprise modelling will concentrate more on step 1 and 2, while information system modelling will concentrate more on steps 2 and 3.		R
Control Version History			
1.0			
Control Dependencies	DG.6 Capability Audit		
References	Common Warehouse Metamodel (CWM) (OMG, 2003) DMBOK (Mosley and Brackett, 2010)		

DM.2	Modelling Artefacts			Version	1
				Suggested Priority	2
Control Standards	The Entity shall generate modelling artefacts using diagrams, notations and documents appropriate to the audience				
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐	

Control Specification		M/R
DM.2.1	The Entity shall develop Data Models at the Conceptual (See DM.5), Logical (See DM.8) and Physical level (See DM.9), with references between them, allowing physical information systems to be mapped to logical models and at a higher conceptual level.	M
DM.2.2	The Entity shall use UML diagrams as the primary modelling notation throughout the software development lifecycle. Exceptions to the UML modelling standard shall be documented and submitted for authorisation by the Data Governance Board. Data modelling primarily uses structural diagrams, such as Class Diagrams, Entity Relationship Diagrams, Component Diagrams and Deployment Diagrams.	M
DM.2.3	The Entity shall use models best suited to communication with business stakeholders. UML diagrams and notation are often too technical for such purposes, and more common tools such as text-based documents, presentation slides and spreadsheets can often be more appropriate media for communicating data model concepts. The Data Governance Board shall inform the development of guidance to ensure appropriate and effective communication to its departments and stakeholders.	M
DM.2.4	The Entity shall use Entity-Relationship diagrams and Class Diagrams to document the structure and relationships of data objects at a conceptual, logical and physical level.	M
DM.2.5	The Entity shall use Data Flow Diagrams to model the movement of data within and between systems, focusing in particular on data that forms part of the Entity's master profiles. The following shall be identified and captured for all types of data flows: • The point where data is captured • Actions that transform and/or aggregate data • Points where data is exported (automatic or manual) • Service end points that emit master and common profiles	M
DM.2.6	Very large models (models with more than 200 tables or other descriptive artefacts) are inherently difficult to read. Large data models should be subdivided into smaller subject area-based models, and aggregated in a higher level model to maintain clarity. Data models should fulfil the purpose of aiding understanding.	M
DM.2.7	Data models shall clearly indicate and differentiate aspects that are current, and those that are not yet implemented.	M
DM.2.8	The Entity shall ensure that the following rules are adhered to when designing new conceptual data models: • Data objects are represented by nouns • Data relationships are represented by verbs The Entity shall ensure that the following rules are adhered to when designing new logical data models: • The appropriate data type shall be used for attributes within tables. This shall take into account performance, storage, and data requirements. Where a String or other variable character data type is used, consideration must have first been given for more appropriate data types The Entity shall ensure that the following rules are adhered to when designing new physical data models: • Primary keys shall be numeric. Where there is not a suitable numeric candidate key, a surrogate key in the form of an auto-numbering key shall be used • Reference data tables shall have a numeric primary key (likewise, tables that use reference data tables shall use the reference table's numeric primary key in the foreign key relationship) • Reference data tables will have, at a minimum, a numeric primary key and a code value represented as a string. Additional payload information (such as textual descriptions) may also exist as reference data (See RM.2.3) • Physical data types that have a length or precision specifier shall have an appropriate length or precision specified, and not left to the default value	M
DM.2.9	Where the Entity identifies duplication of datasets across the enterprise, or where datasets that are full or partially owned by another Entity are used by an information system, the data model should indicate the master /slave/federation rules between the duplicate datasets. This should identify which of the Entity's datasets are managed in one system (master) and propagated to other systems, which are managed externally (slave), and which are managed across multiple systems (federated).	M
DM.2.10	Data modelling artefacts shall form part of the Entity's mandatory system design and architecture documentation	M
DM.2.11	Data modelling artefacts (eg Entity Relationship Diagrams and Data Flow Diagrams) shall be produced equally for structured and unstructured data (See DM.10)	M
DM.2.12	The Entity shall publish data models for reference and re-use within the Entity. Data Architect roles shall be responsible for evaluating other pre-existing data models, and for aligning or re-using data models for new information systems where possible. Where this is not possible, justification shall be given in the system design, and approved by the Data Governance Board.	R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.1 Implement Tools and Methods
References	DMBOK (Mosley and Brackett, 2010)

DM.3	Business Glossary and Data Dictionary	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop a business glossary and a technical data dictionary to provide understanding of terms across the organisation		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DM.3.1	The Entity shall capture and define business terms for data object, attributes, relationships and values that have contextual business meaning. For example, a data object – such as a 'Citizen' – should have a single definition across the Entity. Although not all the attributes may be used by all parts of the Entity, where attributes of a 'Citizen' object are used, they should preserve consistency of meaning. A relationship between two data objects – such as the 'access' relationship between 'Citizen' and 'Service' objects – shall be defined and consistently used across the Entity. Examples of 'contextual values' might include (though not be limited to) a set of values used to indicate state (eg 'Active', 'Inactive' or 'Pending', 'Approved' and 'Rejected'). These values represent reference data, and shall be defined to ensure consistent use in the context of a data attribute within a given data object. Business definitions shall be stored within the business glossary portion of the Entity's Data Catalogue.	M
DM.3.2	The Entity shall produce technical definitions for each term within the business glossary for all information systems under its ownership. These definitions shall be developed to aid data integration and development projects that cover multiple systems. Technical definitions shall take input from logical and physical models (such as attribute types), but may also include technical validations in the form of state diagrams, flow charts, regular expressions, and other documentation as required. Technical definitions shall be populated within the data dictionary of the Entity's Data Catalogue.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DC.3 Data Catalogue Population DC.4 Data Catalogue Usage DM.1 Implement Tools and Methods
References	DMBOK (Mosley and Brackett, 2010)

DM.4	Data Model Metadata	Version	1
		Suggested Priority	2
Control Standards	The Entity shall ensure data models contain sufficient metadata to allow traceability and re-use		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		M/R
DM.4.1	The Entity shall maintain the following minimum data model metadata: • Model Identifier - in the form [Entity Initials]-[Reference Number]-[VERSION] For example: ADSIC-123-V1.0 would be Version 1.0 of model 123 for ADSIC. • Responsibility Assignment – Responsible, Accountable, Consulted, Informed • Published Status – Draft, Published • Change History – including dates, authors and descriptions	M
DM.4.2	The Entity shall maintain metadata to capture the following information about a data model: • Traceability links – where a number of data models are produced to show different views of the same subject area (for example, a logical and physical model), annotations should be used to indicate that other views exist. Links should be made by reference to the Model Identifiers. • Department or other lower level identifier – the Reference Number element of the model identifier does not need to be sequential. This allows the Entity to pre-assign numbers to different subject areas eg the model reference number '3nnnn' could identify financial data models, and '4nnnn' could identify HR data models, etc	R
DM.4.3	The Entity shall maintain other such metadata for its data models that is appropriate to its requirements. The metadata set shall be evaluated by the Data Governance Board, and issued – along with a guide to usage – to staff responsible for maintaining or using data models.	M
DM.4.4	Data models shall be stored in a suitable version controlled repository. A number of options are available, listed in order of recommendation: • Version control repository built into data model tooling • External version control repository or document management system that supports versioning • Version control through file system structure (this should only be used as an interim solution)	R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.2 Modelling Artefacts
References	DMBOK (Mosley and Brackett, 2010)

DM.5	Enterprise Data Model	Version	1
		Suggested Priority	1
Control Standards	The Entity shall maintain an Enterprise Data Model (EDM) comprising Conceptual, Logical and Physical Data Models across the Entity's master data and systems		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DM.5.1	The Entity shall develop an enterprise-wide data model, taking an organisation-wide view of all data that is central to the Entity's core business functions. The enterprise data model represents a key aspect of the baseline and target enterprise data architectures (See Data Architecture).		M
DM.5.2	The Data Governance Board shall maintain oversight and approval of enterprise data models through the Governance Checkpoint Process. The Data Governance Board shall socialise the enterprise data model through working groups to facilitate sharing with other Entities.		M
DM.5.3	When developing new data models for system implementations, the Entity shall ensure alignment with the Entity's Enterprise Data Model. Conceptual, logical and physical data models shall show alignment to the Entity's master profiles and the common profiles in the government Data Catalogue.		M
DM.5.4	The Entity shall align their Enterprise Data Model with government-wide data models as they emerge.		
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DM.1 Implement Tools and Methods DM.2 Modelling Artefacts DM.3 Business Glossary and Data Dictionary DM.4 Data Model Metadata DM.6 Conceptual Data Models		
References	DMBOK (Mosley and Brackett, 2010)		

DM.6	Conceptual Data Models	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop and maintain Conceptual Data Models (CDM) to describe high-level data within and across systems		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DM.6.1	The Entity shall develop conceptual data models to support the architecture, development and operational processes for its data. Conceptual data models shall be required as part of the system development lifecycle, and provided to the Data Governance Board through the Governance Checkpoint Process.		M
DM.6.2	Techniques to develop conceptual data models shall include, but are not limited to: • Interviewing stakeholders, or otherwise undertaking business functional analysis and requirements gathering to understand all relevant business concepts and requirements • Identifying candidate data profiles (typically the 'nouns') related to business processes, and capturing associations between these profiles • Combining candidate data profiles – as appropriate – into master data profiles, transactional data profiles and reference data profiles, and modelling the high level relationships between the data profiles		M
DM.6.3	Conceptual data modelling shall be performed at a system level (or group of information systems with similar concerns), or as part of Enterprise Data Modelling. Care must be taken to identify the view of the data being modelled (system or enterprise). For example, a customer has an order delivered by a courier. 'Customer' is a master profile, while 'Order' represents transactional data. Categorisation of the 'Courier' profile is more ambiguous, and varies depending on how the data needs to be viewed. In an Enterprise Data Model, 'Courier' could be considered reference data, as it is not core to the business functions. However, within a system data model for a Supplier Management System, a 'Courier' is likely to be a master profile (as an extension of 'Supplier').		M
DM.6.4	Conceptual data models shall be used to provide documentation to support development of logical data models, change requests, impact assessments, and/or gap analyses between baseline and target state requirements.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DM.1 Implement Tools and Methods DM.2 Modelling Artefacts DM.3 Business Glossary and Data Dictionary DM.4 Data Model Metadata		
References	DMBOK (Mosley and Brackett, 2010)		

DM.7	Master Profiles	Version	1
		Suggested Priority	1
Control Standards	The Entity shall define, create, and maintain data models for master profiles applicable to their line of business		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DM.7.1	The Entity shall identify and model all master profiles, and the relationships that exist between them. Master profiles comprise the data model, relationships, validations and descriptions of the data that is core to the Entity's line of business. For example, an Entity that provides a service to citizens is likely to include both 'Citizen' and 'Service' as master profiles. A master profile may have a complex structure eg a 'Citizen' profile may include family relationships, multiple contact details, and the history of name changes.	M
DM.7.2	Master profiles shall be documented as part of the Entity's activities to populate the Data Catalogue (see Data Catalogue Standards), both at a conceptual and logical level. Master profiles shall form part of the Entity's enterprise data model.	M
DM.7.3	Each system that physically contains master profile data shall have its data modelled at conceptual, logical and physical levels.	M
DM.7.4	Entity master profiles shall be made available to ADSIC, upon request, to facilitate the development of government-wide common profiles. The Entity shall align their local profiles with government-wide common profiles as they emerge, as appropriate.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.3 Business Glossary and Data Dictionary DM.5 Enterprise Data Model DM.6 Conceptual Data Models	
References	DMBOK (Mosley and Brackett, 2010)	

DM.8	Logical Data Model	Version	1
		Suggested Priority	2
Control Standards	The Entity shall develop and maintain Logical Data Models (LDM) for its information systems		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DM.8.1	The Entity shall develop logical data models that describe the data attributes and the relationships rules between the profiles described in the conceptual data model.	M
DM.8.2	The logical modelling of relationships between profiles shall describe referential integrity and normalisation concerns, unless the design relates to multi-dimensional information systems, such as data warehouses. Where data is de-normalised for performance or other reasons, the Entity shall ensure that this is documented, justified and approved by the Data Governance Board via the Governance Checkpoint Process.	M
DM.8.3	Logical data models shall be independent of technical implementation details. Although tables may be used to represent profiles in a logical model, the physical design might translate into something other than a relational database. Emerging technologies, such as 'No SQL' key/value stores, columnar databases and graph databases may be more appropriate physical data repositories (though careful evaluation, consideration and justification should be given when choosing these technologies over more traditional patterns). For example, a text string representing a Name attribute should not identify a physical data type of String[50]. Instead, this attribute should be defined by a logical data type, such as NameString. Business rules should be associated with NameString, constraining the type to a string, and the maximum length to 50 characters.	M
DM.8.4	Logical data models shall be used to provide documentation to support development of the physical data model, change requests, impact assessments, and/or gap analyses between baseline and target state requirements. The Entity's software development lifecycle shall reflect the requirement to develop and maintain logical data models. Logical data models shall be provided to the Data Governance Board as part of its Governance Checkpoint Process.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.1 Implement Tools and Methods DM.2 Modelling Artefacts DM.3 Business Glossary and Data Dictionary DM.4 Data Model Metadata	
References	DMBOK (Mosley and Brackett, 2010)	

DM.9	Physical Data Model	Version	1
		Suggested Priority	2
Control Standards	The Entity shall develop and maintain Physical Data Models (PDM) for its information systems		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DM.9.1	The Entity shall develop physical data models for system designs and architectures that are based on the appropriate logical data models. A physical data model provides the detailed technical implementation specifications that represent the application and/or data repository perspectives of the data.	M
DM.9.2	A physical data model shall be used to support technical implementation and system operational functions. For example, a SQL query should be written with reference to the physical data model. Physical data models shall be provided to the Data Governance Board as part of its Governance Checkpoint Process.	M
DM.9.3	The Entity shall provide a mapping between the logical data model and the resulting physical design to describe the implementation decisions involved. In the case of relational database systems, the physical data model might explicitly specify configuration details that exploit the capabilities of the particular relational database management system toolset employed (eg to derive performance optimisations, enforce security requirements, or to take advantage of embedded convenience functions, etc). For other types of data store (eg 'No SQL' or graph), the physical data model is likely to be significantly different from the logical model in terms of structure. It is important to highlight any dependencies that emerge as a result of using the embedded features of a toolset.	R
DM.9.4	The Entity should reverse engineer data models from existing supported information systems in order to support baselining data architecture. Physical data models should be linked back to their logical counterparts. Reverse-engineered data models are – by their nature – physical models, and can provide value in contexts such as system support, system development and technical data manipulation tasks undertaken by Data Stewards. Such models are not a substitute for conceptual and logical data models; if reverse engineering is used to assist data analysis and modelling, the resulting information must be considered for inclusion within the appropriate conceptual and logical data models.	R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.1 Implement Tools and Methods DM.2 Modelling Artefacts DM.3 Business Glossary and Data Dictionary DM.4 Data Model Metadata
References	DMBOK (Mosley and Brackett, 2010)

DM.10	Unstructured Data	Version	1
		Suggested Priority	2
Control Standards	The Entity shall prefer structured data over unstructured data and align with the Unstructured Information Management Architecture (UIMA) standards		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DM.10.1	The Entity shall model unstructured data that is linked to structured data through the business terms and logical concepts that are represented by the unstructured data. For example, modelling the concepts expressed in a document that is linked to a Citizen record, such as a medical report or education report.	M
DM.10.2	Semi-structured data (eg. data without a pre-defined schema) or unstructured data (eg. free text, images, audio, video), shall be modelled to document the: • Entities mandatory requirements of the data captured • Metadata that describes the concepts contained within the unstructured data • Associated structured identifying data that may be captured along with unstructured data For example, the mandatory requirements of ID photos of citizens could be that they should contain an image of the full, unobscured face, and metadata, such as the dimensions and resolution of the image. Associated structured identifying data may include the Emirates ID and date of the image. These shall be modelled at a conceptual and logical level.	M
DM.10.3	The Entity shall choose conversion of semi-structured and unstructured data into a structured form through transformation or analytical conversion techniques in order to formally document and model unstructured and semi-structured data.	M
DM.10.4	When attempting to convert unstructured data into a structured form of data, the Entity shall align its processes with the Unstructured Information Management Architecture (UIMA) in order to perform analysis on unstructured artefacts, develop and model artefact metadata.	M
DM.10.5	Unstructured content lifecycle shall be governed through appropriate workflows (see DCM.2).	M
DM.10.6	The Entity shall produce Data Flow Diagrams and Entity Relationship Diagrams for unstructured data. Data Flow Diagrams shall show the flow of unstructured information (and associated metadata and identifying data) between systems. Entity Relationship Diagrams shall show the relationship between the unstructured information concepts and structured identifying data, and the relationships between different unstructured information concepts.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.1 Implement Tools and Methods DM.2 Modelling Artefacts DM.3 Business Glossary and Data Dictionary DM.4 Data Model Metadata
References	Unstructured Information Management Architecture (OASIS, 2009)

