CDMC Controls Procedures and Test Specifications

Version 1.1.1
October 2021

edmcouncil.org/page/CDMC

EDMCouncil

CDMC™ Terms of Use

This document is a constituent part of the Cloud Data Management Capabilities (CDMC™) model ("the Model") and is provided as a free license to any organization registered with EDM Council Inc. ("EDM Council") as a recipient ("Recipient") of the document. While this is a Free License available to both members and non-members of the EDM Council, acceptance of the CDMC Terms of Use is required to protect the Recipient's use of proprietary EDMC property and to notify the Recipient of future updates to the Model.

CDMC™ and all related materials are the sole property of EDM Council Inc. All rights, titles and interests therein are vested in the EDM Council. The Model and related material may be used freely by the Recipient for their own internal purposes. It may only be distributed beyond the Recipient's organization with prior written authorization of EDM Council. The Model may only be used by the Recipient for commercial purposes or external assessments if the Recipient's organization has entered into a separate licensing and Authorized Partner Agreement with EDM Council governing the terms for such use.

Feedback and Additional Information

Proposals of change and improvement to the Controls Procedures and Test Specifications are welcomed and should be provided via the following on-line form:
https://forms.monday.com/forms/342ed5577937d03d7cf5ef39a6e72e0a?r=use1

For further information on the CDMC initiative please visit: https://edmcouncil.org/page/CDMC. Any enquiries regarding EDM Council membership or CDMC Authorized Partnership should be directed to info@edmcouncil.org.

Acknowledgements

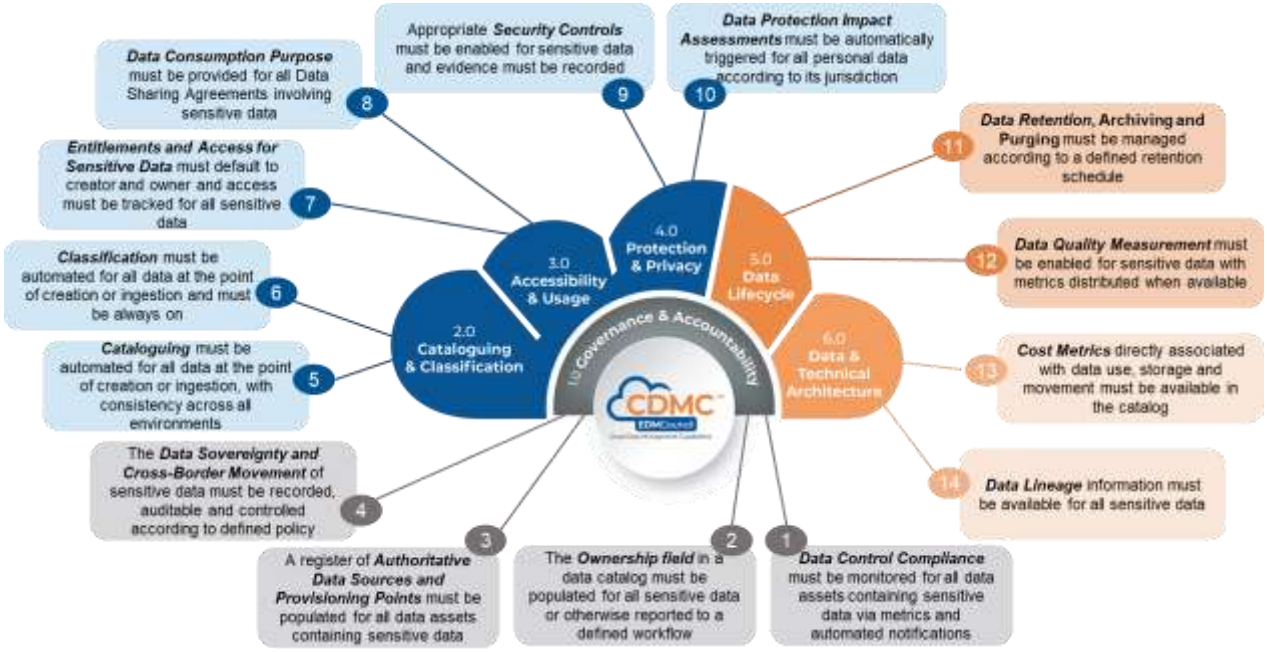
EDM Council would like to acknowledge the contribution of KPMG and Snowflake in proposing draft procedures and test specifications, and the work of the CDMC Go-to-Market Committee in reviewing and finalizing these.

