External Supplier Control Obligations

Data Management

Version 8 May 2020

Control Area	Control Title	Control Description	Why this is important
Governance and Assurance	Roles and Responsibilities	The Supplier must define and communicate roles and responsibilities for Data Management for all Critical Data Elements processed and managed on behalf of ABSA Group Limited. These must be reviewed after any material change to the Supplier's operating model or business.	To ensure that both ABSA and the Supplier fully understand the provisions of the service provided and ABSA data is managed by the supplier appropriately.
		Key roles must include a senior executive, accountable for ABSA Data with the supplier environment.	
		The Supplier must nominate a key Supplier contact to be the liaison with the ABSA Relevant Records Owner.	
	Data Management Risk and incident Reporting	Documented controls and processes must be in place to ensure Data Management incidents are reported and managed.	To ensure that Data incidents are reporting and managed appropriately.
		Data Management Incidents and breaches should be responded to by the Supplier and reported to ABSA immediately. An incident response process for timely handling and reporting of intrusions involving ABSA's information and/or services used by ABSA should be established.	
		The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and shared and agreed with ABSA.	
Data Service Level Agreement	Data Management Service Level Agreement	A Service Level Agreement (SLA) for external data suppliers, must be in place according to the Absa Group Limited Group Procurement requirements.	To ensure that an appropriate Service Level agreement is in place for all ABSA critical data created, processed, stored, retained, integrated of Critical Data Elements or Entities as data/data elements/Entities that is vital to the success of the business area objectives and operations and if the data is compromised or not managed appropriately the business will be exposed to risks that could lead to financial losses, bankruptcy, legal issues and the loss of licence to operate as a registered Financial Service Provider.
	Metadata Management	Supplier must comply with Data Taxonomy provided by the ABSA Data Owner and ensure that controls are in place to identify, activate and manage data domains, to identify data elements and to define and manage business, operation and technical metadata as agreed in the SLA.	
	Data Integration	If the Supplier integrates data , sufficient controls must be implemented to effectively monitor the successful transfer of critical data between environments to ensure that the data remains fit for purpose, i.e. delivered without loss (integration completeness) and its original state (integration accuracy), without accidental or undesirable modification.	

Control Area	Control Title	Control Description	Why this is important
Data Management Service Level Agreement.	Data Quality	The supplier must comply with the Data Quality attributes defined and agreed in the Service Level Agreement between the ABSA Data Owner and the Supplier.	To ensure that the applicable Data Quality attributes as per the SLA is consistently applied to the ABSA Data Managed.
	Data Management is Subcontracted	If the supplier has a Sub Contractor that has access to and manages data on behalf of the supplier, the ABSA Data Owner will need to approve the sub-contractor and the supplier will need to ensure that appropriate measures are in place to manage and protect the data.	To ensure that both ABSA and the Supplier fully understand the provisions of the service provided and ABSA data is managed by the supplier appropriately
	Data Lineage	The supplier must establish and implement Data Lineage Principles and Guidelines for Critical Data managed on behalf of the ABSA Data Owner.	To ensure that Critical Data is managed in line with applicable laws, regulations, business risk, strategy and architecture.
	Data Migration	If the supplier migrates ABSA Critical data from any source (Platform, Database, Server, Cloud Storage, and Application) to a Target source, the scope of the migration must be documented and agreed by the ABSA Data Owner.	
	Data Jurisdictions	If the supplier needs to select Suitable Data Jurisdictions for Storing Data written approval will be required by the Absa Data Owner. The supplier must ensure that data is stored in the appropriate jurisdictions (e.g. countries. Not Sanction countries), in line with applicable laws, regulations, business risk, strategy and architecture. Any supplier working with data, moving data across borders and utilizing public cloud technologies should engage with relevant ABSA Data Owner receiving the service to ensure the appropriate compliance, privacy, risk, engineering, architecture and security teams are engaged to ensure that Data is managed appropriately that the correct assessments are undertaken, and the appropriate sign-offs or risk acceptances are achieved.	