14.5 DESCRIBED: Data Architecture

DA.1	Architecture Methodology		Version	1
			Suggested Priority	1
Control Standards	The Entity shall use the defined architecture framework and methodologies in order to produce the required data architecture deliverables within the Governance Checkpoint Process			
Control Type	Directive ☑	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		M/R
DA.1.1	The Entity shall develop data architecture within an Enterprise Architecture Framework, specifically The Open Group Architecture Framework (TOGAF). The phases within TOGAF shall be followed, with the Data Governance Board performing architecture reviews at the appropriate governance checkpoints. Enterprise Architecture shall align with business modelling processes and frameworks within the Entity. The Data Governance Board shall determine the required architecture deliverables specific to each governance checkpoint. The Entity shall develop data architectures at the system and enterprise level. Enterprise data architecture covers the business functions and concepts across the Entity as a whole. System level architectures relate to technology systems, and are specific to a single application group of applications within a business function. The high-level data architecture development process is as follows: • System baseline data architectures, describing the architecture of information systems containing data • Enterprise baseline data architecture, taking input from the key system baseline architectures • Enterprise target data architecture, demonstrating the desired architectural state across the Entity at some point in the future • Target data architecture roadmap, designed to fill the gaps between the baseline and target enterprise architectures • System target data architecture, as influenced by the roadmap in order to fill the gaps System architectures are likely to be evolving during this process, and the Entity should plan to maintain architectures as part of the software development lifecycle, and validated as part of the Governance Checkpoint Process.	M
DA.1.2	The Entity shall develop appropriate data architecture deliverables for production at the appropriate governance checkpoints. Deliverables shall be of appropriate detail for the audience who will use them. Data architecture deliverables include, but are not limited to: • Enterprise Data Model – this is a combination of the Entitiy's Conceptual Data Models, Logical Data Models and Physical Data Models describing the data its relationships that are core to the organisations function • Conceptual Data Model – showing the high level conceptual relationships and themes within the data; this is ideal for business users to understand • Logical Data Model – showing the system independent tables, fields and relationships; this can be used to aid development discussions • Physical Data Model – showing the specific implementation details; this is used to implement and support systems, and to understand technical change • Data Flow Diagrams – showing how data flows within and between systems; these can exist at multiple levels of detail • Component model – showing the technology components that make up the data architecture eg MDM/RDM, ESB, ETL tooling, and how they relate to specific applications or technology systems • Data profile/business function matrix – describing the business functions that use the data profiles • Data profile/business requirements matrix – describing the requirements that are met by the data profiles • Data lifecycle model – showing the lifecycle of data profiles (capture, management, transformation, archival, disposal) within the systems; some data profiles may be more stable or long lived than others • Data security compliance design – showing key security touch points (see Data Security and Privacy standards) • Data quality compliance design – showing key data quality initiatives, such as validation and cleanse services (See Data Quality) • Data model change process – showing the change process required in order to change data profiles Where a deliverable is deemed to be not required, justification shall be given. The data dictionary and business glossary defined in DM2 shall be referenced to ensure consistency of terminology in architecture development. These data architecture standards apply equally to all data domains within this standards document; other data domains may have more specific requirements that are detailed within the standards for that domain.	M

DA.1.3	Data Architecture deliverables shall be produced for all domains of the Data Management Programme including, but not limited to: • Metadata, data dictionary, business glossary and Data Catalogue systems • Data quality tooling including MDM and RDM, data profiling and cleansing • Data security and privacy systems • Open data management systems • Document and content management, or workflow systems • Systems for extract, transform, load (where they do not form an architectural component of another system) • Data warehouse, business intelligence and analytics systems • Line-of-business management systems, such as ERP, CRM, Spatial Data, Statistical management, and other specialist information systems appropriate to the Entity • Generic business management systems, such as HR, facilities management, and project management	M
DA.1.4	The Entity shall classify architectural elements according to the following categories: • Emerging – components that are a yet to be proven in a live environment; these components are likely to require proof of concept development, or collaboration through government working groups in order to assess suitability • Current – suitable components that are in development or deployment • Strategic – components that are expected to be available in the medium term eg big data technologies, mobile apps, or other components that are anticipated to provide strategic advantage to the Entity's operation. It is likely that some 'Strategic' components are also classified as 'Emerging' • Retirement – components that no longer help the Entity meet its strategic goals, and that are due to be decommissioned, replaced or archived	M
DA.1.5	The Entity shall use specialist data architecture standards drawn from centres of excellence within the Abu Dhabi Government. These include: • Statistical Data Standards • Geospatial Data Standards	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DM.1 Implement Tools and Methods DM.2 Modelling Artefacts	
References	DMBOK (Mosley and Brackett, 2010) The Open Group Application Framework (TOGAF) (Open Group, 2014)	

DA.2	**Baseline Data Architecture**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop and maintain a baseline data architecture, both for information systems and components, and at an overarching enterprise level		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DA.2.1	The Entity shall develop baseline data architectures for information systems and components under their control, and a baseline enterprise data architecture across all key systems. The Data Manager – acting on behalf of the Data Governance Board – shall develop and execute a plan to ensure full coverage of information systems that shall include: • Initial baseline data architecture production of all information systems controlled and maintained by the Entity • Baseline Enterprise Data Architecture, covering the high-level architectural view across information systems that support the key business functions of the Entity, including information systems not directly under the Entity's control (such as those hosted and managed by third parties, partners, other Entities or centrally run within the Abu Dhabi Government). Key information systems are those systems that include touch points with the Entity's master profiles (as defined by DM.2) • Baseline data architecture maintenance at the appropriate data governance checkpoints, for system-level data architectures and enterprise data architectures		M
DA.2.2	Development of baseline data architecture deliverables shall include consideration of the following elements: • The business and technical requirements that the data architecture supports, and those that are not currently supported by the data architecture • Identification of technical data architecture themes (for example, service-based/batch processing/data silos/data integration) • Constraints, where known, that have been placed upon the baseline data architecture; these may include factors such as licencing, legal, technical, training constraints, or others		M
DA.2.3	System-level baseline data architecture shall be presented as part of any system construction, change, upgrade, replacement or retirement. The baseline data architecture, detailing the current state of the information systems in place, shall be used to enable the discussion and validation of any target data architecture or roadmap presented, and ensure that the target architecture fulfils the requirements gap between the baseline and target architectures. These shall be reviewed at the appropriate points in the system development lifecycle by the Data Governance Board, as part of the Governance Checkpoint Process.		M

DA.2.4	Baseline data architectures are a continuously maintained set of deliverables, and shall be versioned and updated at the appropriate governance checkpoints. For example, when a system goes live, its target data architecture becomes the new baseline data architecture for that system (assuming the implementation met the target). This shall trigger an update of the baseline enterprise data architecture to reflect the system's new baseline data architecture.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.5 Enterprise Data Model DA.1 Architecture Methodology	
References	DMBOK (Mosley and Brackett, 2010) The Open Group Application Framework (TOGAF) (Open Group, 2014)	

DA.3	**Target Data Architecture**		**Version**	1
			Suggested Priority	1
Control Standards	The Entity shall develop and maintain a target data architecture both for information systems and components, and at an overarching enterprise level			
Control Type	Directive ☑	Preventive ☑	Detective ☐	Corrective ☐
Control Specification				**M/R**
DA.3.1	The Entity shall produce a target enterprise data architecture. The completion of a baseline data architecture is not a prerequisite for development of a target enterprise data architecture, but may be informed by it. The Data Governance Board should give consideration and justification to the appropriate time to produce the target enterprise data architecture. The target enterprise data architecture is expected to be a continuously evolving set of deliverables, reacting to external factors such as technology changes, business requirements and external factors. The Data Governance Board shall ensure that the target enterprise data architecture is maintained as information systems and components are implemented, revised or decommissioned.			M
DA.3.2	The Entity shall produce target data architectures for information systems as they go through natural change cycles. A system's target data architecture shall be required for the appropriate phase in the Governance Checkpoint Process.			M

DA.3.3	A target data architecture (system or enterprise level) shall: • Address the gaps between the business and technology requirements and the baseline architecture • Encourage data integration across the Entity between information systems and services • Seek removal of duplication in terminology (eg a single definition of 'customer' across multiple systems) • Seek to remove duplication of data processes • Seek alignment of reference and master data across the Entity's systems • Align with emerging government-wide technology platforms • Integrate with government-wide reference and master data services and standards as they emerge • Show re-use of data and system architectures both within the Entity itself and through collaboration with other Entities • Be influenced by the data management requirements emerging from the data quality, data security, data privacy, data integration and interoperability, and data storage domains, both within the Entity and as delivered from central government programmes	M
DA.3.4	The target data architecture shall influence technology and data requirements for system changes, in addition to the standard business and quality (non-functional) requirements.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.6 Enterprise Data Model DA.1 Architecture Methodology	
References	DMBOK (Mosley and Brackett, 2010) The Open Group Application Framework (TOGAF) (Open Group, 2014)	

DA.4	**Data Architecture Roadmap**		**Version**	1
			Suggested Priority	1
Control Standards	The Entity shall perform an architectural gap analysis, and develop, maintain and follow an architecture roadmap			
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐
Control Specification				**M/R**
DA.4.1	The Entity shall identify the gaps between the baseline enterprise data architecture and the target enterprise data architecture. This gap analysis shall include detail of the: • Business data requirements that are not currently being met • Technical data components missing between the baseline and target • Capability gaps (in terms of roles, skills, tools and training)			M

DA.4.2	The gap analysis shall be used to develop a roadmap that moves the baseline enterprise data architecture towards the target enterprise data architecture. As both the baseline and target enterprise data architectures are constantly evolving, the roadmap is also required to undergo periodic review by the Data Governance Board so that it is aligned with the baseline and target enterprise data architectures. The roadmap shall show the timeline required to implement the components and systems, provide budgetary estimates and capabilities required by the Entity, in alignment with business priorities. The roadmap shall indicate the priority and order by which the Entity changes, upgrades, replaces or retires components and systems. However, this must be flexible enough to react to business priorities. The Data Governance Board shall evaluate justifications for changes of priority or requests in exception to the roadmap.	M
DA.4.3	The Entity shall follow the roadmap when information systems and components are requested, developed, implemented, renewed or retired. This shall require development of a system or component-specific target data architecture that shows alignment with the enterprise target data architecture, and shall be validated through the Governance Checkpoint Process. Where these data architectures are not in alignment with the target enterprise data architecture, the Data Governance Board shall seek justification for non-alignment, and shall determine what – of the system, component, target enterprise architecture and/or roadmap – should change.	M
DA.4.4	The Entity shall annually report upon the effectiveness of the roadmap implementation, by identifying gaps between the starting and ending baseline enterprise data architectures. The gaps between the baseline enterprise data architectures should align with the roadmap for the same time period reported upon. Where there are significant differences, root cause should be identified and presented to the Data Governance Board in order to demonstrate lessons that have been learned.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.8 Logical Data Model DM.9 Physical Data Model DA.2 Baseline Data Architecture DA.3 Target Data Architecture	
References	DMBOK (Mosley and Brackett, 2010) The Open Group Application Framework (TOGAF) (Open Group, 2014)	

14.6 QUALITY: Data Quality

DQ.1	**Data Quality Plan**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop a plan for the rollout of a data quality initiative		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DQ.1.1	The Entity shall provide definitions of quality data. These definitions shall be used to determine whether data is of sufficient quality for the purposes of the Entity's business. Data quality definitions shall be stored in the Entity's business glossary (business audience) and data dictionary (technical audience). Definitions shall exist for: • Master profiles – the profiles used across the Entity's business, in key line-of-business systems, or across multiple departments and data silos (see Data Modelling domain) eg 'Citizen' profile in multiple systems • System profiles – profiles within single systems, silos or departments eg Project (in a Project management system) • Reference data – data that is effectively static within systems, subject to periodic refresh • Audit data – data stored log files, history tables and monitoring systems • Analytical data – data gathered through automated mechanisms, such as website user clicks, physical sensors (eg entry barriers), tracking metrics • Spatial data – geographical, address, geolocation or other location-based data • Metadata – metadata that is gathered about structured datasets, such as ownership, definitions, access rights (see Metadata domain) • Metadata annotating unstructured or semi-structured data. This may include metadata attached to images, audio recordings, video recordings (such as duration, dimensions, location, encoding), etc. Metadata attached to semi-structured data may include, for example, author, workflow steps and access permissions of documents, etc		M
DQ.1.2	Data quality definitions shall be mapped to business processes. This shall provide the capability to assess the impact of both high and low quality data on business processes. For example, a business process may include contacting a citizen. Where there is poor data quality in telephone number or address capture (such as the omission of a country, area or postal code), there may be a severe impact upon the business process. Accurate and timely capture of a telephone number enables the business process to continue.		M

DQ.1.3	Data quality definitions shall include – but are not limited to – the minimum measures of data quality for: • Validity – Describing what constitutes valid data. This will show how data validity is controlled and measured. This shall include a description of the business rules (expressed both as a text-based description, and technically eg as a regular expression) that enforce this validity. Data validity may include the range of acceptable values or combination of values across multiple attributes and tables. For example: a Citizen is valid if there is at least one Address marked active in the last year. • Timeliness – Describing the acceptable latency between data capture, use, transformation, reporting, and sharing. For example: The correct departments have access to Citizen data in order to process a service request with sufficient time to meet an SLA; mapping data changes over time as properties are constructed, so mapping data that is a year old may be less useful than mapping data that is two months' old. • Integrity – Describing how the integrity between different data sources is maintained both within and across and business functions. For example, using the Emirates ID across multiple information systems to uniquely identify a person, using a contact reference number across multiple systems, and enforcing validation through a master service. • Accuracy – Describing the acceptable margin of error against reality to support the intended purpose(s) of the data. For example, historical dates of Citizen access to a government service must be accurate to within +/- one week to support capacity planning. • Reliability – Determining the level of consistency and completeness required for the intended purpose(s) of the data. For example, telephone numbers are always captured in the same format to be consistent, and address records must contain the correct district in order to be considered complete. For each of these measures, the Entity shall: • Assess the impact on business processes for failing to reach the specified criteria • Determine whether there a business benefit as quality increases	M
DQ.1.4	The Entity shall define metadata in line with the data quality definitions in order to populate the Data Catalogue with data quality metadata for the datasets under its control. Data quality metadata should include a combination of both quantitative and qualitative measures. Some examples of quantitative measures include: • Percentage of data that is considered 'complete' • Number of data patterns identified in the data (such as phone number patterns) • Range of values for specific fields Some examples of qualitative measures include: • Results from user satisfaction surveys • Highlighted user issues The Entity shall define appropriate measures sufficient to describe the quality of the data being published. The metadata shall include the valid range of measures and values, and appropriate definitions where qualitative measures are used.	M
DQ.1.5	The Entity shall produce a data quality checklist, appropriate to the datasets under its control that will enable the Entity to audit its data in line with the Entity's data quality definitions.	M
DQ.1.6	The Entity shall develop a plan for a data quality audit, monitoring and maintenance. This shall include: • The quality of the Entity's master profiles • The quality of the datasets under the Entity's control • Data quality issues experienced by technical and business users This plan shall include the tools and techniques and roles required, and will draw upon the data quality checklist and definitions. The planned output shall be the data quality metadata and a set of data quality requirements (distilled from data quality issues identified by the audit and from users). Data quality roles shall include, but are not limited to: • Data Auditors – perform data quality audits and monitoring • Data Stewards – undertake data quality cleansing and management • Subject Matter Experts – provide the knowledge of the impact of high and low quality data Data quality tooling shall include, but is not limited to: • Data profiling – used for performing data set analysis to understand the range of values, relationships between and across datasets, completeness and other data quality metrics • Data cleansing – used to validate, match, merge, and enrich data within and across systems • Data quality issue logging – to record data quality issues and track workflow, and provide metrics to support data quality improvement The following tooling contributes to data quality initiatives: • Data Catalogue – to record data quality metadata • Master data management – can be used part of data cleansing initiative and/or to provide central data services with a single 'enterprise' view of master profiles • Reference data management – to provide structured management of reference data outside of specific systems, datasets or silos, typically across the Entity	M

	The Data Governance Board shall direct the strategic roadmap of the plan, by performing one or more of the following: • One-off data quality audit to ensure full coverage • Incremental data quality audit as part of checkpoint processes • Focused data quality audit by data and system category (eg strategic or critical systems first) The Data Governance Board shall document the justification for the choice	
DQ.1.7	The Entity shall ensure that business requirements for new information systems, systems undergoing change, or dataset extract or transformation include specific data quality requirements. In the unlikely case that there are no data quality requirements, this should be explicitly documented. Data quality requirements should be documented using the appropriate data quality metadata definitions. These requirements shall form the basis of internal data quality SLA, where data is shared internally, and contractual Service Level Agreements should be considered where data is shared externally.	M
DQ.1.8	The Entity shall ensure that data quality audits are included in the data Governance Checkpoint Process. This shall include: • A data quality audit within information systems undergoing change • Plans for maintaining or improving data quality (including data validation rules) • Documented data quality requirements and definitions The specific checkpoints where these are required shall be defined by the Data Governance Board. For example, data quality definitions for integrity in a system may be required at a budgetary checkpoint, whereas the data quality requirements for accuracy and reliability may be required to be provided at a design checkpoint. A system undergoing change may require that a data quality audit be completed as part of the development of the baseline data architecture, with plans provided to improve data quality provided as part of the target architecture.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DM.7 Master Profiles DA.4 Data Architecture Roadmap	
References	DMBOK (Mosley and Brackett, 2010) Good Basic Data For Everyone (Agency of Digitalisation, 2012) ISO/TS 8000 Data Quality (ISO, 2009-2011)	