CONTENTS

INTRODUCTION

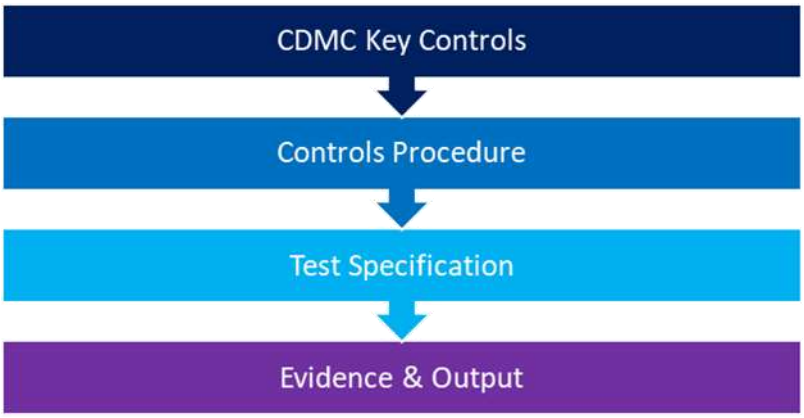
KEY CONTROLS OVERVIEW

The key controls are summarized in the following diagram:



CONTROLS PROCEDURES AND TEST SPECIFICATIONS OVERVIEW

The procedures and test specifications within this document provide the basis for the Certification of cloud platforms and solutions against the CDMC Key Controls within the CDMC Framework. The diagram below represents the overall process flow from the controls, through procedures and specifications to evidence and outputs.



INITIAL PROCEDURE FOR MULTIPLE CONTROLS

The following test procedures are recommended as an initial set of pre-requisites to reduce redundancy in the test steps per each control. It is understood that for the benefits of CDMC controls to be leveraged to achieve their full value, that a data catalog is a key component, and specific functionality should be enabled to effectively meet each control and attain the full automation benefits.

Controls Pre-requisite	Establish data catalog and enable metadata discovery
Procedures Impact	Many of the procedures require a data catalog to be in place and metadata discovery to be enabled as part of the initial test steps
Procedure Assumptions	Where more than a few controls are to be tested, this procedure can be executed once covering all controls, avoiding repetition in the testing for each control.
Control Dependencies	• Data assets are established • Catalog is established • Environment with metadata scanning enabled and scheduled
Test Specification	1. Determine data catalog is established 2. Create data catalog entries with sufficient metadata attributes populated to support all controls being assessed 3. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule

CONTROL & PROCEDURE 1: DATA CONTROL COMPLIANCE	
Component	**1.0 Governance & Accountability**
Capability	**1.1 Cloud data management business cases are defined and governed**
Control Description	**Data Control Compliance** must be monitored for all data assets containing sensitive data via metrics and automated notifications. The metrics must be calculated from the extent of implementation of the CDMC Key Controls specified in subsequent sections.
Assessment Procedure	Confirm the availability of metrics that demonstrate the extent of implementation of all other Key Controls and the automation of notifications when metrics do not meet defined thresholds.
Procedure Assumption	This procedure targets the calculation and reporting of metrics on subsequent controls and procedures in this document. Calculation of metrics may be automated or manual (by inspection). Reporting of metrics outside threshold limits must be automated.
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to confirm where data assets are classified as sensitive that they comply with all CDMC Key Controls.
Control Dependencies	• Tracking and reporting of CDMC controls for sensitive data assets.
Test Specification	1. Confirm data asset controls are continuously operational and tracked for sensitive assets for all other CDMC controls. 2. Generate report/dashboard that presents the metrics for sensitive data controls. 3. Confirm the ability to set an escalation threshold for each metric. 4. Test the automated reporting against threshold limits: 4.1 Impact the effectiveness of a Key Control in a manner that causes a metric threshold to be outside threshold limits. 4.2 Confirm the automated reporting of the move outside threshold limits.
Data Requirements	• Metadata data catalog and data assets classified as sensitive.
Evidence & Output	• Report evidencing all data assets, where classification is sensitive, comply with CDMC Key Controls.