DQ.2	**Data Quality Audit**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall perform a data quality audit of data, information systems and services under their control		
Control Type	Directive ☐	Preventive ☐	Detective ☑	Corrective ☐
Control Specification			**M/R**
DQ.2.1	The Entity shall ensure that its master profiles (as identified in Data Modelling standards) are audited for data quality at three-monthly intervals across all data sources where they are contained. Where data quality does not align across data sources, the Entity shall identify discrepancies in master profile data quality in the different data sources, and determine the root cause for the discrepancy. Where data quality does not align with the stated data quality definitions for master profiles, the Entity shall identify discrepancies between master profile data quality and the stated data quality definitions for the master profiles, and determine the root cause for the discrepancy. Once the root cause of the discrepancy is known and understood, the Data Governance Board shall determine if corrective action needs to be taken.		M
DQ.2.2	The Entity shall define appropriate time intervals to audit data types that are not part of the common profiles (as defined in DM2). Once the root cause of the discrepancy is known and understood, the Data Governance Board shall determine if corrective action needs to be taken.		M
DQ.2.3	The Entity shall perform spot checks on data quality of third party data to ensure that the data meets service level agreements from the data supplier. Where there are no service level agreements from the data supplier, the Entity shall develop its data quality requirements for the third party data in order to monitor data being supplied. The Entity should share these data quality requirements with the data supplier. A data supplier could be another government Entity, business partner, customer, service provider or other stakeholder.		M
DQ.2.4	The Entity shall use data profiling tools systematically to audit the data. Data profiling tools shall have the following analysis capabilities as a minimum: • Structured data column analysis – analysing columns for data patterns, value ranges, redundancy and duplication • Data structure independent integrity analysis – determining relationships between tables and datasets based upon data alone • Pattern definition and identification – for example, standard telephone patterns • Reporting generation – to highlight key areas for concern • Comparison of data audits over time to detect significant changes in quality		M
DQ.2.5	The Entity shall store the data quality measures gathered during the data quality audit as metadata in the Data Catalogue.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DQ.1 Data Quality Plan		
References	DMBOK (Mosley and Brackett, 2010) ISO/TS 8000 Data Quality (ISO, 2009-2011)		

DQ.3	Data Quality Uplift			Version	1
				Suggested Priority	2
Control Standards	The Entity shall perform monitoring and cleansing of data as required by the plan				
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☑	
Control Specification					**M/R**
DQ.3.1	The Entity shall identify the gaps between the stated data quality definitions and the audited data quality measures, and execute a data cleansing initiative to improve data quality. Data quality improvement initiatives shall be determined by the Data Governance Board, and may be carried out: • On a system-by-system basis • By master profile or other data type, across multiple systems • According to business benefit Strategies to improve quality will require tools and expertise to understand the data structures and business context. Appropriate tools may include: • Master data management – with matching, merging rules and data stewardship interfaces • Reference data management – to provide centralised reference data mapping and matching • Extract Transform Load – to perform the movement of data between systems • Cleansing tools – to form the knowledge base of cleansing rules and mappings • Third party services – for example: address cleansing, Emirates ID matching and enrichment				M
DQ.3.2	The Entity shall ensure that target data architectures serve to improve the data quality across information systems and services. Target data architectures should include appropriate components to monitor data quality, provide common validation across systems, and perform data cleansing. Priority shall be given to the master profiles, and extended to other data types as defined by the Data Governance Board.				M
DQ.3.3	An end-to-end data cleansing process is detailed below; however, data cleansing is typically an iterative process that shall be repeated to improve and maintain data quality as business and technical requirements change. 1. Extract data from operational data sources for profiling Data profiling tools perform complex analysis on data, and to perform this analysis directly against live data sources is not recommended. Data extraction may be performed using separate ETL tools, or may be a capability of the data profiling tools themselves. 2. Perform data profiling analysis This shall occur as part of a regular data audit process, enabling data quality issues to be identified. The output of data profiling shall be used to build the technical knowledge base for data cleansing.				M
	3. Build cleansing knowledge base for each data profile The cleansing knowledge base includes mappings and correction rules that may be automatically applied. For example, The range of mobile phone formats identified by data profiling may include (nnn) nnn nnnn, +nnn nnnnnnn, nnn nnn-nnnn. The knowledge base should include the rules for converting these formats into a single format. A knowledge base may include the ability query external data services, such as telephone number validation, reference data management systems, and data enriching systems, such as an Emirates ID service to provide more Citizen profile data. Physically, the knowledge base may be one or more systems, and may include master data management tools, reference data management tools, and vendor specific data cleansing solutions. 4. Automated cleansing using knowledge base Automated cleansing may be performed in batch against live systems, typically out of hours, and subject to sufficient testing. The size of the batch chosen should be determined by the smallest batch of data that can reasonably be completed within the time window allowed. The choice of records that form part of the each cleansed batch shall be defined, for example, through order of insertion, age based (newest/oldest) first, or most active records first. Automated cleansing can also be applied to data extracts; however, the plan to refresh the live data with the cleansed data must be considered carefully to avoid conflicts where the live data has since changed. 5. Interactive data cleansing Automatic matching will reject data that cannot be cleansed. The Data Steward shall use this rejected data to perform manual cleansing. The recording of cleansing decisions should be fed back into the knowledge base to improve the quality of automated matching. This iterative cycle will initially occur often during the development of the knowledge base. 6. Automated cleansing services Automated cleansing services can then be delivered as interactive services, allowing information systems to have data validated and cleansed at the point of data entry. For example, a CRM system for capturing a citizen's name and address may make a service request to the automated cleansing service to enrich the address, validate the telephone number, and match the individual citizen with their other records stored in datasets elsewhere within the Entity.				

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DA.4 Data Architecture Roadmap DQ.2 Data Quality Audit
References	DMBOK (Mosley and Brackett, 2010) ISO/TS 8000 Data Quality (ISO, 2009-2011) Data Warehousing, The Keys for a Successful Implementation (Pitney Bowes, 2010)

14.7 ACCESS: Data Security and Privacy

DSP.1	Information Security Standards	Version	1
		Suggested Priority	1
Control Standards	The Entity shall apply and show compliance with the approved Information Security Standards in the Abu Dhabi Governemnt to data managed by and for the Entity		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DSP.1.1	The Entity shall apply the latest version of the approved Information Security Standards in the Abu Dhabi Governemnt. These Standards shall take precedence over these Data Management Standards in the event of conflict. The Data Governance Board shall record conflict issues and the outcome of any decisions taken to resolve such conflicts.	M
DSP.1.2	The Entities data architecture, and the information systems and components that form that architecture, shall show alignment with approved Information Security Standards in the Abu Dhabi Governemnt. The Data Governance Board shall certify evidence of alignment with approved Information Security Standards in the Abu Dhabi Governemnt through the Governance Checkpoint Process. Information systems and components include, but are not limited to: • Data integration and interoperability components, formats, specifications • Line of business management systems, such as ERP, CRM, Spatial data • Back office systems, such as issue management, HR, facilities management • Data analysis systems, data stored in data warehouses, big data repositories or data made otherwise available through business intelligence tooling • Data quality tooling, such as Master and Reference Data Management, data profiling, data cleansing • Data and information systems managed and provided by third parties on behalf of the Entity	M
DSP.1.3	The Entity shall ensure that data proposed for release as Open Data (see Open Data standards) includes a statement demonstrating compliance with both the approved Information Security Standards in the Abu Dhabi Governemnt and Data Management Standards, and is presented to the Data Governance Board, which will ratify the decision to publish the data as Open Data.	M
DSP.1.4	The Entity shall extend the classification of systems to identify information systems that may be at risk of privacy breaches in accordance with the Entity's privacy policy (see DSP.2).	M
DSP.1.5	The Entity shall ensure compliance with the Payment Card Industry (PCI) Security Standards – through the Governance Checkpoint Process – for information systems that store or process credit card data.	R
DSP.1.6	The Entity shall ensure that cloud suppliers meet ISO/IEC 27017 Cloud Security Standards and ISO/IEC 27018 Handling of Personally Identifiable Information Standards as they become ratified by the International Standards Organisation.	R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit
References	Abu Dhabi Government Information Security Standards (2013) UAE Information Assurance Standards Data Security Standards (PCI Security Standards Council, 2013) ISO/IEC 27017 Cloud Security Standards (ISO, draft) ISO/ISC 27018 Handling of Personally Identifiable Information (ISO, draft)

DSP.2	Data Privacy Policy	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop a data privacy policy in line with current Abu Dhabi Government legislation with regards to privacy		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DSP.2.1	The Entity shall develop a privacy policy that aligns with current government privacy legislation. The privacy policy shall encompass the guidance within these Standards, with specific reference to the data within the Entity's line of business. The policy should by augmented with appropriate information and guidance. Consideration shall be given, where appropriate, to: • Structured, transactional data • Spatial, geographical or other location-based data • Data collected from sensors or other automated devices • Biometric data collected, stored, or otherwise used by the Entity • Surveillance data collected by the Entity, including audio/visual data and metadata gathered from monitoring and recording, such as phone record information • Data stored in other unstructured or semi-structured formats, such as reports, documents and images All these data formats have the ability to breach an individual's privacy if exposed to the wrong audience.	M
DSP.2.2	The privacy policy shall contain a public privacy statement that provides its service stakeholders with a clear and unambiguous description of the stakeholders' privacy rights, and the Entity's privacy obligations. The Entity shall ensure that its privacy policy remains in alignment with any policy that emerges from cross-government working groups.	M
DSP.2.3	Consideration (in consultation with appropriate legal experts) shall be given for the individual – about which data is gathered – to have the following minimum rights: • Have visibility of data that is held about them • Correct inaccuracies in data that is held about them • Request removal of data that is held about them, but is no longer relevant or applicable to the business of the Entity	R

DSP.2.4	Consideration (in consultation with appropriate legal experts) shall be given for the Entity to have the following minimum obligations to its stakeholders: • Clarify why personal data is needed, and how it will be used at the point of collection • Provide a mechanism for stakeholders to subscribe or opt out of activities that are not core to the Entity's business	R
DSP.2.5	The Entity shall produce and maintain privacy metadata for the Entity's master profiles. This shall clearly identify the profile attribute or combinations of attributes that contain private data. Privacy metadata shall be stored in the Data Catalogue.	M
DSP.2.6	The Entity's Open Data policy shall be in alignment with the Data Privacy policy. No data that could breach individual privacy shall be made open. Special attention shall be given to avoiding the so-called 'mosaic effect', which can occur when data across multiple datasets is disaggregated and combined in order to identify specific individuals.	M
DSP.2.7	The Entity shall develop an awareness programme for its data privacy policy, which shall be disseminated to all users of private data (both from business and technical areas) in order to remind the users of the Entity's obligations and users' personal responsibilities concerning data privacy.	M
Control Version History		
1.0		
Control Dependencies	DG.2 Data Management Policy DG.3 Data Management Programme	
References	Better Practice Guide for Big Data (Data Analytics Centre of Excellence, 2014) Government Privacy and Best Practices workshop (Department of Homeland Security, 2009) Privacy By Design, (2014) UAE Information Assurance Standards	

DSP.3	**Privacy By Design**		**Version**	1
			Suggested Priority	3
Control Standards	The Entity shall adopt the principles of 'Privacy by Design' into its data architecture and training programmes			
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐
Control Specification				**M/R**
DSP.3.1	The Entity shall adopt the principles of 'Privacy by Design'. The principles of 'Privacy by Design' are: • Proactive not Reactive – Anticipating privacy risks and addressing them before they occur • Privacy as the Default Setting – The individual does not have to perform any actions in order to safeguard their privacy • Privacy Embedded into the Design – Privacy is built into information systems and business processes rather than being added after the fact			R

	• Fully Functional – Accommodate all legitimate interests and requirements so as to avoid unnecessary trade-offs or compromises, such as privacy vs security • End-to-end Security (full protection across the data lifecycle) – Data privacy is respected from the point of data capture through to the data being archived or destroyed, or the process concluding • Visibility and Transparency – Ensuring that privacy within information systems and business processes is available for external audit, satisfying the needs of users and providers • Respect for User Privacy – Upholding the interests of both individuals and users within architectures and designs Using the principles of 'Privacy by Design' enables the Entity to identify privacy issues early, and reduce privacy risk and cost through corrective actions.	
DSP.3.2	The Entity shall produce training and awareness materials about the principles and goals of 'Privacy by Design' for delivery to the Entity's technical and business users responsible for designing information systems and processes.	R
DSP.3.3	The Entity shall identify any shortcomings concerning its existing data sources' compliance with the principles of 'Privacy by Design'. The Entity shall use the requirements from the gap analysis as an input into the Entity's target data architecture, both at the Enterprise level, and within specific information systems as necessary.	R
DSP.3.4	The Entity should use data governance checkpoints to validate alignment with the principles of 'Privacy by Design' when: • Building new information systems for accessing or storing accessing personal data • Designing data sharing initiatives • Using data for new purposes other than those originally intended	R
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DA.3 Target Data Architecture	
References	Privacy By Design, (2014)	

DSP.4	Privacy Management	Version	1
		Suggested Priority	3
Control Standards	The Entity shall operate a data privacy management workflow in line with the Entity's data privacy policy, to identify and manage privacy-related data issues and risks		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
DSP.4.1	The Entity shall develop a privacy management workflow that enables the Entity to identify, log, investigate and resolve data privacy-related issues in accordance with the Entity's own privacy policy. This workflow should include the ability to capture and investigate privacy issues identified both by internal users and external stakeholders, including steps for evidence gathering, post-incident analysis, reporting, and taking corrective action. This workflow shall be used to monitor the effectiveness of the implementation of the Entity's privacy policy, and as such, the Entity shall report privacy-related metrics to the appropriate cross-government working group.		M
DSP.4.2	The Entity shall ensure that there is a route for individuals to maintain/correct private data held about themselves. Such updates shall be incorporated into a data quality audit.		M
DSP.4.3	Where permitted by the Entity's privacy policy, the Entity shall respond within a reasonable amount of time (as determined by the Data Governance Board) to requests from an individual for disclosure of the data held about them by the Entity. These requests shall be monitored to ensure that they are actioned within the time targets established by the Data Governance Board.		M
DSP.4.4	The Entity shall evaluate requests for removal of data about an individual, as allowed by the Entity's privacy policy. The Entity shall establish a request evaluation process that balances business need for the data, and the privacy of the individual. Such requests should be handled internally by the Entity, though an appeal process should be available to individuals, and this may require cross-Entity collaboration. The Data Manager shall be the final arbiter.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DSP.3 Privacy By Design		
References	Better Practice Guide for Big Data (Data Analytics Centre of Excellence, 2014) DMBOK (Mosley and Brackett, 2010) Government Privacy and Best Practices workshop (Department of Homeland Security, 2009) Privacy By Design, (2014)		

DSP.5	Data System Protection	Version	1
		Suggested Priority	2
Control Standards	The Entity shall implement data security protection measures at a system level		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐
Control Specification			**M/R**
DSP.5.1	The Entity shall take measures to prevent data loss and data privacy breaches. Appropriate architectural components shall be considered to strengthen the protection of information systems that are susceptible to data loss or data privacy breaches (whether used in production or for development, test, or training purposes). These components can include: • Data-loss prevention tools and techniques – detect and block sensitive data from passing over the network using a combination of traffic analysis techniques, software agents, or 'air-gaps' to physically isolate networks • Database activity monitoring (DAM) tools – to audit all access and modification of data, and to provide alerts for exceptional data activity • Data discovery tools – to discover data that exists where it is uncontrolled eg database extracts on developer laptops The Data Governance Board shall consider the risk of data loss for each system under evaluation according to business value, sensitivity, and criticality of the data contained within that system. Any technical components implemented to mitigate data security and privacy risks shall be introduced into the appropriate target data architectures (at the system or enterprise level as appropriate).		M
DSP.5.2	The Entity shall ensure that data security and privacy requirements are appropriately observed for production information systems within test, development and training environments. Where a subset of production data is used in other environments, appropriate data masking technologies shall be used. Data Masking techniques include physically transforming, obfuscating or randomising data within datasets. Live data masking can be implemented using a role or permission-based service that transparently intercepts data in real-time – masking the data according to predefined rules, while maintaining the original underlying data. Consideration should be given to the requirement for data within test or training environments to preserve the characteristics of real 'Live' data (eg replacing phone numbers with asterisks would not represent a real-world situation and does not therefore represent optimal test data). Good quality masked data is highly dependent upon the quality of data being masked. In order to assist the masking rules or transformations to provide good quality masked data a data quality audit (see Data Quality standards) shall be performed against any system where data masking is being considered.		M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DA.3 Target Architecture DA.4 Data Architecture Roadmap DSP.1 Information Security Standards
References	DMBOK (Mosley and Brackett, 2010) Three Guiding Principles to improve Data Security and Compliance (IBM, 2012)

14.8 ACCESS: Data Storage

DS.1	**Baseline Data Storage Architecture**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall document the baseline data storage architecture of datasets, information systems and services under its control		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		**M/R**
DS.1.1	The Entity shall engage an infrastructure audit team familiar with platform utilisation metrics and the hardware and software configurations prevalent across the Entity.	M
DS.1.2	The Entity shall undertake a comprehensive audit of physical inventory both within the Data Centres and at any other site or location. The following fields shall be recorded for every system discovered: • Data Centre Location • Service/Application Name • Server Name • Server Type (Rack-mount, Blade or Tower) • Hardware Model • VMhost (if virtualised) • Computer Model • CPU (Type/Model, N CPUs, No Cores per CPU) • RAM (GB) • SAN Type (SATA, SSD, Flash) and Size (in GB) • Backup Type (Disk, Tape) and Size (in GB) • O/S Version • Power and Cooling requirements (Watts and BTUs) • Criticality to Business • Requires SAN (Y/N) • IP Addresses and MAC addresses • Current Redundancy Levels (Power, Network, CPU)	M
	• Status (delivered, commissioned, in use, decommissioned, dismounted) • Server Provisioning Date • Decommissioned Date or Planned Decommissioning Date • Server End Of Life Date (EOL) • Server End Of Support Date (EOS) • Application Owner • Notes	
DS.1.3	The Entity shall conduct a logical audit of network inventory to check against the physical inventory and ensure that all omissions and additions are accounted. • The Entity should use tools (eg Spiceworks, SolarWinds, HP Open Computers and Software Inventory Next Generation, etc) or an CMDB instance to perform this logical audit • All discrepancies between the physical audit and the logical audit must be accounted for – and a remediation plan executed – to bring the two into alignment	M
DS.1.4	The Entity shall conduct infrastructure utilisation audits on all of their information systems and servers to determine the actual loads across the usage scenarios. These audits shall (for both peak and baseline measures): • Record server CPU loads • Record server Memory loads • Record server disk IO loads • Record server Network IO loads • Record server availability • Power and Cooling loads (Watts, BTUs) • Record top processes for CPU loads • Record top processes for Memory loads • Record top processes for IO loads • Record top processes for Network loads • Track server utilisation for a minimum of 30 consecutive days • Track server utilisation for up to 90 days if application use cases indicate the need (eg quarterly billing)	M
DS.1.5	The Entity shall determine from the physical, logical and utilisation audits: • The capacity of current infrastructure • The precise current infrastructure utilisation • The infrastructure utilisation trends • The server consolidation ratio achievable • The capacity requirements for the next three to five years	M

DS.1.6	The Entity shall categorise their inventory in terms of business criticality and establish priority based on precedence. Criticality levels shall be determined by the business and the Data Owner and are used to classify the IT system from a business perspective based on the kind of loss risks evaluated (monetary or reputational), as follows: • Core Infrastructure – Information systems that must be functioning and are considered core components, which will need to be operational before other dependent systems can perform as they are intended (eg DNS and DHCP, AAA, and Active Directory) • Critical – Information systems that are critical to support Entity business operations; failure of these solutions will have a disastrous impact on operations (eg Core Application, ERP, CRM etc) • High – Information systems that are required to support primary Entity business operations. Failure of these systems will have a significant impact on operations (eg HRMS, Procurement etc) • Medium – Information systems that are important to Entity business operations; failure of these systems will have a small impact on operations (eg Email, Intranet Service etc) • Low – Information systems that improve Entity efficiency; failure of these systems will have negligible impact on operations (eg Wikis, Bulletin Boards) Once information systems have been classified, they can be prioritised in order of criticality to the business. Considerations should be given to prerequisites (for example, DNS and Active Directory should be rated above Email Servers, Relational Database Management Systems (RDBMS) might be required before the application layers, etc).	M
DS.1.7	The Entity shall classify all information systems in one of the portability categories: Legacy, Virtualise-able, Cloud-able. This will help the Entity to determine the suitability of an application of system for a chosen target architecture, and will assist in the determination of its suitability for migration.	M
DS.1.8	The Entity shall produce a migration list showing the migration targets, taking into consideration: • Portability • Criticality • Precedence	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DA.2 Baseline Data Architecture	
References	DMBOK (Mosley and Brackett, 2010)	

DS.2	**Target Data Storage Architecture**		**Version**	1
			Suggested Priority	1
Control Standards	The Entity shall develop and maintain a target data storage architecture			
Control Type	Directive ☑	Preventive ☑	Detective ☐	Corrective ☐
Control Specification				**M/R**
DS.2.1	The Entity shall engage an infrastructure Architecture team to determine a suitable target architecture for the Entity Data Centres.			M
DS.2.2	The Entity shall ensure that its target architecture reflects the latest flexible infrastructure capabilities eg Private Cloud, Virtualisation, Storage Virtualisation, Infrastructure-as-a-Service, Platform-as-a-Service, etc. One of the following models is preferred: • Infrastructure-as-a-Service (IaaS) This allows the consumer to provision processing, storage, networks, and other fundamental computing resources, and to deploy and run arbitrary software (including operating systems). The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and possibly limited control of selected networking components (eg Compute, VM, Firewalls, Load Balancers etc). • Platform-as-a-Service (PaaS) This allows the consumer to deploy onto the cloud infrastructure user-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (including network, servers, operating systems, or storage, or deploy OS and standard applications) but has control over the deployed applications, and possibly configuration settings for the application-hosting environment (eg OS, Standard Applications, SharePoint, Oracle DB, Oracle Apps, Web Servers, Applications Servers etc).			M

DS.2.3	The Entity shall determine the appropriate cloud deployment model to suit its requirements and the emerging data centre capabilities of the Abu Dhabi Government, as follows: • Private cloud The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (eg departments). It may be owned, managed and operated by the organisation, another government Entity, a third party vendor, or some combination of these, and may exist on or off premises. • Community cloud For example 'government Cloud' or ('gCloud'), where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (eg operational need, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the government Entities in the community, a third party vendor, or some combination of these, and it may exist on or off premises. • Public cloud The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic or government organisation or some combination of these. It exists on the premises of the cloud provider. • Hybrid cloud The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain discrete, but are bound together by standards that enables data and application portability. Note: Public Cloud Services are not appropriate hosts for Abu Dhabi Government Data.	M
DS.2.4	The Entity shall consult TIA942 Data Centre Standards, Annexe G, and determine which Tier is most appropriate to their needs, as summarised below. Tier I – Basic: 99.671% Availability: • Susceptible to disruptions from both planned and unplanned activity • Single path for power and cooling distribution, no redundant components (N) • May or may not have a raised floor, UPS or generator • Takes three months to implement • Annual downtime of 28.8 hours • Must be shut down completely to perform preventive maintenance Tier 2 – Redundant Components: 99.741% Availability • Less susceptible to disruption from both planned and unplanned activity • Single path for power and cooling disruption, includes redundant components (N+1) • Includes raised floor, UPS and generator • Takes three to six months to implement • Annual downtime of 22.0 hours • Maintenance of power path and other parts of the infrastructure require a processing shutdown	M

	Tier 3 – Concurrently Maintainable: 99.982% Availability • Enables planned activity without disrupting computer hardware operation, but unplanned events will still cause disruption • Multiple power and cooling distribution paths but with only one path active, includes redundant components (N+1) • Takes 15 to 20 months to implement • Annual downtime of 1.6 hours • Includes raised floor and sufficient capacity and distribution to carry load on one path while performing maintenance on the other Tier 4 – Fault Tolerant: 99.995% Availability • Planned activity does not disrupt critical load, and data centre can sustain at least one worst-case unplanned event with no critical load impact • Multiple active power and cooling distribution paths, includes redundant components (2 (N+1), ie 2 UPS each with N+1 redundancy) • Takes 15 to 20 months to implement • Annual downtime of 0.4 hours	
DS.2.5	The Entity shall refer to TIA942 for Data Centre Standards for all infrastructure including – but not limited to – access, power, cooling and networking.	M
DS.2.6	The Entity shall set its Data Centre Standards to comply with the Tier determined in DS2.4 and the Cloud Deployment Model considered in DS2.3.	M
DS.2.7	The Entity shall consider all options before committing to any Data Centre Strategy, taking into consideration Abu Dhabi Government Data Centre solutions as they emerge.	M
DS.2.8	The Entity must consider the costs and benefits of its data centre and cloud investments, and look to other Entities to share capacity and cost burdens, while increasing resilience.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DA.3 Target Data Architecture DS.1 Baseline Data Storage Architecture	
References	Telecommunications Infrastructure Standard for Data Centers, (Telecommunications Industry Association, 2005)	

DS.3	Data Storage Roadmap	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop and maintain a data storage roadmap		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐
Control Specification			**M/R**
DS.3.1	The Entity shall plan a Data Centre Transformation programme to progress from its current state (as determined in DS1) to its target architecture (DS2) within the timeframe of the Abu Dhabi Government Data Management Programme. The Entity shall: • Consider current capacity • Consider current utilisation • Consider current utilisation growth trend • Consider expected future requirements to the end of the Data Management Programme • Consider requirements for ten years past the end of the Data Management Programme • Consider current and future budgetary requirements and constraints • Plan to share capacity and resources with other Entities		M
DS.3.2	The Entity shall submit its Data Centre Transformation Programme to ADSIC for review and approval.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DA.4 Architecture Roadmap DS.1 Baseline Data Storage Architecture DS.2 Target Data Storage Architecture		
References	DMBOK (Mosley and Brackett, 2010) GCloud Overview (Cabinet Office, 2010)		

DS.4	Storage Roadmap Implementation	Version	1
		Suggested Priority	2
Control Standards	The Entity shall implement the rollout of the data storage roadmap		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐
Control Specification			**M/R**
DS.4.1	The Entity shall execute its Data Centre Transformation Plan as approved by ADSIC in DS3.		M
DS.4.2	The Entity shall establish a 'Cloud' Centre of Excellence team consisting of the following roles: • Cloud Manager • Cloud Specialist • Cloud Capacity Analyst • Cloud Architecture Lead • Cloud Service Manager • Cloud Administrator • Cloud Operator • Storage Administrator • Access Administrator • Backup Administrator • Network Administrator • Database Administrator • Middleware Administrator • Operating System Administrator Some of these roles may be shared with other Entities.		M
DS.4.3	The Entity shall continuously monitor capacity and utilisation, and proactively manage the physical and virtual resources.		M
DS.4.4	The Entity shall regularly audit capacity and utilisation using the same methodology as described in DS1. The Cloud Centre of Excellence Team shall meet quarterly and review capacity and utilisation, and keep their capacity planning up to date on a ongoing basis.		M
DS.4.5	The Entity shall keep a Data Centre development plan up to date at all times, review the plan annually and complete a major plan refresh exercise at least once every three years.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DS.3 Data Storage Roadmap		
References	Organizing for the Cloud (Lees, K, 2012) GCloud Overview (Cabinet Office, 2010) Government Data Centre Consolidation (ncia.go.kr, 2012)		

DS.5	Data Backup and Recovery	Version	1
		Suggested Priority	2
Control Standards	The Entity shall develop and execute a data backup and recovery plan		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		M/R
DS.5.1	The Entity shall implement a backup plan as described in the approved Information Security Standards in the Abu Dhabi Governemnt.	M
DS.5.2	The Entity shall define Recovery Point Objectives (RPO), accompanied by Recovery Time Objectives (RTO) for each system covered by the backup plan. These Objectives shall be approved by the Data Governance Board.	M
DS.5.3	The Entity shall conduct a regular backup availability test so that: • System backup and restoration policies are prioritised as in DS1.6 • RPO or RTO are validated and proven • Backup schedules are revisited twice yearly • A restoration testing schedule is maintained and verified • The restoration schedule should ensure: 1. All Core and Critical information systems are tested for restoration (bare metal) once a year 2. All High information systems are tested once every two years 3. All Medium and Low information systems are tested every three years • A log of all restoration attempts is maintained alongside the schedule • Care must be taken accurately to log the total time taken for restorations • In the event of a failure to restore a system when tested, a mitigation plan is to be put in place and the system re-tested • Additional restoration testing of randomly selected backup files should be conducted on a fortnightly basis	M
DS.5.4	Entity should use as preference remote disk backup as an offsite backup option. Whether using tape backup media or remote disk, the Entity shall ensure that backup copies are stored in an environmentally protected and access-controlled secure offsite location. The offsite location must: • Be monitored by security services (ie alarmed to a certified security organisation) • Provide installation of appropriate and effective fire detection and suppression systems • Provide a fire-rated secured vault for storage of backup copies • Provide security policies and procedures for the retention and retrieval of data storage • Enable regular audit reviews, including evidence of internal reviews and action taken	M
DS.5.5	The Entity shall conduct a Cost/Benefit analysis on improving the backup processes deployed. • Preference should be given to Disk-to-Disk-to-Government Cloud solutions • Disk-to-Disk-to-Tape should be retained for offline archiving and long-term backup	M

Control Version History	
1.0	
Control Dependencies	DA.4 Data Architecture Roadmap DS.3 Data Storage Roadmap
References	Abu Dhabi Government Information Security Standards (2013)

DS.6	Disaster Recovery and Business Continuity	Version	1
		Suggested Priority	2
Control Standards	The Entity shall develop and execute a disaster recovery plan		
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		M/R
DS.6.1	The Entity shall Implement a Business Continuity and Disaster Recovery (BCDR) plan as described in approved Information Security Standards in the Abu Dhabi Governemnt.	M
DS.6.2	The Entity shall determine the appropriate BCDR strategy for: • Protecting critical activities • Stabilising, continuing and restoring critical activities • Mitigating impacts for the incidents • Prioritising the time frame for restoring each critical activity • Evaluating the disaster recovery and business continuity capacity of vendors • Planning and executing annual BCDR drills as well as quarterly BCDR paper scenario exercises	M
DS.6.3	The Entity's BCDR plan shall contain: • Defined roles and responsibilities for the teams authorised to act on behalf of the Entity during and in the aftermath of an incident • A defined process for activating a response to an incident • A defined set of actions to mitigate the initial consequences of an incident, prioritising: 1. Safety and welfare of individuals 2. Short, medium and long-term options for response to the incident 3. A mitigation plan to prevent further impact on critical activities • A concise communication plan, including prime and alternate methods for communicating with: 1. Employees 2. Customers 3. Senior Managers and Executives 4. Other Stakeholders • A prioritised recovery plan setting out the priorities and timelines required to recover firstly critical data and information systems, and the follow up activities that need to be addressed during the rehabilitation period	M

	• A media plan 1. A concise communication strategy 2. A clearly designated spokesperson and succession plan 3. Template communications – ready to be issued • A stand-down plan to demobilise the activities at the end of the incident	
Control Version History		
1.0		
Control Dependencies	DA.4 Data Architecture Roadmap DS.3 Data Storage Roadmap DS.5 Data Backup and Recovery	
References	Abu Dhabi Government Information Security Standards (2013) ISO 22301 Business Continuity Management Systems (ISO, 2012)	

DS.7	**Data Lifecycle**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall document the data lifecycle of data within information systems and services under its control		
Control Type	Directive ☑	Preventive ☐	Detective ☑	Corrective ☐
Control Specification			**M/R**
DS.7.1	The Entity shall develop a clear policy and standards for the management of all recorded information (irrespective of its form) that has been created or received and maintained by the Entity in the course of its business. The states of the Information Life Cycle are: • Creation • Retention (organisation, storage, security, etc) • Maintenance • Use (retrieval, access levels etc) • Retirement (archival offline or nearline) • Disposal (timely, with appropriate and secure media destruction methods used) The intention is that recorded Information held by the Entity shall always be: • Of high quality • Accurately captured • Timely • Up to date • Secure • Easily retrievable • Available when needed		M

DS.7.2	All data (including documents and records) created and held with an Entity should be: Authentic: • Have its provenance clearly identified showing chain of custody to its ultimate source • Recorded information can be traced and proven to be what it appears to be • Have been created or sent by the person who appears to have created or sent it • Have been created or sent at the time suggested Reliable: • The data can be trusted as an accurate representation of the information or facts as shown, and that it can be relied upon in the course of subsequent processes Complete and Unaltered: • The integrity of data relates to it being complete and lack of alteration • Data must be safe against unauthorised changes • Policies and procedures must specify what additions, alterations or redactions can be made to a data after it is created, under what circumstances these may be authorised, and which parties are authorised to manipulate them; any authorised additions, alterations or redactions must be explicitly shown, and fully audited and traceable Useable: • Useable data is one that the Entity can locate, retrieve, present and interpret • Data must be fully traceable to the business transaction that produced the data • The accompanying metadata data should hold the information needed to understand the transaction and processes used to create the data that created it and process that it followed • It should be possible to identify a record to the corresponding business activities that generated or modified the record	M
DS.7.3	For all classes of data held, by the Entity an Entity shall: • Identify the Data Owner of the given dataset • Determine the creation and disposal requirements for a data class • Identify information-sharing requirements within the Entity and between Entities, and between the Entity and third parties • Identify which data is stored electronically, which are stored as physical documents, and those data profiles which are 'hybrid' (ie stored partly electronically and partly as a hardcopy) • Allow data to be related to current retention schedules so that – where appropriate – superfluous, stale or replicated data can be retired and then destroyed • Ensure that its staff with data management responsibilities (and their managers) are adequately trained, and regularly participate in refresher training sessions • Identify deficiencies in the physical or electronic storage of data, and initiate a remediation plan for any deficiencies found	M