CONTROL & PROCEDURE 2: OWNERSHIP FIELD	
Component	**1.0 Governance & Accountability**
Capability	**1.2 Data ownership is established for both migrated and cloud-generated data**
Control Description	The **Ownership field** in a data catalog must be populated for all sensitive data or otherwise reported to a defined workflow.
Assessment Procedure	Inspect the data catalog and classification to confirm data ownership is assigned to all sensitive data assets.
Procedure Assumptions	• The control recommends automation; however, an ad hoc report is sufficient as part of a regular data governance review. • It is accepted that organizations will likely have established preferences on ownership and/or stewardship for the roles and responsibilities, as long as either one is defined as part of policy, customization by the organization can be accepted as part of the control assessment. • The policy defines the level of detail for this control, whether that is at the database, schema or data element level of granularity; therefore the implementation and assessment is based on capability if level of granularity can be met, regardless of current policy (e.g. database but not implemented at data element).
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data ownership at the point of creation and/or classification of data assets as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established. • Catalog is established. • Classification and Ownership attribute is established for sensitive data. • Environment with metadata scanning enabled and scheduled.
Test Specification	1. Determine data catalog is established. 2. Create data catalog entries with ownership populated & ownership not populated. 3. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 4. Generate report using catalog metadata classification for ownership to determine whether populated or not populated. 4.1 Review report and identify data assets with no assigned ownership. 4.1.1 Confirm workflow automation where data assets containing sensitive data and with no owner defined are sent for remediation. 4.2 Review report and identify data assets with assigned ownership. 4.2.1 Verify that owners listed are active employees and the authorized owner per data asset.
Data Requirements	• Metadata data catalog and data assets classified as sensitive. • Environment populated with test data asset records.
Evidence & Output	• Report evidencing all data assets, where classification is sensitive, have data ownership metadata populated.

CONTROL & PROCEDURE 3: AUTHORITATIVE DATA SOURCES AND PROVISIONING POINTS	
Component	**1.0 Governance & Accountability**
Capability	**1.3 Data sourcing and consumption are governed and supported by automation**
Control Description	A register of **Authoritative Data Sources and Provisioning Points** must be populated for all data assets containing sensitive data or otherwise must be reported to a defined workflow.
Assessment Procedure	Inspect the data register to confirm it contains information on authoritative data sources and consuming users/distributors of the information or otherwise must be reported to a defined workflow.
Procedure Assumptions	The control recommends automation, however an ad hoc report is sufficient as part of a regular data governance review.
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data source to be populated at the point of creation and/or classification of data assets as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established. • Register of authoritative data sources and provisioning points. • Data assets that identified as either authoritative or non-authoritative. • Use of data assets can be logged and reported via metadata.
Test Specification	1. Determine data catalog is established. 2. Create data catalog entries and confirm authoritative / non-authoritative indication is populated in register of authoritative data sources 2.1. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 2.2. Confirm default setting is 'non-authoritative'. 3. Create a new data asset flagged as containing sensitive data. Confirm either: 3.1. Data asset is populated into register of authoritative data sources and provisioning points with appropriate indication of authoritative / non-authoritative, or 3.2. Workflow is triggered for remediation if data asset not recorded in the register.
Data Requirements	• Data assets classified as sensitive/critical data assets. • Register of authoritative sources and authorized distributors.
Evidence & Output	• Reporting/dashboard evidencing all data assets, where classification is sensitive, have an assigned authoritative source that can be found in the register.