	• Facilitate both internal and external audits related to data (eg Audit Department, DED Audits, Security Audits) • Maintain a central inventory of data classes, and ensure it is reviewed annually (see Data Catalogue standards) • Annually remind managers and owners of data assets to update document inventory entries to guarantee their accuracy and completeness	
DS.7.4	For all classes of data held, an Entity shall: • Maintain an inventory of data in the Data Catalogue, so as to facilitate an annual report provided to the Entity Data Governance Board for review and sign off • The report will: 1. Describe the status of the Data Inventory 2. Report departmental compliance with Data Management Standards 3. Identify areas where there is risk of non-compliance in the Information Lifecycle 4. Make recommendations, and mandate action plans and timescales for mitigating such risks	M
DS.7.5	All data held by and managed by the Entity shall be tightly governed by the Entity's Information Lifecycle process, referencing the following states: • Creation: 1. Available when needed 2. Accessible to all members of staff that require access in order to enable them to carry out their business-as-usual activities 3. Understandable, clear and concise 4. Trusted, accurate and relevant 5. Secure • Retention: 1. Documented information shall be retained only for as long as it is needed and in line with the timescales within the Entity's Document Retention and Disposal policy • Maintenance: 1. All data shall be maintainable throughout their lifecycle • Use: 1. All data shall be used consistently, only for the purpose for which it was intended, and never for an individual employee's personal gain or other purpose 2. If in doubt, employees shall seek guidance from the Chief Information Security Officer 3. Contractors must also be monitored, and their access and use of documents controlled 4. Only specific data required should be disclosed to authorised third parties 5. Data should only be disclosed with strict adherence to Data Management Policy and Standards	M

	• Retirement: 1. All data that is approaching end-of-life should be first retired to a secure offline or near-line repository 2. After a cooling off period, and ensuring there is no operational impact, data should be made ready for disposal 3. This does not affect the data's overall disposal schedule, and offline retirement should be carried out ahead of a document's disposal window • Disposal: 1. Data (irrespective of their media) must be retained and disposed of in a timely way in accordance with Entity's policy 2. Only the minimum set of data should be retained consistent with cost-effective and efficient operations 3. Disposal of data is undertaken promptly and conducted by authorised staff 4. All data disposal must be fully documented 5. The policy includes provision for permanent preservation and transfer of information with archival value 6. The Data Owner can advise on archiving and transfer of documents to approved archive	

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DA.4 Data Architecture Roadmap DS.3 Data Storage Roadmap DS.4 Storage Roadmap Implementation
References	DMBOK (Mosley and Brackett, 2010)

14.9 USE AND SHARE: Data Integration and Interoperability

DIO.1	Strategic Integration Platform	Version	1
		Suggested Priority	1
Control Standards	The Entity shall include data integration architecture within the Entity's data architecture		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DIO.1.1	The Entity shall implement a Strategic Integration Platform to provide the infrastructure to connect internal and external information systems and data feeds. The Strategic Integration Platform is an architectural component or set of services that allows: • Data transfer – physically moving data from one system to another • Data transformation – mapping data from one set of data formats to another where there are differences between systems • Access auditing – logging users, services, requests • Performance monitoring – monitoring data volumes and frequency • Security controls – ensuring controlled access to data • Transaction management – management of long running transactions in the case of two-way data transfer The Strategic Integration Platform shall be included in the Entity's target enterprise data architecture (see Data Architecture Standards).	M
DIO.1.2	The Entity shall ensure that its strategic integration platform aligns with metadata requirements of the Abu Dhabi Government Interoperability Framework (eGIF).	M
DIO.1.3	The Entity shall develop and publish a policy for usage of its strategic integration platform. This shall cover sharing (i) internally; (ii) with trusted third parties; and (iii) externally. • Internal data sharing policy should encourage data sharing initiatives across business functions. • The policy for sharing data with trusted third parties (which include other Entities, commissioned third parties and service suppliers) shall include consideration for developing service level agreements (See Data Integration and Interoperability Standards). External users of the Entity's data that are not affiliated with the Abu Dhabi Government or its contracted suppliers shall be bound by usage licences developed by the Entity. Such usage licences shall align with the Entity's Open Data standards (see Open Data Standards).	M
DIO.1.4	The Entity shall give consideration to migrating existing data feeds into and out of information systems through the Strategic Integration Platform within the Entity's target data architecture. The Data Governance Board shall consider the business value and applicability for re-use of each data feed.	R
DIO.1.5	The Entity shall ensure that external integration with data from other Entities is made through the ADSIC Enterprise Service Bus (ESB). The Entity shall not engage in peer-to-peer data transfers with other Abu Dhabi Government Entities. Datasets made available through the ADSIC ESB shall be published in the Entity's Data Catalogue.	M
DIO.1.6	Data shall be exchanged in a secure and audited manner. Data made available through the Strategic Integration Platform shall comply with the information exchange requirements of the approved Information Security Standards in the Abu Dhabi Governemnt.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DA.4 Data Architecture Roadmap DQ.2 Data Quality Audit DQ.3 Data Quality Uplift DSP.1 Information Security Standards DSP.3 Privacy By Design DSP.5 Data System Protection DS.3 Data Storage Roadmap
References	Abu Dhabi Government Information Security Standards (2013) Case Study and Best Practices of eGov Interoperability in Korea (Joohaeng, 2010) DMBOK (Mosley and Brackett, 2010) UK Government Reference Architecture UKRA (HM Government, 2012)

DIO.2	Integration Architecture	Version	1
		Suggested Priority	1
Control Standards	The Entity shall include data integration architecture within the Entity's data architecture		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DIO.2.1	The Entity shall ensure that consideration is given at the data architecture level for appropriate data exchange methods when integrating data between applications and information systems. Acceptable data exchange methods include (but are not limited to): • File based data exchange – transferring a data file to a central physical location, where it may be processed, validated, and transformed before being collected by the receiving system • Message based data exchange – exchanging information through formatted messages via a service bus, typically in a publisher/subscriber model or broadcast model (see DIO.3) • Database to database data exchange – typically used with ETL systems, data may be passed through an intermediary database for transformation and validation before routing to its final destination; information systems should not exchange data directly into each other's databases The Entity shall describe the data exchange methods used in system data architectures (see Data Architecture).	M
DIO.2.2	The Entity shall include the plan to migrate peer-to-peer application data sharing to the Strategic Integration Platform in its target data architecture. For example, a time sheet system may pull the list of employees from a human resources system. The Entity shall plan to migrate the provision of the employee list via the Strategic Integration Platform, allowing greater opportunities for data re-use. Where migration to the Strategic Integration Platform is not possible due to proprietary software, the Entity shall provide justification through the Data Governance Board.	M
DIO.2.3	The integration platform shall provide the capability to broker interactions across different integration patterns allowing, for example, file-based data exchanges and message-based data exchanges to be integrated. Data exchange integration capability shall be shown on the Entity's target data architecture.	R
DIO.2.4	The Entity shall ensure that data architectural consideration is given to the data formats allowed by each data service integrated. Acceptable data formats include (but are not limited to): • Value separated data formats – such as CSV and Tab-delimited files • Fixed length record formats – such as 80-column VSAM files • XML and JSON data formats – such as those compliant with Schemas generated in compliance with the Abu Dhabi Government eGIF • Industry or proprietary data formats – such as the MARC bibliographic record format XML and JSON data formats shall be the preferred mechanism for data transfer between Entities. Industry or proprietary data formats are allowed where there are restrictions within commercial tools or industry practice; however, the Entity should seek to use open formats, and show justification for use of proprietary data formats within data architectures. Acceptable access formats shall be published in the Entity's Data Catalogue.	M
DIO.2.5	The Entity shall ensure that data architectural consideration is given to the data transfer protocols allowed for connecting information systems to the Strategic Integration Platform Acceptable protocols include (but are not limited to): • File Transfer Protocols (FTP/SFTP) • Hyper Text Transfer Protocols (HTTP/HTTPS) • Simple Object Access Protocol (SOAP) • Database Connectivity Protocols (ODBC/JDBC) Protocols may be combined as appropriate to produce an end-to-end solution. For example, it is typical for SOAP to run over HTTP. Acceptable access protocols for each data source shall be demonstrated through the target data architecture, and published in the Entity's Data Catalogue.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.5 Enterprise Data Model DM.7 Master Profiles DA.3 Target Data Architecture DA.4 Data Architecture Roadmap DS.3 Data Storage Roadmap DIO.1 Strategic Integration Platform
References	DMBOK (Mosley and Brackett, 2010)

DIO.3	Integration Patterns	Version	1
		Suggested Priority	2

Control Standards	The Entity shall design data integration architectures according to common integration patterns			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☑

Control Specification		M/R
DIO.3.1	The Entity shall favour the use of one-way integration patterns for sharing data with other systems. Possible one-way integration patterns include: • Publish/Subscribe – where the data publisher publishes data to a specified location (eg file system, message bus), and the subscriber detects the publish event and retrieves and removes the data from the publish location • Request/Response – where the consumer requests data and the publisher responds • Broadcast – where the data is published as above, and multiple subscribers retrieve the data without removing it from the publish location	M
DIO.3.2	The Entity shall provide justification for using two-way or interactive integration patterns through the Governance Checkpoint Process. Two-way or multi-way data integration – where data is passed between more than one system –is more complex than one-way data integration, and the following aspects should be considered: • Transaction management, failure and repeatability across system boundaries • Concurrency between information systems where volatile data may change before data is successfully transferred	M
DIO.3.3	The Entity shall give consideration to data integration designs for the following requirements: • Detect data delivery failure – detecting that data has not been delivered after a pre-defined period • Repeatable/idempotent retries – repeatedly sending data should not have adverse side effects • Statelessness – the transport mechanism should not store domain business knowledge of the producer or consumer • High availability – sufficient capacity should be provided for all the producers and consumers of data The Data Governance Board shall evaluate these requirements presented in the form of data architecture designs.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DIO.2 Integration Architecture
References	DMBOK (Mosley and Brackett, 2010) Enterprise Integration Patterns (Hohpe, Woolf, 2003)

DIO.4	Service Level Agreements	Version	1
		Suggested Priority	2

Control Standards	The Entity shall develop a framework for data integration service level agreements			
Control Type	Directive ☐	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		M/R
DIO.4.1	Service level agreements shall include agreement on the following areas: • Data quality (See Data Quality Standards) • Data volume – the amount of data each party commits to sending and receiving • Availability of service – planned uptime, or service availability windows • Variety of data – the structure of the dataset, including data model and definitions • Change control process – the mechanism of informing data consumers of changes to the underlying data sets or data formats • Exception escalation path – the mechanism for investigating data errors, service outages, and exceptions to the SLA • SLA monitoring frequency – the frequency at which the service level shall be measured (for example, 99.995% availability shall be measured on a per-monthly or annual basis)	M
DIO.4.2	The Entity shall produce internal service level agreements where data is shared between information systems within the Entity. Disputes arising through the provision of services under the agreement shall be resolved through the Data Governance Board, which will take a pragmatic view as to a solution that most benefits the Entity's business as a whole.	M
DIO.4.3	The Entity shall produce binding service-level agreements where data is shared between Abu Dhabi Government Entities through the ADSIC ESB. Similar commitment should be between ADSIC and the Prodcuer for the provision of the transport service between the Entity's service endpoints. In the event of services not meeting the service-level agreements, the exception escalation path described in the service-level agreement shall be followed, with ADSIC providing diagnostic support (where log files and other diagnostic information is required). The Producer and Consumer Entities shall engage cooperatively to investigate potential exceptions to the service level agreement.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DIO.1 Strategic Integration Platform DIO.2 Integration Architecture
References	DMBOK (Mosley and Brackett, 2010)

14.10 USE AND SHARE: Open Data

OD.1	Open Data Identification		Version	1
			Suggested Priority	2
Control Standards	The Entity shall define and identify open data in their business context			
Control Type	Directive ☐	Preventive ☐	Detective ☑	Corrective ☐

Control Specification		M/R
OD.1.1	The Entity shall perform an Open Data Review of all of its data sources (structured and unstructured) in a systematic audit using its Risk Assessment process. The Entity shall evaluate each data source from an 'Open By Default' perspective. All data sources are to be deemed 'Open' unless there is a quantifiable reason for keeping the sources closed. Criteria for closing a source include: • Demonstrable Security concerns • Demonstrable Privacy concerns • Data Quality concerns The criteria and decision log for closing a source are to be reviewed annually by the Data Governance Board. In the event that data quality is a concern, a remediation plan with a clear open data quality threshold is to be put in place to allow publication. The Entity shall define the extent of the data source that is to be made available to users that are both internal – and external – to the government. The Entity should include definitions of what constitutes an internal or an external user.	M
OD.1.2	The Entity, having conducted an Open Data Review, shall keep systematic records, showing the sources, and clearly and explicitly indicating their Open Status (Open or Closed). The Entity shall provide a definition in their Data Catalogue for each open data set, written clearly and in plain language (in line with the context of its business).	M
OD.1.3	All datasets that are deemed 'open' in the Open Data Review are to be made available through: • The Open Data Portal (an adjunct of the Abu Dhabi Portal) in machine-readable form • The Open Data Portal (an adjunct of the Abu Dhabi Portal) in human-readable form (where practicable)	M
OD.1.4	The Entity shall ensure that to the extent possible all data is made available in the form closest to the source as possible. Data should not be manipulated, aggregated, redacted, anonymised or obfuscated to the extent possible and allowable, with due regard for privacy and security concerns. Where such concerns exist, aggregation, redaction, anonymisation obfuscation and other manipulations should be carried out to the minimum extent possible to alleviate the concern. The following should be considered: • Is it reasonably likely that an individual can be identified from those data and from other data? • What other data is available, either to the public or to researchers or other organisations? • How and why could your data be linked to other datasets? • What is the likelihood of re-identification being attempted? • What is the likelihood the re-identification would be successful? • Which anonymisation techniques are available to use? • What is the quality of the data after anonymisation has taken place, and whether this will meet the quality gate for this data set's Open Data release?	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DM.5 Enterprise Data Model DM.7 Master Profiles DM.8 Logical Data Model DSP.1 Information Security Standards DSP.3 Privacy By Design DSP.4 Privacy Management
References	Project Open Data (2014) The Open Data Handbook (2014)

OD.2	Open Data Publishing Plan	Version	1
		Suggested Priority	2

Control Standards	The Entity shall develop and publish a plan to release open data from the data, information systems and services under their control			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
OD.2.1	The Entity shall develop an Open Data Plan, working from its Open Data Review, to release the data through the Open Data Portal. The Open Data Plan shall allow for: • The dataset to be reviewed and duly approved for release as Open Data • The dataset to be released once it has passed its predetermined quality gate • Any aggregation, redaction, anonymisation or obfuscation required for privacy or security concerns has been approved and undertaken	M
OD.2.2	The Entity shall ensure that the Open Data Plan prioritises the release of Open Data by: • Addressing security and privacy concerns • Addressing the business priorities of the Entity • Addressing the demand from third parties for data • Addressing the measurable quality of the data	M
OD.2.3	The Entity shall ensure that the Open Data Plan systematically addresses all of the datasets identified in the Open Data Review.	M
OD.2.4	The Entity shall ensure that progress against the Open Data Plan is monitored, and the plan is reviewed quarterly.	M

Control Version History	
1.0	
Control Dependencies	DG.2 Data Management Policy DG.3 Data Management Programme DSP.3 Privacy By Design DSP.5 Data System Protection
References	Project Open Data (2014) The Open Data Handbook (2014)

OD.3	Open Data Publishing	Version	1
		Suggested Priority	2

Control Standards	The Entity shall publish Open Data in the Abu Dhabi Government Open Data Portal			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
OD.3.1	The Entity shall publish its Open Data in the Abu Dhabi Government Open Data Portal	M
OD.3.2	The Entity shall take care to ensure that all Open Data is reviewed regularly and ensure that: • The data continuously continues to meet its quality definition • Security and privacy concerns are continuously reviewed, specifically: 1. Is it reasonably likely that an individual can be identified from those data and from other data? 2. What other data are available, either to the public or to researchers or other organisations? 3. How and why could your data be linked to other datasets? 4. What is the likelihood of re-identification being attempted? 5. What is the likelihood the re-identification would be successful? 6. Which anonymisation techniques are available to use? 7. What is the quality of the data after anonymisation has taken place and whether this will meet the quality gate for this data set's Open Data release?	M
OD.3.3	In the event that the Open Data fails to meet its quality level or there is a concerns regarding security or privacy, the Entity shall: • Suspend the publication of that dataset as Open Data • Undertake a new Open Data Review for that dataset • Establish and execute a mitigation plan for the new concerns and/or quality issue • If necessary, relist the data as 'Closed' until such issues can be resolved	M
OD.3.4	The Entity shall capture usage trends and statistics regarding access to its data, and report these trends and statistics to the Government Data Governance Committee.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme MD.2 Metadata Management Programme DC.2 Data Catalogue Principles OD.1 Open Data Identification OD.2 Open Data Publishing Plan
References	Project Open Data (2014) The Open Data Handbook (2014)