CONTROL & PROCEDURE 4: DATA SOVEREIGNTY AND CROSS-BORDER MOVEMENT	
Component	**1.0 Governance & Accountability**
Capability	**1.4 Data sovereignty and cross-border data movement are managed**
Control Description	The **Data Sovereignty and Cross-Border Movement** of sensitive data must be recorded, auditable and controlled according to defined policy.
Assessment Procedure	Inspect data catalog/registry to observe region-specific storage classifications and usage rules for all sensitive data assets.
Procedure Assumptions	• Storage location and changes (via audit trail) are tracked to identify cross-border movement and the triggering of data sharing agreements where required. • The control applies to all environment types including development, test, production and archive.
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data ownership at the point of creation and/or classification of data assets as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established. • Data assets can identify region specific storage and usage specific rules. • Use of data assets can be logged and reported via metadata. • Use and movement of data assets can be logged and reported.
Test Specification	1. Determine data catalog is established. 2. Create data catalog entries with region specific storage and usage rules populated, and not populated. 3. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 4. Generate report using catalog metadata for current storage location & audit trail of movement: 4.1. Review Report and identify data assets classified as sensitive with no storage location specified. 4.2. Confirm workflow automation where data assets with no storage location defined are sent to for remediation. 5. Update data asset to new storage location: 5.1. Confirm trigger initiates for cross border data sharing agreements. 5.2. Confirm audit trail correctly recorded data movement. 6. Create new consumption of an existing asset from a new jurisdiction: 6.1. Confirm trigger initiates for cross border data sharing agreements. 6.2. Confirm audit trail correctly recorded data movement.
Data Requirements	• Data assets are classified and have data owners identified.
Evidence & Output	• Report of audit trail for data asset storage location, movements and data sharing agreements.

CONTROL & PROCEDURE 5: CATALOGING

Component	**2.0 Cataloging & Classification**
Capability	**2.1 Data catalogs are implemented, used, and interoperable**
Control Description	**Cataloging** must be automated for all data at the point of creation or ingestion, with consistency across all environments.
Assessment Procedure	Inspect to confirm existence and current usage of one or more data catalog(s); Confirm that metadata discovery & scanning is enable on select systems, applications, and reports where data assets captured in the cataloged.
Procedure Assumptions	N/A
BAU Procedure Frequency	Annual review to determine cataloging has been implemented, is being used, interoperable where required, and consistently maintained.
Control Dependencies	• Catalog is established. • Environment with metadata scanning enabled and scheduled.
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Create a new data asset: 3.1 Confirm the data catalog has generated a new entry for this data asset. 4. Update an existing data asset: 4.1 Confirm the data catalog has updated the data asset after the next regularly scheduled metadata scan completes.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Catalog is documented as in place and metadata discovery is enabled and configured.

CONTROL & PROCEDURE 6: CLASSIFICATION	
Component	**2.0 Cataloging & Classification**
Capability	**2.2 Data classifications are defined and used**
Control Description	**Classification** must be automated for all data at the point of creation or ingestion and must be always on. • Personally Identifiable Information auto-discovery • Information sensitivity classification auto-discovery • Material Non-Public Information (MNPI) auto-discovery • Client identifiable information auto-discovery • Organization-defined classification auto-discovery
Assessment Procedure	Inspect to confirm existence and current usage of one or more data catalog(s) and classifications are defined for all control description sensitive descriptions (e.g. PII, MNPI, etc.); Confirm that metadata discovery and scanning is enable on select systems, applications, and reports where data assets captured in the cataloged.
Procedure Assumptions	N/A
BAU Procedure Frequency	Annual or quarterly compliance is reviewed to require data classification at the point of creation where data asset is classified as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established. • Catalog is established. • Classification(s) is established. • Environment with metadata scanning enabled and scheduled.
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate report using catalog metadata classification in place for sensitivity and aligned to control description (e.g. PII, Information sensitive, MNPI, etc.): 3.1 Review report and identify data assets with no assigned sensitivity description: 3.1.1 Confirm that assignment of no sensitivity is correct. 3.2 Review report where sensitivity and description are defined: 3.2.1 Verify with random sample that sensitivity description is accurate for each data asset's classification. 4. Create a new data asset: 4.1 Confirm the data catalog has generated a new entry for this data asset and triggered classification completion. 5. Update an existing data asset in a way that changes the classification: 5.1 Confirm the data catalog has updated the data asset after the next regularly scheduled metadata scan completes.

Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Catalog is documented as in place, metadata discovery is enabled and populated with accurate data asset classification sensitivity categories.

CONTROL & PROCEDURE 7: ENTITLEMENTS AND ACCESS FOR SENSITIVE DATA	
Component	**3.0 Accessibility & Usage**
Capability	**3.1 Data entitlements are managed, enforced, and tracked**
Control Description	1. **Entitlements and Access for Sensitive Data** must default to creator and owner until explicitly and authoritatively granted. 2. Access must be tracked for all sensitive data.
Assessment Procedure	Inspect the data catalog and entitlement classification to confirm data entitlement is assigned to all sensitive data assets.
Procedure Assumptions	The control recommends automation. However, an ad hoc report is sufficient as part of a regular data governance review.
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data entitlement at the point of creation and/or classification of data assets as sensitive.
Control Dependencies	• Data assets are established. • Catalog is established. • Entitlement classification(s) is established for sensitive data. • Environment with metadata scanning enabled and scheduled.
Test Specification	1. Determine the data catalog is established. 2. Create data catalog entries with entitlement populated. 3. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 4. Generate report using catalog metadata for entitlement to determine whether populated or not populated: 4.1 Review report and identify data assets with assigned entitlement 4.1.1 Verify that data assets have alignment of data asset privileges mapped to user entitlements - check evidence that the entitlements are reflected in the access controls. 4.1.2 Verify users listed are active employees and the entitlements are granted per data asset. 4.2 Confirm workflow automation where data assets with no entitlements defined are sent to for remediation. 5. Create new data asset: 5.1 Confirm entitlements and access are defaulted to creator and owner.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	Report evidencing all data assets, where classification is sensitive, have entitlement metadata is populated.

CONTROL & PROCEDURE 8: DATA CONSUMPTION PURPOSE	
Component	**3.0 Accessibility & Usage**
Capability	**3.2 Ethical access, use and outcomes of data are managed**
Control Description	**Data Consumption Purpose** must be provided for all data sharing agreements involving sensitive data. The purpose must specify the type of data required and include country or legal entity scope for complex international organizations.
Assessment Procedure	Inspect the data catalog and classification to confirm purpose (accepted use and entitlements) is tracked for sensitive data and usage tracking is enabled and monitored.
Procedure Assumptions	• Report captures if a data sharing agreement exist, yes or no? If no, then a resolution is expected such as policy/rule around the data sharing agreement that is measured against for consumption. • Data Sharing Agreement (DSA) represents a form of policy, therefore assessment is based on assumption that policy exists and will drive implementation, whether an asset is identified as sensitive and should have a DSA, or a rule is in place for specific triggers and actions for specified data assets.
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data purpose at the point of creation and/or classification of data assets as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established. • Catalog is established. • Classification(s) for accepted use and purpose is established. • Usage tracking is enabled for data asset. • Environment with metadata scanning enabled and scheduled.
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate report using catalog metadata with purpose tracking populated and not populated: 3.1 Review report and identify data assets with no assigned purpose and classified as sensitive. 3.2 Create a new consumption use case of an existing data asset: 3.2.1 Confirm a new data sharing agreement is generated and that workflow is triggered to complete purpose tracking. 3.2.1 Verify that purpose tracking is accurate and is compliant with the data sharing agreement. 3.3 Update an existing use case for a new consumption purpose: 3.3.1 Confirm workflow automation flagging the data sharing agreement flagged for review based on changes.

Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Report and/or documentation to indicate data asset purpose tracking is populated for data assets classified as sensitive. • Report and/or documentation to indicate that additional usage/access of data assets is identified and flagged for review.

CONTROL & PROCEDURE 9: SECURITY CONTROLS	
Component	**4.0 Protection & Privacy**
Capability	**4.1 Data is secured, and controls are evidenced**
Control Description	1. Appropriate **Security Controls** must be enabled for sensitive data. 2. Security control evidence must be recorded in the data catalog for all sensitive data.
Assessment Procedure	Inspect the data catalog and classifications to confirm security policy aligned to the appropriate security controls.
Procedure Assumption	N/A
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require sensitive data at the point of creation and/or classification of data assets as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established. • Catalog is established. • Classification(s) for security controls is established. • Environment with metadata scanning enabled and scheduled.
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate report using catalog metadata classification for sensitivity controls where populated and not populated: 3.1 Review report and identify data assets classified as sensitive: 3.1.1 Confirm security control definition is applied to data asset. 3.2 Update security classification to a new sensitivity definition: 3.2.1 Confirm security control definition is applied to data asset. 3.3 Review report where security classifications are populated: 3.3.1 Verify with random sample that security description is accurate for each data asset's classification. 3.3.2 Verify with random sample that the specified security control has been applied to the data asset.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Report and/or documentation to indicate data asset classification is populated and categorized by sensitivity. • Documentation to indicate data asset security controls align to sensitivity classification.