OD.4	Open Data Awareness	Version	1
		Suggested Priority	3
Control Standards	The Entity shall engage external interested parties in an Open Data awareness campaign		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
OD.4.1	The Entity shall undertake annual awareness campaigns to ensure potential users and stakeholders are aware of the existence, nature and quality of the Open Data being offered by the Entity. The awareness campaign needs to consider: • Progress of the Open Data Plan • The need to inform and educate internal stakeholders • The need to inform and educate external stakeholders • The need to inform and educate the wider public The awareness campaign should include: • Details on where to find Open Data • Details on where to find the Open Data Catalogue • Information on privacy and security concerns, including (in a general sense) the provisions made for: 1. Aggregation 2. Redaction 3. Anonymisation 4. Obfuscation • Explanations in plain language on the type of data and its context • An indication on the Age (or Age Window) of the data • An Indication on the quality that can be expected form the data	M
OD.4.2	In the event that an Entity does not publish a dataset or datasets, it shall use its annual awareness campaign to: • Explain to the extent possible the reasons for withholding a dataset • Indicate if and/or when a dataset will be published • To provide a clear statement if a particular dataset is to remain unpublished for the foreseeable future	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme OD.3 Open Data Publishing
References	Project Open Data (2014) The Open Data Handbook (2014)

14.11 IMPLEMENT: Reference and Master Data Management

RM.1	Reference Data Management Plan	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop a Reference Data Management Plan		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
RM.1.1	The Entity shall plan and publish a schedule of the activities necessary to identify all of the reference data used in the information systems owned and operated by the Entity (or by third parties working on behalf of the Entity). The Reference Data Management Plan shall identify the following: • Mobilisation and allocation of required resources • Scoping of the information systems involved • Schedule for discovery and alignment • Schedule for regular reviews of the plan, information systems, and external influences	M
RM1.2	The Entity shall establish a team to be responsible for the management of the Entity's reference data, with supporting resources required to perform the discovery and alignment activities plus the ongoing change management and coordination of reference data for all of the Entities information systems.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DM.5 Enterprise Data Model DM.7 Master Profiles DM.8 Logical Data Model DM.9 Physical Data Model
References	DMBOK (Mosley and Brackett, 2010) IBM RedBooks Reference Data Management (IBM Redbooks, 2013) Orchestra Networks RDM Field Report (The MDM Institute, 2012)

RM.2	Identify Reference Data	Version	1
		Suggested Priority	1
Control Standards	The Entity shall identify the reference data used in its Information Systems		
Control Type	Directive ☐	Preventive ☐	Detective ☑	Corrective ☐

Control Specification		M/R
RM.2.1	The Entity shall identify and define the reference data that is used by each of the information systems owned and operated by the Entity, documenting the values and semantic definition.	M
RM.2.2	The Entity shall ensure that all reference data values are codified and implemented as contiguous non-whitespace values. Code values shall be unique in their context and shall not be case sensitive. All codes shall have an associated description, and may have additional properties, attributes and synonyms defined in their metadata.	M
RM.2.3	The Entity shall align the semantic definition and values of the identified reference data with the following sources as they become ratified standards: • Definitions published by the Abu Dhabi Government for common use 1. Reference datasets and codelists from EGIF 2. Data standards catalogue from the EGIF 3. SCAD Dataset and Variable Elements Standard • Local standards in common use within the Entity 1. Codelists introduced through common practice This alignment will provide the 'master reference data' dataset.	M
RM.2.4	The Entity shall conduct regular reviews of the 'master reference data' dataset to incorporate new information systems or to review information systems that may have implemented changes.	M
RM.2.5	The Entity shall either: • Align the reference data used by the information systems with the 'master reference data' dataset, or; • Provide a mapping schema to link every reference data value used in the Entity's information systems with a value in the 'master reference data' dataset. The mapping must account for bi-directional transformations (so that where there is a one-to-many relationship, it is unambiguous as to how the mapping from a single value to many possible values will be determined)	M
RM.2.6	The Entity shall ensure that all reference data values are described in Arabic and English.	R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.5 Enterprise Data Model DM.7 Master Profiles DM.8 Logical Data Model DM.9 Physical Data Model RM.1 Reference Data Management Plan
References	DMBOK (Mosley and Brackett, 2010) IBM RedBooks Reference Data Management (IBM Redbooks, 2013) Orchestra Networks RDM Field Report (The MDM Institute, 2012)

RM.3	Reference Data Change Management	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop and execute reference data change management processes		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
RM.3.1	The Entity shall develop and execute processes within the organisation to actively manage reference data values. The Entity will provide a mechanism to allow new reference data values to be requested, evaluated, and either applied to the reference dataset or to have an alternative existing value suggested for that use.	M
RM.3.2	The Reference Data Change process will define how: • The requests are submitted • The requests are evaluated • External parties are identified and consulted • The value assessment is made • New values are propagated to the Entity's information systems • The values are applied to the information systems • Who is responsible for updates to the information systems • External parties are notified • Codelists are propagated to the EGIF	M
RM.3.3	The Entity shall ensure that the process execution can be evidenced through the capture and recording of requests, consultations and decisions.	M
RM.3.4	The Entity shall implement the necessary processes to be able to audit the population of reference data across all information systems.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit RM.2 Identify Reference Data
References	DMBOK (Mosley and Brackett, 2010) IBM RedBooks Reference Data Management (IBM Redbooks, 2013) Orchestra Networks RDM Field Report (The MDM Institute, 2012)

RM.4	Reference Data Platform	Version	1
		Suggested Priority	1
Control Standards	The Entity shall implement a Reference Data Management platform		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
RM.4.1	The Entity shall implement reference data export features from all of the information systems so that they can be compared to the Entity's 'master reference data' dataset to monitor alignment of the reference data values across the organisation. The output from the exports can also be used by the Entity to discover the reference data stored in the information systems, and used for the initial analysis.		M
RM.4.2	The Entity shall implement a Reference Data Management platform that is capable of delivering the following features, including (but not limited to): • Reference data workflow management • Multiple versions of reference data • Support for import of reference data • Support for API integration • Support for mapping between versions of managed datasets • Support for hierarchical datasets • Support for XML export • Point of entry validation and batch data matching, with native Arabic support • Support for multilingual reference data values • Support for data inheritance to allow localised data extensions • Model-driven to minimise technical dependency for changes and extensions • Distributed server capabilities • Integrated customisable UI capability • Integrated web-service capability • File import and export capability • Dynamic data exchange of selected data elements between distributed instances • Support for encrypted data persistence and secure data exchange		M
RM.4.3	The Entity shall implement appropriate system processes to detect and identify the use of new or unrecognised reference data values to trigger audit and process reviews. This will establish the validity of the values and how a new value has been introduced outside of the reference data change management process.		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DA.3 Target Data Architecture DA.4 Data Architecture Roadmap RM.1 Reference Data Management Plan RM.2 Identify Reference Data RM.3 Reference Data Change Management		

References	DMBOK (Mosley and Brackett, 2010) IBM RedBooks Reference Data Management (IBM Redbooks, 2013) Orchestra Networks RDM Field Report (The MDM Institute, 2012)

RM.5	Master Data Management Plan	Version	1
		Suggested Priority	1
Control Standards	The Entity shall develop a Master Data Management plan		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
RM.5.1	The Entity shall plan and publish a schedule of the activities necessary to identify all of the master data used in the information systems owned and operated by the Entity or by third parties on behalf of the Entity. The Master Data Management plan shall identify the following: • Mobilisation and allocation of required resources • Master data discovery and cleansing initiative • Ongoing master data stewardship • Scoping of the information systems involved • Schedule for discovery and alignment • Schedule for regular reviews of the plan, information systems and external influences		M
RM.5.2	The Entity shall establish a team to be responsible for the management of the Entity's master data, with supporting resources required to perform the discovery, alignment and cleansing activities, and the ongoing management, coordination and stewardship of the master data for all of the Entity's information systems. The organisation description shall include ownership, accountability and responsibility for the management of each master data dataset for the Entity spanning across all information systems. It shall also list the stakeholders for each master data dataset for consultation in the event of significant dataset changes (in terms of structure or content).		M
Control Version History			
1.0			
Control Dependencies	DG.3 Data Management Programme RM.5 Master Data Management Plan		
References	DMBOK (Mosley and Brackett, 2010) London Councils MDM Best Practice Summary Report (Troy, Ellis, 2008) Master Data Management in Government (Informatica, n.d.)		

RM.6	Identify Master Data	Version	1
		Suggested Priority	1
Control Standards	The Entity shall identify the master data used in its Information Systems		
Control Type	Directive ☐	Preventive ☐	Detective ☑	Corrective ☐

Control Specification		M/R
RM.6.1	The Entity shall identify and define the master data that is used by each of the information systems owned and operated by the Entity, documenting the semantic definition of the master data profile and the data elements that form its composition. The Entity shall also identify and define the lifecycle of each master data profile, establishing the data's origin, use, maintenance and disposal, in both business and technical contexts.	M
RM.6.2	The Entity shall ensure that all master data records can be uniquely identified and codified with contiguous non-whitespace values. Code values shall be unique in their context and shall not be case-sensitive.	M
RM.6.3	The Entity shall develop and publish key performance indicators and metrics by data profile for the measurement and monitoring of the numbers of duplicated master data records held in each information system.	M
RM.6.4	The Entity shall implement measures to identify a primary master data record where there are duplicates, and implement systematic controls to limit the use non-primary records within the information systems where it is practicable to do so.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DM.5 Enterprise Data Model DM.7 Master Profiles DM.8 Logical Data Model DM.9 Physical Data Model RM.6 Identify Master Data
References	DMBOK (Mosley and Brackett, 2010) London Councils MDM Best Practice Summary Report (Troy, Ellis, 2008) Master Data Management in Government (Informatica, n.d.)

RM.7	Operate Master Data	Version	1
		Suggested Priority	1
Control Standards	The Entity shall operate master data profiles across their organisation		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
RM.7.1	The Entity shall match and link equivalent master data records within each information system to identify where there are duplicate records.	M
RM.7.2	The Entity shall assess and identify by information system those master data profiles that will deliver a tangible benefit to the organisation by merging duplicated master data records. The benefit analysis must recognise that data that references the affected master data records will need to be processed, and references changed to point to the surviving master data record.	M
RM.7.3	Where a compelling benefit case can be identified, or where a government-wide mandate is issued, the Entity shall schedule and execute a master data initiative to cleanse the master data and associated data to re-duplicate entries.	M
RM.7.4	The Entity shall match and link equivalent master data records across all of the information systems owned and operated by the Entity (and by third parties working on behalf of the Entity). The Entity shall match and link equivalent master data records with records held in centrally managed cross-government information systems, paying special attention to those information systems recognised as a primary system (such as Emirates ID).	M
RM.7.5	The Entity shall develop and publish key performance indicators and metrics. For each information system and master profile, indicators shall measure the numbers of master data records and their equivalent records in each system, both within the Entity's systems, and across government-wide information systems such as the Emirates ID system.	M
RM.7.6	The Entity should be able to identify any master data records that have not been linked to any equivalent records, to allow them to be a focus for data stewardship activities. The Entity shall ensure that frequent reviews of highlighted master data records are conducted, and that the actions taken are auditable.	M
RM.7.7	The Entity shall implement appropriate system safeguards to monitor the reference data values used in master data records to ensure that values are recognised as approved reference data for the master data profile and is suitable for the context of the master data record in its containing information system.	M
RM.7.8	The Entity shall conduct regular reviews as set out in the Master Data Initiatives plan, to incorporate new information systems or to reassess information systems that may have implemented recent changes that might not have been identified through operational processes.	M
RM.7.9	The Entity shall ensure that all master data values can be described in more than one language.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit DM.5 Enterprise Data Model DM.7 Master Profiles DM.8 Logical Data Model DM.9 Physical Data Model
References	DMBOK (Mosley and Brackett, 2010) London Councils MDM Best Practice Summary Report (Troy, Ellis, 2008) Master Data Management in Government (Informatica, nd)

RM.8	**Master Data Change Management**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall develop and execute master data change management processes		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
RM.8.1	The Entity shall develop and execute processes within the organisation to actively manage master data records. Each Entity will provide a mechanism to allow master data issues to be identified, prioritised and handled in a manner appropriate to the importance of the data to the organisation, the impact the issue is having on the organisation, and the urgency to resolve the issue.		M
RM.8.2	The Master Data Change process will define how: • The primary information system is identified (that being the system against which all other information systems are benchmarked for the master data profile) • The master data records for each master data profile shall be maintained, be it in the primary system and interfaced to other systems, or manually maintained in multiple systems, and shall include details of the process checkpoints that will audit the maintenance of the master data records • Master data records from sources external to the Entity are incorporated into the Entity's information systems • Master data records shall be published to external targets where the Entity is the primary external source for the master data for another party		M
RM.8.3	The Entity shall ensure that the process execution can be evidenced through the capture and recording of changes, consultations and decisions.		M
RM.8.4	The Entity shall implement the necessary processes in order to audit the population of master data across all information systems, which shall include the development of key performance indicators and metrics to measure the latency between updates to each information system, and alignment of data values between information systems.		M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit
References	DMBOK (Mosley and Brackett, 2010) London Councils MDM Best Practice Summary Report (Troy, Ellis, 2008) Master Data Management in Government (Informatica, n.d.)

RM.9	**Master Data Platform**	**Version**	1
		Suggested Priority	1
Control Standards	The Entity shall implement a Master Data Management Platform		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification			**M/R**
RM.9.1	The Entity shall implement master data export features from all of the information systems so that they can be compared to the Entity's 'primary master data' dataset for each master data profile in order to monitor alignment of the reference data values across the organisation. The output from the exports can also be used by the Entity to discover the nature of the master data stored in the information systems, and used for the initial analysis.		M
RM.9.2	The Entity shall implement a Master Data Management platform that is capable of delivering the following features, including, but not restricted to: • Master data workflow management with support for multi-level approval • Multiple versions of master data • Support for import of master data • Support for API integration • Support for mapping between versions of managed datasets • Support for hierarchical datasets • Support for XML export • Point of entry and batch validation • Point of entry and batch data matching (with native Arabic support) • Merging or linking equivalent records for the same information system or different systems • Support for multi-lingual operation • Support for multi-lingual master data values • Support for data inheritance to allow localised data extensions		M

	• Being model driven to minimise technical dependency for changes and extensions • Distributed server capabilities • Integrated customisable UI capability • Integrated web-service capability • File import and export capability • Dynamic data exchange of selected data elements between distributed instances • Support for encrypted data persistence and secure data exchange • Integrated support for data security, privacy and data element grain permission control • Integration with the Reference Data Management platform	
RM.9.3	The Entity shall implement appropriate system processes to detect and identify the use of new or unrecognised master data values to trigger audit and process review. This will establish the validity of the values and monitor new values introduced outside of the master data change management process.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DA.3 Target Data Architecture DA.4 Data Architecture Roadmap	
References	DMBOK (Mosley and Brackett, 2010) London Councils MDM Best Practice Summary Report (Troy, Ellis, 2008) Master Data Management in Government (Informatica, nd)	

14.12 IMPLEMENT: Document and Content Management

DCM.1	**Document and Content Quality Standards**			**Version**	1
				Suggested Priority	1
Control Standards	The Entity shall define standard formats, style guides and versioning guidelines for any documents or content produced				
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐	
Control Specification					**M/R**
DCM.1.1	The Entity shall establish quality standards for all document and content types being managed. As a minimum, these quality standards should establish: • A language style guide describing the expected written standard for the writing, and important guides for design (look and feel) • Naming conventions to be followed • Review and editorial processes to be undertaken and documented • Version management processes and procedures				M
Control Version History					
1.0					
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit				
References	ISO 15489-1:2001 Information and documentation (ISO, 2001)				