CONTROL & PROCEDURE 10: DATA PROTECTION IMPACT ASSESSMENTS	
Component	**4.0 Protection & Privacy**
Capability	**4.2 A data privacy framework is defined and operational**
Control Description	**Data Protection Impact Assessments** (DPIAs) must be automatically triggered for all personal data according to its jurisdiction.
Assessment Procedure	Inspect data catalog and classification to confirm appropriate classification to support generation of privacy impact assessment (PIA) report.
Procedure Assumptions	N/A
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data sensitivity and privacy classification at the point of creation, and consistently maintained.
Control Dependencies	• Data assets are established • Catalog is established • Classification(s) for privacy is established • Environment with metadata scanning enabled and scheduled
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate report using catalog metadata for personal data that is populated and not populated: 3.1 Review report and identify data assets where sensitive and no privacy classification assigned for personal data: 3.1.1 Confirm workflow automation where data assets classified as sensitive where no privacy requirements are defined for personal data and sent for remediation. 3.2 Create a new data asset: 3.2.1 Confirm that data catalog has generated new entry for this personal data and identified as sensitive and private (triggering privacy requirements). 3.2.2 Observe that PIA updates to reflect new data asset. 3.3 Update an existing data asset with new storage location: 3.3.1 Confirm that PIA updates accordingly. 3.4 Create new use or sharing of an existing data asset from a new location: 3.4.1 Confirm that PIA updates accordingly.
Data Requirements	Metadata data catalog and data assets for testing specification Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Report produced ad hoc or on a regularly scheduled basis to indicate privacy impact assessment for one or more data assets.

CONTROL & PROCEDURE 11: DATA RETENTION, ARCHIVING AND PURGING	
Component	**5.0 Data Lifecycle**
Capability	**5.1 The data lifecycle is planned and managed**
Control Description	**Data Retention, Archiving, and Purging** must be managed according to a defined retention schedule.
Assessment Procedure	Inspect data asset to determine that data lifecycle and schedules are established and automated.
Procedure Assumptions	The assessment can be achieved assuming the capability is available, however, the policy will drive implementation (e.g. policy may be to never purge, and while the capability exists, policy does not implement).
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data lifecycle is defined as the point of creation and/or during updates, and consistently maintained.
Control Dependencies	• Data assets are established • Catalog is established • Data retention schedules established • Environment with metadata scanning and profiling enabled & scheduled
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate report using catalog metadata classification for data lifecycle classifications: 3.1 Review report and identify data assets where sensitive or critical and no data lifecycle is specified. 4. Create and/or update existing data asset to observe data lifecycle triggers: 4.1. Create a new data asset: 4.1.1. Confirm that a retention schedule is attached. 4.2. Update an existing data asset / schedule to trigger archival: 4.2.1. Observe that data lifecycle flags or triggers workflow for archival of data asset. 4.3. Update an existing data asset / schedule to trigger purge: 4.3.1. Observe that data lifecycle flags or triggers workflow for purge of data asset.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Report produced ad hoc or on a regularly scheduled basis to indicate data lifecycle requirements and compliance to data asset lifecycle schedules.

CONTROL & PROCEDURE 12: DATA QUALITY MEASUREMENT	
Component	**5.0 Data Lifecycle**
Capability	**5.2 Data quality is managed**
Control Description	**Data Quality Measurement** must be enabled for sensitive data with metrics distributed when available.
Assessment Procedure	Observe that data quality metrics are established per system generated data profiles and/or user defined data quality metrics.
Procedure Assumptions	N/A
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to generate data quality at the point of creation, and consistently maintained.
Control Dependencies	• Data assets are established • Catalog is established • Data quality metrics established • Environment with metadata scanning and profiling enabled & scheduled
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate report using catalog metadata for data quality metrics: 3.1. Where applicable – if data quality metrics are system generated: 3.1.1. Confirm data quality profiling is enabled for a data asset. 3.1.2. Influence a change that would result in a change in quality metrics. 3.1.3. Observe changes reflected in data quality report. 3.2. Where applicable – if data quality metrics are user defined: 3.2.1. Confirm data quality user-defined rule is created and deployed. 3.2.2. Influence a change that would result in a change in quality metrics. 3.2.3. Observe changes reflected in data quality report. 3.3. Confirm workflow is automatically generated and sent to data owner(s) where data quality issue is potentially identified. 3.4. Confirm workflow is automatically generated and sent to data owner(s) on a recurring schedule.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Report produced ad hoc or on a regularly scheduled basis to indicate data quality metrics per data profiling and/or user defined metrics for one or more data assets.