DCM.2	Document and Content Requirements	Version	1
		Suggested Priority	1
Control Standards	The Entity shall implement document and content management appropriate to their requirements		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DCM.2.1	The Entity shall define requirements for Documents and Content Management that includes, but is not restricted to: • A document standard that specifies what documents are mandatory in each Entity process, and the data that must be included in each document • What document types should be used in each case (eg Word DOCX, Adobe PDF, Scans TIFF or JPEG etc) • The metadata to be captured with the document, and throughout the document lifecycle • How the document metadata will be captured and managed • Procedures for retrieving, using and sharing documents between business processes • Determination of how long documents need to be kept to satisfy business, privacy and regulatory requirements • Determination of the file structure (file plan) for the proper organisation of documents • Assessment of the risks of failure to the management or access of documents • Persisting documents and their availability over time to meet business needs • Proper considerations of any legal and regulatory frameworks or requirements • Referencing the Information Security policy to ensure documents are in a safe and secure environment • Retirement and disposal of documents so that they are retained only for as necessary and required	M
DCM.2.2	All documents and records created and held with an Entity should be: Authentic • Have their provenance clearly identified showing chain of custody to its ultimate source • Recorded information can be traced and proven to be what it appears to be • Have been created or sent by the person who appears to have created or sent it • Have been created or sent at the time suggested Reliable: • The content of a document can be trusted as an accurate representation of the information or facts as shown, and that it can be relied upon in the course of subsequent processes	M
	Complete and Unaltered: • The integrity of documented information relates to its completeness and lack of alteration • Documents must be safe against unauthorised changes • Policies and procedures must specify what additions, alterations or redactions can be made to a document after it is created, under what circumstances these may be authorised, and which parties are authorised to manipulate them; any authorised additions, alterations or redactions must be explicitly shown, and fully audited and traceable Useable: • A useable document is one that the Entity can locate, retrieve, present and interpret • A document must be fully traceable to the business transaction that produced it • The metadata accompanying a document should carry the information needed to understand the transaction that created it, and the process that it followed • It should be possible to identify a record with the corresponding business activities that generated or modified it	
DCM.2.3	The Entity's implementation plans for document systems shall include: • Establishing a documents file plan • Establishing the repositories for Document and Content • Training staff in the use of the document repositories, procedures and policies • Transferring and if necessary converting documents to new documents systems • Establishing the standards and measuring compliance and performance against those standards • Establishing retention and disposal timelines • Ensuring document management strategies are part of the Entity's strategic plan • All systems and processes (manual and automated) should be designed, modified or redesigned so that documents can be created and captured as a routine part of undertaking business activities	M
DCM.2.4	When a document system or process is to be decommissioned, no new documents may be created in that system, but existing documents should remain accessible in accordance with retention, retirement and disposition policy. Alternatively, documents may be converted or migrated to a new system with their metadata (and those same policies) continued on the new system.	M
DCM.2.5	The Entity shall determine the appropriate retention policy for each document type based on: • An assessment of the business need • The regulatory environment • Accountability and audit requirements • The risks assessed • The right to privacy and data protection The rights, privileges, duties and interests of all stakeholders must be considered when making a determination on retention periods. Under no circumstances may a retention, retirement or disposal decision be made as a means to circumvent any rights of access or other legal requirements.	M

DCM.2.6	The Entity shall establish (unless already established under its Information Security Policy) a Document Classification scheme to: • Ensure all documents are consistently named over time • Enable the efficient retrieval of documents by function of business process etc • Determine the appropriate security provisions for that document type • Ensure access is correctly granted to use roles • Ensure the appropriate document management processes and active roles are selected for a given document type • Determine the appropriate retention, retirement and disposal policies for a document or document type	M
DCM.2.7	The Entity shall ensure correct retirement and disposal techniques are employed. No disposal should occur without the explicit knowledge that the record is no longer required (for work, evidence, support litigation etc. Appropriate retirement and disposal techniques may include: • The physical destruction of media, including overwriting and secure deletion • Retention for a further period within the Entity in an offline or nearline repository • Handover to an appropriate archive facility or body • Assignment to another Entity that has assumed responsibility in ongoing management	M
DCM.2.8	The Entity shall ensure that the document lifecycle and processes around its documents and content are clearly documented and regularly reviewed.	M
DCM.2.9	The Entity shall regularly undertake monitoring and compliance checking to ensure that document systems and processes are implemented in accordance with established policies and standards. The review should include coverage of, but not be limited to: • Performance of the document management processes • Compliance with the retention, retirement and disposal policies (including maximum, total and average variances) • User satisfaction	M
DCM.2.10	The Entity shall establish, maintain and review an ongoing training and awareness programme for document and content management establishing: • The training requirements for roles and individuals • The policies and processes around the documents • The legal and regulatory framework • The document systems and how they are used Training records should be retained, and refresher training be carried out at regular intervals (annually being recommended)	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DCM.1 Document and Content Quality Standards	
References	Requirements for Electronic Records Management Systems (2002)	

DCM.3	**Document and Content Tools**		**Version**	1
			Suggested Priority	2
Control Standards	The Entity shall implement appropriate repository and workflow management tools			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification				**M/R**
DCM.3.1	The solution chosen by the Entity shall: • Enable the building and maintenance of classification scheme • Enable the management of folders and documents • Enable the management of metadata associated with folders and documents • Manage versioning of documents and records • Manage the transitions from documents to records • Search and retrieve documents and records • Consistently manage and enforce the document retention, retirement and disposal policies for document types and classifications • Manage the multiple policies that may be inherited from standard policies, document classification and other sources • Manage access to folders and documents as well as their metadata for appropriate roles • Maintain a log of access and an audit of actions on documents and records • Provide an interface that enables and promotes the proper management of documents without excessive or onerous burden on the existing processes			M
DCM.3.2	The Entity may refer to related international standards when selecting a software platform for Document management.			M
Control Version History				
1.0				
Control Dependencies	DG.3 Data Management Programme DA.3 Data Target Architecture DA.4 Data Architecture Roadmap DS.3 Data Storage Roadmap DCM.1 Document and Content Quality Standards DCM.2 Document and Content Requirements			
References	Requirements for Electronic Records Management Systems (2002)			

14.13 IMPLEMENT: Data Warehouse, Business Intelligence and Analytics

DWBA.1	Data Warehouse, Business Intelligence and Analytics Business Goals		Version	1
			Suggested Priority	2
Control Standards	The Entity shall develop a data warehouse, BI and analytics effort that aligns with business goals and data management domains			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DWBA.1.1	The Entity shall ensure that any data warehouse, business intelligence and analytics initiative is driven by a clear business vision. Data warehouse, business intelligence and analytics initiatives – whether or not designated as having 'enterprise' scope – represent large, complex streams of work that typically require significant time and financial investment. The Data Governance Board shall be the key stakeholder in the outcome of any such initiative.	M
DWBA.1.2	The Entity shall develop Service Level Agreements (SLAs) – determined by business requirements – to regulate and support stakeholders in their exploitation of data within the data warehouse. Data warehouse SLAs shall include at a minimum: • Data warehouse availability – when and how often the data within the data warehouse will be available for querying eg there may be routine scheduled unavailability due to batch loads and processing • Data load latency – the period between data appearing in an operational system and being available for query within the data warehouse • Data retention period – the period of time that any given data will be retained in the data warehouse • Data quality – the minimum quality requirements for data stored in the data warehouse (see Data Quality Standards)	M
DWBA.1.3	The Entity shall monitor the effectiveness of the data warehouse initiative in order to meet and report against the requirements of the established SLA. Reporting shall also reflect the level of technical alignment with the architectural roadmap, implementation and usage experiences, lessons learned, and business successes. Findings shall be reported to the Data Governance Board to facilitate the sharing of experiences across Abu Dhabi Government Entities.	M
DWBA.1.4	The Entity shall agree SLAs with external data suppliers (see Data Integration and Interoperability standards) in order to provide the Entity with confidence when relying upon externally produced and managed datasets. Externally supplied authoritative data shall: • Be managed and stored separately from the data produced within the Entity • Have clear ownership both within the Entity, and within the external supplier • Have defined issue resolution workflow • Have documented data refresh cycles • Have clearly defined data quality requirements and other performance metrics	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DG.6 Capability Audit
References	Data Warehouse Governance (Walker, 2007) DMBOK (Mosley and Brackett, 2010)

DWBA.2	Data Warehouse, Business Intelligence and Analytics Architecture		Version	1
			Suggested Priority	2
Control Standards	The Entity shall ensure that data warehouse, business intelligence and analytics architecture uses the appropriate architectural components			
Control Type	Directive ☑	Preventive ☑	Detective ☐	Corrective ☐

Control Specification		M/R
DWBA.2.1	The Entity shall employ a data-staging environment to collect source system data for cleansing, matching, and merging (as appropriate) before adding it into the data warehouse. A data-staging environment might be a stand-alone intermediary data store, part of a Master Data Management system (see Reference and Master Data Management Standards) or implemented within tooling for Extract, Transform and Load (ETL).	M
DWBA.2.2	Data warehouse, business intelligence and analytics initiatives typically depend on many aspects of data management. The Entity shall ensure that these initiatives take appropriate account of other domains, which may include: • Metadata – to describe the types, formats and definitions of data contained within the warehouse • Data Catalogue – to document the content the datasets contained within the warehouse • Data Modelling and Design – to model the data contained within the warehouse • Data Architecture – to align with target data architecture, enterprise architecture, business processes and functions, and existing components within the baseline data architecture • Data Quality – to control and determine the quality of data contained within the warehouse • Data Security – to protect the data contained within the warehouse (as with any system, the data within data warehouses can be commercially sensitive; however, given the high volumes, the commercial sensitivity of data can be amplified within the context of a data warehouse) • Data Storage – to ensure the appropriate physical components and infrastructure required to support the storage of data is provisioned and managed, and also to govern the information lifecycle • Data Integration and Interoperability – feeding data from source information systems into the data warehouse should use the Entity's standard integration technology	M

	• Master Data Management – merged, matched and de-duplicated authoritative master profile records from across the Entity's information systems • Reference Data Management – static, versioned, mapped and transformed reference data that annotates records brought into the data warehouse • Open Data – analytical datasets and reports may be candidates for release under the Entity's Open Data policy	
DWBA.2.3	The Entity should explore the feasibility of sourcing and using external data to enrich the data it owns, in order to maximise business intelligence. Examples of external data might include, but is not limited to: • Static historical data feeds, such as historical weather or traffic data • Live data, such as the results from social media sentiment analysis	R
DWBA.2.4	The Entity shall prefer Commercial Off The Shelf (COTS) or Open Source tooling in preference to internally developed tooling. Where there is a decision to develop tooling internally, justification shall be provided through the governance checkpoint process.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.3 Business Glossary and Data Dictionary DM.5 Enterprise Data Model DM.6 Conceptual Data Models DM.7 Master Profiles DA.3 Target Data Architecture DA.4 Data Architecture Roadmap DQ.1 Data Quality Plan DQ.2 Data Quality Audit DQ.3 Data Quality Uplift DSP.1 Information Security Standards DS.3 Data Storage Roadmap DWBA.1 Data Warehouse, Business Intelligence and Analytics Business Goals	
References	The Data Warehouse Lifecycle Toolkit 2nd Edition (Kimball et al, 2008)	

DWBA.3	**Data Warehouse Design and Modelling**	**Version**	1
		Suggested Priority	2
Control Standards	The Entity shall design and model data warehouses and data marts using accepted conventions		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☑
Control Specification			**M/R**
DWBA.3.1	The Entity shall implement data warehouse architectural designs that favour usability over ease of implementation. Implementation complexity should also be considered. An incremental business-focused approach towards developing a data warehouse capability (including populating it with data) is recommended. Each Entity master profile might represent a suitable candidate segment of data to be cleansed and moved into the warehouse. The Data Governance Board shall require the Entity to submit data warehouse design proposals for evaluation and approval.		M
DWBA.3.2	The Entity shall use special-purpose table types when modelling the data warehouse. Conceptual, logical and physical modelling shall be undertaken to enhance understanding by stakeholders with varying levels of technical knowledge. Data warehouse table types include: • Data staging tables – containing the data from source information systems prior to processing • Dimension tables – containing the objects required by the business for reporting purposes (typically, these objects will include date and text-based fields, such as Citizen, Address, Service, Service Outcome Type etc) • Fact tables – containing measures, usually in numeric form, that may be the result of processing relationships in the input data eg the count and/or average of service outcome types by district for a given date period. In addition to measures, fact tables may also contain metadata to describe dimensions of the data. Such metadata might include (though not be limited to) source system, date of data capture, and other information to provide traceability and validity as appropriate. Fact tables link to multiple dimension tables		M
DWBA.3.3	Dimension tables should have synthetic or surrogate primary keys to support performance optimisations.		R
DWBA.3.4	The Entity shall use the simplest schema possible when designing a data warehouse or data mart. Star schemas are the simplest schemas for end users to understand, and should be the preferred choice. A star schema contains a single fact table with a single primary key relationship with each of the dimension tables. The fact table is at the centre of the star with the dimensions forming the points. Where a design deviates from a star schema, justification shall be provided in the design, for evaluation by the Data Governance Board through the Governance Checkpoint Process.		M

DWBA.3.5	The Entity should attempt to conform dimensions for reuse across multiple fact tables. A conformed dimension is one that is identical for different subject areas. For example, the Time Period dimension – which may contain a combination of week/month/year – may be applied to multiple fact tables. This supports both a gradual development of multiple star or snowflake schemas within a data warehouse, and the ability to provide multiple data marts with the same dimensions.	R
DWBA.3.6	The Entity shall ensure that sources for data calculations are present and maintained in the data warehouse, and are managed through audited workflows.	M
DWBA.3.7	The Entity shall develop performance metrics to control the quality, volume and timeliness of the data within the data warehouse.	M
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DM.5 Enterprise Data Model DM.7 Master Profiles DM.8 Logical Data Model DM.9 Physical Data Model DWBA.2 Data Warehouse, Business Intelligence and Analytics Architecture	
References	DMBOK (Mosley and Brackett, 2010) The Data Warehouse Lifecycle Toolkit 2nd Edition (Kimball et al, 2008)	

DWBA.4	**Data Marts**		**Version**	1
			Suggested Priority	2
Control Standards	The Entity shall consolidate its Data Marts into a federated Data Warehouse			
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐
Control Specification				**M/R**
DWBA.4.1	The Entity shall normalise data warehouse tooling and technology to consolidate departmental Data Marts into a federated data warehouse. A federated data warehouse consists of a number of data marts, each for analysing a single business subject. The federated data warehouse uses common tooling for data input (eg ETL), processing and analysis: • Common data staging tools for data load, validation, cleansing, and transformation to populate the data marts • Managed reference and master data across all the data marts • Common data warehouse technology platform for storing and processing facts and dimensions across all data marts • Common tools for data access, analysis and reporting across all data marts			M

DWBA.4.2	The Entity shall include on their data architecture roadmap the timeline for consolidating data marts across the organisation into a federated data warehouse. Where data marts exist on different technology platforms, the Entity shall develop and execute a plan for migrating to a single data warehouse platform.	M
DWBA.4.3	The Entity shall normalise and reuse dimensions across data marts, enabling reuse of data processing and allowing reporting across the breadth of data in the data warehouse.	R
DWBA.4.4	The Entity shall identify the most effective and utilised data marts within the organisation in order to develop the Entity's maturity and personal competancy across the range of data marts within the Entity.	R
Control Version History		
1.0		
Control Dependencies	DG.3 Data Management Programme DQ.1 Data Quality Plan DQ.2 Data Quality Audit DQ.3 Data Quality Uplift DSP.1 Information Security Standards DWBA.1 Data Warehouse, Business Intelligence and Analytics Business Goals DWBA.2 Data Warehouse, Business Intelligence and Analytics Architecture DWBA.3 Data Warehouse Design and Modelling	
References	DMBOK (Mosley and Brackett, 2010) Data Warehousing, The Keys for a Successful Implementation (Pitney Bowes, 2010)	

DWBA.5	**Operational Data Stores**		**Version**	1
			Suggested Priority	2
Control Standards	The Entity shall distinguish between an Operational Data Store and a Data Warehouse in its data architecture			
Control Type	Directive ☑	Preventive ☐	Detective ☑	Corrective ☐
Control Specification				**M/R**
DWBA.5.1	Where an operational data store (ODS) exists as an architectural component on the Entity's data architecture, it shall act as a data source for the enterprise data warehouse.			M
DWBA.5.2	The Entity should ensure a clear separation between data for an ODS and data within a data warehouse (both use similar technology and processes – such as dimensional modelling and de-normalisation – but to different ends. An ODS is designed to contain current, operationally volatile data). For example, both an ODS and data warehouse could contain the current address for a Citizen. If the address changes, a single record would usually be updated within the ODS, whereas both address versions would be stored within the data warehouse, with each being indicated as correct at different ranges of time.			R
DWBA.5.3	The Entity should use the capability of an ODS to integrate, analyse and report on current data from across the organisation, where the functionality meets the business requirements.			R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DQ.1 Data Quality Plan DQ.2 Data Quality Audit DQ.3 Data Quality Uplift DSP.1 Information Security Standards DWBA.1 Data Warehouse, Business Intelligence and Analytics Business Goals DWBA.2 Data Warehouse, Business Intelligence and Analytics Architecture DWBA.3 Data Warehouse Design and Modelling
References	DMBOK (Mosley and Brackett, 2010) Data Warehousing, The Keys for a Successful Implementation (Pitney Bowes, 2010)