CONTROL & PROCEDURE 13: COST METRICS	
Component	**6.0 Data & Technical Architecture**
Capability	**6.1 Technical design principles are established and applied**
Control Description	**Cost Metrics** directly associated with data use, storage, and movement must be available in the catalog.
Assessment Procedure	Inspect data asset to confirm cost usage monitoring based on policy requirements and current data architecture.
Procedure Assumptions	The procedure should ensure that cost metrics are comprehensive – not limited to use storage and movement, for example, including cost of disposal.
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data cost monitoring at the point of data asset creation, and consistently maintained.
Control Dependencies	• Data assets are established • Catalog is established • Cost metrics reporting is established • Environment with metadata scanning and profiling enabled & scheduled
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate data cost report for a specified data asset. 4. Create a new data asset: 4.1 Observe cost tracking for movement, storage, and associated usage cost. 5. Update an existing data asset in a way that changes the costs associated with use, storage or movement: 5.1 Observe changes to cost usage over time per data architecture updates for movement, storage, and associated usage cost.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Data cost report generated for selected data assets and/or sets of data.

CONTROL & PROCEDURES14: DATA LINEAGE	
Component	**6.0 Data & Technical Architecture**
Capability	**6.2 Data provenance and lineage are understood**
Control Description	**Data lineage** information must be available for all sensitive data. This must at a minimum include the source from which the data was ingested or in which it was created in a cloud environment.
Assessment Procedure	Inspect traceability of data asset from source and/or changes to data asset lineage.
Procedure Assumptions	N/A
BAU Procedure Frequency	Compliance is reviewed regularly such as quarterly and/or automated to require data lineage at the point of creation and/or classification of data assets as sensitive, and consistently maintained.
Control Dependencies	• Data assets are established • Catalog is established • Data lineage is enabled • Environment with metadata scanning and profiling enabled & scheduled
Test Specification	1. Determine the data catalog is established. 2. Inspect to confirm metadata discovery (scanning) capability is enabled and set to a recurring schedule. 3. Generate data lineage report for a specified data asset: 3.1 Confirm the data lineage report includes, at a minimum, the source from which the data was ingested or in which it was created. 4. Create a new data asset classified as sensitive: 4.1 Observe that data lineage report accurately reflects creation of the data asset. 5. Update an existing data asset to a new source and/or target destination: 5.1 Observe that data lineage report accurately reflects changes to lineage.
Data Requirements	• Metadata data catalog and data assets for testing specification. • Environment populated and previously populated where applicable into the data catalog.
Evidence & Output	• Data lineage report generated for sensitive data assets.

ADDITIONAL DOCUMENTATION

This document is a constituent part of the CDMC™ framework focusing on the key controls for effective management of data risk in cloud, multi-cloud and hybrid environments. This section provides a summary of additional parts of the overall framework.

CDMC Framework

Full documentation of the 6 components, 14 capabilities and 37 sub-capabilities of the CDMC framework, along with the 14 Key Controls. This 160+ page document details the objectives of each sub-capability and presents best practice advice written from both the data practitioner and cloud service and technology provider perspectives. A set of questions, artifacts and scoring guidance for each sub-capability provide the basis for organizations to perform capability assessments.

Reference: CDMC Framework Version 1.1 – published September 2021

CDMC Information Model

An ontology that draws on and combines related open frameworks and standards to describe the information required to support cloud data management. This provides a foundation for interoperability of data catalogs and automation of controls across cloud service and technology providers.

Reference: CDMC Information Model Version 1.1 – to be published Q4 2021

Data Management Business Glossary

A standard set of over 200 data management terms, with definitions and commentary for each.

Reference: https://www.dcamportal.org/glossary/