DWBA.6	**Business Intelligence**	**Version**	1
		Suggested Priority	2
Control Standards	The Entity shall develop Business Intelligence solutions that align with business goals		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		**M/R**
DWBA.6.1	Throughout the design and development of business intelligence solutions, the Entity shall ensure that realistic data is used to provide clarity when engaging with business stakeholders. Furthermore, reference shall be made to the Entity's data dictionary and business glossary. Business intelligence solutions are architectural components that provide users with reporting, investigation and drill-down and discovery functionality on data available in the data warehouse. Decision makers, subject matter experts and technical specialists shall collaborate, and make use of actual data (ie rather than test data) so as to derive the most value from reports and dashboards. Exploratory and investigative proof-of-concept implementations can be developed iteratively as the business need emerges. Business intelligence initiatives shall report to the Data Governance Board through the Governance Checkpoint Process, and should be presented in the form of an executive summary of the issues raised in order to demonstrate suitable engagement across the organisation.	M
DWBA.6.2	The Entity shall classify business intelligence initiatives according to type, in order to locate them appropriately within the Entity's data architecture roadmap. These types include: • Tactical Business Intelligence – to support short-term business decisions eg a spike in service usage recurring in the same month in each of the previous three years might suggest the need to plan for a similar spike in the following year • Strategic Business Intelligence – to provide enterprise-level reporting to facilitate Entity performance measurement and long-term decision making eg showing a rapid increase in mobile access of services through the Entity's website might lead to a change of target data architecture to micro-services, provide a business case for investment in mobile apps, and reassignment of front-line staff to handle data from mobile service use • Operational Business Intelligence – to support operational business decisions eg observing a steady increase in service usage in the run up to a major event might lead to an operational decision to a temporary increase in front-line staffing levels. Operational business intelligence systems are tied to business functions and usually require a relatively more complex architecture to facilitate near real-time requirements. Before embarking on such a project, the Entity shall present a comprehensive analysis of the requirements, and the impact of implementing an operational business intelligence architecture for approval by the Data Governance Board	M
DWBA.6.3	The Entity should ensure that business intelligence reporting integrates with any existing enterprise reporting solution, or else becomes established as the enterprise reporting solution. Enterprise reporting is a separate concern from application reporting. Application reporting is typically employed to produce reports such as invoices and statements to external service users. Though not mandated by these standards, it may be desirable to standardise application reporting across the organisation. In contrast, enterprise reporting provides the ability to develop dashboards, interactive drill-down within datasets, and ad hoc queries against the data stored in the data warehouse. The enterprise reporting solution is an architectural component that should be modelled appropriately (using techniques described in the Data Architecture and Data Modelling standards). The Entity shall use the Governance Checkpoint Process to verify architectural alignment with Enterprise reporting solutions for any Business Intelligence initiative.	R
DWBA.6.4	The Entity shall refrain from using non-authoritative Volunteered Geographical Information (VGI) in compliance with government directives. Non-authoritative VGI includes Google Maps, Bing Maps and other base map data. The same base map data shall be used for all location-based analytics across government and is provided to Entities by the ADSIC Spatial Data Centre.	M
DWBA.6.5	The Entity shall use business intelligence tooling to produce key performance indicators, dashboards and scorecards that show their business objectives. KPIs and metrics include (but are not limited to): • Financial and budgetary indicators • Customer satisfaction levels • Service delivery effectiveness	M
DWBA.6.6	The Entity shall develop and publish statistical data in line with the Statistics Centre Abu Dhabi (SCAD) requirements. Where statistical data is provided by SCAD for the purposes of enriching Entity data, a service level agreement as described in DWBA.1.4 shall be produced.	M

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DA.3 Target Data Architecture DA.4 Data Architecture Roadmap DSP.1 Information Security Standards DSP.5 Data System Protection DWBA.1 Data Warehouse, Business Intelligence and Analytics Business Goals DWBA.2 Data Warehouse Architecture
References	DMBOK (Mosley and Brackett, 2010) North Carolina Government BI Competency Center Programme (North Carolina Office of the State Controller, 2013)

DWBA.7	Analytics and Big Data	Version	1
		Suggested Priority	2
Control Standards	The Entity shall provide Analytics and Big Data tooling and training to encourage innovation and to develop analytics capabilities		
Control Type	Directive ☑	Preventive ☐	Detective ☐	Corrective ☐

Control Specification		M/R
DWBA.7.1	The Entity should produce a initiative to develop data analysis capabilities suitable for the types of data within its ownership. The Entity shall evaluate suitable training opportunities within its Data Management Programme and its roadmap for data architecture, in order to enhance the Entity's data analytics capabilities. Data analysis techniques include, but are not limited to: • Machine learning – information systems that develop understanding of patterns within the data without being explicitly programmed • Clustering algorithms – to identify groups of data variables that influence each other • Classification and regression – attempting to automatically classify new data on the basis of known historic data Data analytics development and usage is more ad hoc than typical business intelligence activities, and must be undertaken in collaboration with business users.	R
DWBA.7.2	The Entity should identify data that is very high in volume, velocity or variety, and apply 'Big Data' analysis techniques to encourage innovation. While the term 'Big Data' is imprecise, typically it identifies data that cannot be processed using traditional data analysis capabilities. The Entity shall identify Big Data initiatives in order to document and share experiences through the Data Governance Board to other Entities.	R
DWBA.7.3	The Entity should implement event stream-based analytical processing to support high velocity data analysis. Event processing allows time-window analysis of data (typically, data produced from automated sensors eg temperature gauges, crowd monitors or traffic sensors). Stream-based analytics resulting from event processing allow near real-time reporting of event trends. The Data Governance Board shall evaluate justification for implementation of this technology as suitable business requirements emerge.	R

Control Version History	
1.0	
Control Dependencies	DG.3 Data Management Programme DA.3 Target Data Architecture DA.4 Data Architecture Roadmap DSP.1 Information Security Standards DSP.2 Data Privacy Policy DSP.3 Privacy By Design DSP.4 Privacy Management DSP.5 Data System Protection DS.4 Storage Roadmap Implementation DWBA.1 Data Warehouse, Business Intelligence and Analytics Business Goals DWBA.2 Data Warehouse, Business Intelligence and Analytics Architecture DWBA.3 Data Warehouse Design and Modelling
References	Better Practice Guide for Big Data (Data Analytics Centre of Excellence, 2014) Big Data Strategy (Australian Government Information Management Office, 2013)

15. Appendices

15.1 Glossary of Terms

Checkpoint: A point within a business process where rationales, justifications, decisions, designs and other deliverables are subject to external scrutiny, for example, when budget is requested; when requirements gathering is complete; when design is complete (see also **Governance Checkpoint Process**)

Common Profile: A government-wide data profile, applicable to many government Entities, containing fields, attributes, validations, descriptions and reference data (see also **Master Profile**)

Component: A technology element that by itself does not form an information system, but forms part of a wider information system (see also **Information System**)

Conceptual Data Model: The high-level concepts and their relationships within an information system

Data Architecture: A set of deliverables that show the how (at various levels of detail depending upon the audience) information systems store data at rest facilitate the movement of data between information systems. Data architecture is part of a wider Enterprise Architecture (see also **Enterprise Architecture**)

Data Feed: A data source exposing a dataset as a service (see also **Dataset, Data Source**)

Data Governance Board: The board formed within the Entity to provide oversight of the data management programme and ensure information systems adhere to these controls (see also **Checkpoint, Governance Checkpoint Process**)

Data Governance Committee: The government-wide committee formed from representatives from across the Abu Dhabi Government Entities

Data Manager: The person with responsibility for executing the data management programme, under the direction of the data governance board

Data Mart: Subject-based data analytical tool (or tools) that may join other data marts to form a data warehouse (see also **Data Warehouse**)

Data Object: A modelled data entity within an Entity Relationship Diagram

Dataset: A discreet set of data, comprising multiple records. An information system may contain, use or maintain one or more datasets. A dataset may be published outside the information system that created it (see **also Data Source**)

Data Source: A source system that provides a dataset for re-use (see also Information System)

Data Steward: A technology or business expert with understanding of the datasets and information systems, with responsibility for implementing the requirements data management programme under the direction of the Data Manager (see also **Data Manager**)

Enterprise Architecture: The design and management of business, technology and governance across the Entity's information systems and business processes (see also **Data Architecture**)

Enterprise Data Model: A combination of the Entitiy's Conceptual Data Models, Logical Data Models and Physical Data Models describing the data its relationships that are core to the organisations function (see also **Conceptual Data Model, Master Profile**)

Enterprise Information System: An information system that crosses departmental boundaries to use and/or maintain data from across the Entity, for example, Master Data Management systems or a Data Warehouse (see also **Information System**)

Enterprise Integration Platform: An enterprise-wide architectural component to facilitate the successful, secure, audited transfer of data between information systems (see also **Component, Data Architecture, Enterprise Information System**)

Governance Checkpoint Process: The set of checkpoints defined by the data governance board for confirming an information systems compliance with these controls as it progresses through its lifecycle (see also **Checkpoint, Data Governance Board**)

Information System: An installed or developed application or group of applications working together to complete a discreet business process (see also **Component, Enterprise Information System**)

Integration Patterns: Pre-defined and document industry models for enabling data transfer between information systems (see also **Enterprise Integration Platform**)

Logical Data Model: The information system independent data model, documenting the tables, relationships and rules that form the full range of data used by an information system

Master Data Management (MDM): A set of tools and business processes by which master profile data from multiple systems can be compared, matched and merged (logically or physically) in order to create a 'golden view' of each record (see also **Master Profile**)

Master Profile: An Entity wide data profile used across many departments in order to fulfil the Entity's core business, containing fields, attributes, validations, descriptions and reference data. Entity master profiles should align with the government-level Common Profiles as they emerge (see also **Common Profile**)

Open by Default: An Open Data principle that allows sharing and publishing data managed by the Entity unless there is sufficient justification not to

Physical Data Model: A physical implementation of a Logical Data Model constrained by specific vendor hardware and software

Privacy by Design: A set of design principles that ensure the privacy of personal information is managed through the information systems implementation and associated processes

Reference Data Management (RDM): A set of tools and business processes for versioning, refreshing, transforming and distributing to information systems the reference data developed both internally and externally

Recovery Point Objective (RPO): A defined objective for disaster recovery that limits the volume of data (in terms of new or changed data) that would potentially be lost in the event of a disaster (see also **Recovery Time Objective**)

Recovery Time Objective (RTO): A defined objective for disaster recovery that limits the amount of downtime or service outage when recovering data in accordance with the Recovery Point Objective (see also **Recovery Point Objective**)

Semantic Definitions: Forms of metadata that go beyond defining, and add meaning to data entities

Semantic Modelling: Modelling where a meaning as well as a definition is attached to an entity, which in turn allows non-human interrogative actors to make judgements on the value of including data they access. For example 'Country name' may be a definition, but 'developing country' adds meaning

15.2 Example Roles and Responsibility Matrix

A number of key roles are required to implement a data management programme that successfully transitions into a 'business as usual' steady state. These roles and their responsibilities are as follows:

	Accountable	Responsible	Consulted	Informed
Policy Development	Chair – Data Governance Board	Data Manager	Data Architect Enterprise Architect Subject Matter Experts Data Owner Data Steward	Data Governance Committee Programme Manager Project Manager Data Architect Enterprise Architect Subject Matter Experts Data Owner Data Steward
Policy Compliance	Chair – Data Governance Board	Data Manager Programme Manager Data Architect Enterprise Architect	Programme Manager Project Manager Architects SME Data Owner Data Steward	Data Governance Committee
Policy Training and Awareness	Chair – Data Governance Board	Data Manager Programme Manager	HR Project Manager	Staff
Effectiveness Monitoring	Chair – Data Governance Board	Data Manager	Programme Manager Project Manager Data Architect Enterprise Architect Subject Matter Experts Data Owner Data Steward	Data Governance Committee
Policy Revision Deve1. lopment	Chair – Data Governance Board	Data Manager	Data Architect Enterprise Architect Subject Matter Experts Data Owner Data Steward	Data Governance Committee Programme Manager Project Manager Architects Subject Matter Experts Data Owner Data Steward
Policy Approval	Chair – Data Governance Board	Data Manager	Data Architect Enterprise Architect Subject Matter Experts Data Owner Data Steward	Data Governance Committee Programme Manager Project Manager Architects Subject Matter Experts Data Owner Data Steward

15.3 References and Bibliography

ADSIC. (2009). Abu Dhabi Government Interoperability Framework (eGIF). Abu Dhabi Government.

ADSIC. (2013). Abu Dhabi Information Security Standards. Abu Dhabi Government.

Agency of Digitalisation, (2012). Good Basic Data for Everyone. Copenhagen: Danish Ministry of Finance.

Alasem, A. (2009). An overview of e-government metadata standards and initiatives based on Dublin Core. Electronic Journal of e-Government, 7(1), pp.1–10.

Data Analytics Centre of Excellence, (2014). Better Practice Guide for Big Data. Australian Government.

Department of Homeland Security, (2009). Government 2.0: Privacy and Best Practices. DHS Privacy Office.

Dublincore.org, (2014). DCMI Home: Dublin Core® Metadata Initiative (DCMI). [Online]. Available at: http://dublincore.org/ [Accessed 2 April 2014].

European Commission, (2012). Building Semantic Interoperability in Europe.

European Commission, (2012a). Case Study Digitalisér.dk Semantic Asset Repository. ISA.

European Commission, (2012b). Case Study XRepository semantic asset repository. ISA.

Cabinet Office, (2010). G-Cloud Overview.

Griffin, J. (2010). Four Critical Principles of Data Governance Success. [Online]. Information Management Magazine. Available at: http://www.information-management.com/issues/20_1/four-critical-principles-of-data-governance-success-10016929-1.html [Accessed 12 May 2014].

HM Government, (2012). UK Government Reference Architecture (UKRA).

HM Government. (2002). Requirements for Electronic Records Management Systems.

Hohpe, G & Woolf, B (2003) Enterprise Integration Patterns: Addison-Wesley.

IBM. (2012). Three guiding principles to improve data security and compliance: IBM Corporation, Somers.

IBM Redbooks, (2013). Reference Data Management. 1st ed. [e-book] IBM Redbooks. Available at: http://www.redbooks.ibm.com/technotes/tips1016.pdf [Accessed 19 June 2014].

Indiana Health Information Exchange, (2012). Building Effective Data Governance Models, Policies, and Agreements in a Hi Tech world.

Informatica, (nd). Master Data Management in Government.

ISO/IEC, (2004). ISO/IEC 11179-1 Information Technology - Metadata Registries. ISO/IEC.

ISO/TS (2009-2011), ISO8000 Data Quality: ISO/IEC

ISO/IEC (draft). ISO 27017 Cloud Security Standards: ISO/IEC

ISO/ISC (draft). ISO 27018 Handling of Personally Identifiable Information: ISO/IEC

ISO/IEC (2012). ISO 22301 Business Continuity Management Systems: ISO/IEC

ISO/IEC (2001) ISO 15489-1:2001 Information and documentation: ISO/IEC

Joohaeng, C. (2010). Case Study and Best Practices of e-Government Interoperability in Korea. 1st ed. [e-book] Samsung SDS. Available at: http://www.gobiernofacil.go.cr/e-gob/gobiernodigital/Foro_Ddigital/presentaciones/e_Government_Interoperability_in_Korea.pdf [Accessed 19 June 2014].

Kimball, Ross et al (2008). The Data Warehouse Lifecycle Toolkit 2nd Edition, Wiley.

Ladley, J. (2012). Data governance. 1st ed. [S.l.]: Morgan Kaufmann.

Lees, K (2012). Organizing for the Cloud: VMWare Inc [Online], Available at:
http://www.vmware.com/files/pdf/services/VMware-Organizing-for-the-Cloud-Whitepaper.pdf
[Accessed 8 October 2014].

Maali, F., Cyganiak, R. and Peristeras, V. (2010). Enabling Interoperability of Government Data Catalogues.
Galway: National University of Ireland.

Mosley, M. and Brackett, M. (2010). The DAMA guide to the data management body of knowledge
(DAMA-DMBOK guide). 1st ed. Bradley Beach, N.J.: Technics Publications.

ncia.go.kr, (2012). Korea›s Government Data Centre Consolidation.

OASIS. (2009). Unstructured Information Management Architecture (UIMA). [Online].
https://www.oasis-open.org/committees/uima/ [Accessed 7 Aug 2014].

OMG. (2003). Common Warehouse Metamodel (CWM). [Online].
http://www.omg.org/spec/CWM/1.1/ [Accessed 2 June 2014]

Open Knowledge Foundation. (2014). The Open Data Handbook. [Online]. Available at:
http://opendatahandbook.org/ [Accessed 23 June 2014].

Opengroup.org, (2014). The Open Group Application Framework (TOGAF). [Online]. Available at:
http://www.opengroup.org/togaf/

Pitney Bowes, (2010). Data Warehousing, The Keys for a Successful Implementation. Business Insight Series.
Pitney Bowes Insight.

Privacy By Design, (2014). Privacy By Design. [Online]. Available at:
http://www.privacybydesign.ca [Accessed 11 May 2014].

Project-open-data.github.io, (2014). Project Open Data. [Online]. Available at:
http://project-open-data.github.io [Accessed 19 June 2014].

PCI Security Standards Council (2013) Data Security Standards. [Online], Available at:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf [Accessed 23 Oct 2014].

Soares, S. (2010). The IBM data governance unified process. 1st ed. Ketchum, ID: MC Press Online.

Telecommunications Industry Association (2005). Telecommunications Infrastructure Standard for Data Centers.
[Online], Available at: http://manuais.iessanclemente.net/images/9/9f/Tia942.pdf
[Accessed 12 October 2014].

The MDM Institute, (2012). Field Report: Orchestra Networks Reference Data.

Troy, C. and Ellis, T. (2008). Best Practice Guide for MDM Implementations. London Data Connects.

W3.org, (2014). Data Catalog Vocabulary (DCAT). [Online]. Available at:
http://www.w3.org/TR/vocab-dcat/ [Accessed 2 April 2014].

W3C Government Linked Data Working Group, (2013). Asset Description Metadata Schema (ADMS). [Online].
Available at: http://www.w3.org/TR/vocab-adms/ [Accessed 20 May 2014].

W3C RDF Working Group (2014), Resource Description Framework (RDF). [Online]. Available at:
http://www.w3.org/RDF/ [Accessed 20 May 2014].