Control Area	Control Title	Control Description	Why this is important
Data Management Service Level Agreement.	Data Destruction	The Supplier must ensure ABSA's Data is not destroyed without ABSA's prior written consent. Service providers must confirm in writing the details of data that is destroyed when approval is granted. Evidence of the authorisation and destruction of data and records must be maintained, using controls such as: • Physical certificates of destruction; and / or • Electronic records audit trail / reports of data and records deleted and / or • Destruction reports for storage media.(i.e. Hard Disks, cd's, microfiche);	To ensure that ABSA data is not destroyed without prior consent when instructed to destruct data and audit trail is provided by the supplier.
	Protection	The Supplier must ensure ABSA Data is protected using physical, environmental and logical controls to prevent unauthorised loss, modification or damage throughout their retention and protected according to their confidentiality classification against the ABSA Information Classification Scheme defined in the Information Security Supplier Control Requirements Schedule. Information should be classified and handled as per Appendix A – Table A and B.	To ensure that ABSA data is protected appropriately.
	Access	The Supplier must have physical / logical controls to ensure access to ABSA Data is restricted to only those Supplier Personnel who are appropriately authorised and need access to perform their duties.	
	New Joiner education and awareness	The Supplier must ensure that all new Supplier Personnel, within a reasonable time period, complete training which ensures they understand their Data Management roles and responsibilities.	To ensure that Supplier Personnel understand their Data Roles and Responsibilities.
	On-going education and awareness	The Supplier must ensure that once a year all Supplier Personnel complete mandatory training ensuring that they are aware of their Data Management roles and responsibilities.	

Definitions	
Critical Data Element/Entities	**Critical Data Elements/ Entities** are defined as data/data elements/Entities that is vital to the success of the **business area** objectives and operations and if the data is compromised or not managed appropriately the business will be exposed to risks that could lead to financial losses, bankruptcy, legal issues and the loss of license to operate as a registered Financial Service Provider.
Conceptual Data Model	A **Conceptual Data Model** is a first-pass of the data modelling process and can be seen as a summary or abstract-level model.
Data	Data is a set of values of qualitative or quantitative variables at its most raw and unorganised form. In general, data may exist inside electronic stores (like systems) or inside of physical stores (a filing cabinet). It may be structured (like SWIFT messages) or unstructured (free text or images). Raw data, is typically difficult to interpret, since it lacks context and meaning,
Data Domain	A **Domain** is a grouping of related concepts or subjects together, for convenience, design or implementation purposes. Architecturally, it often helps to group related concepts together since they may be dealt with by the same **business area** or in the same system. **Domains help us to communicate, reason, understand and infer, but more importantly to organize and build.**
Data Lineage	**Data Lineage** is the life cycle of a piece of data, beginning with that data being created, how that data moves around the organization to reach its destinations, how it is transformed or manipulated in doing so and ultimately to where it is destroyed. These activities may take place whether by business process or by system activity. Data lineage exists so that we can understand where the data we use comes from and can make rapid decisions or changes over fast-moving data sets reliably. Data Owners should ensure that Data Lineage is mapped for all **Critical Data Elements/Entities.**
Data Integration	The disciplines of moving data between systems and encompass Extract-transform-load type techniques or modern integration practices like real-time streaming and APIs. Sound data integration is an essential part of Data Lineage.
Data Transformation	The process of converting data from one format or representation to another.
Data Consumer	A system or person that receives data for a specific use, which, in an ETL context may also be referred to as a Target System. It should be noted that ETL mechanisms are somewhat outdated and it is architecturally preferred to use other technologies such as APIs or streaming (which are real-time rather than batch oriented) where these are appropriate and feasible.
Destruction	**Destruction** of data / **record** no longer required / expired aligned to the **retention period** set out in the **Country Retention Schedules**.

Definitions	
Golden Source	A **Golden Data Source** is the system where data enters the organisation by being created, amended, generated through programmatic mechanisms or externally sourced.
Glossary	A **Glossary** is a collection of definitions, typically collected for ease of reference purposes and typically organised alphabetically. However, in enterprise applications they have limited benefit since the meaning of a term typically varies depending on the context in which it is used (e.g. a "shoe" is very different if you are a "shoemaker" or a "horse rider").
Information	**Information** is a collection of data that is presented in a context which gives it meaning, often making it more easily interpreted by machines or by human beings
Information Asset	This is **information** relevant to the operation of the bank. The asset can be in the form of a:
Logical Data Model	Describes the data of the Domain in as much detail as possible, but excludes details around the physical implementation and is technology agnostic. Logical models contain entities in a more fleshed out form.
Ontology	An **Ontology** is a set of concepts (things) and the relationships between them that describes an area of subject matter. It typically contains formal naming and definition of these concepts, as well as the relationships between them and their categorization
Personal Data	Any data (including special personal data) relating to a living, natural person and where applicable, an existing juristic person, either in electronic or hard copy format, from which an individual or juristic person can be identified. This includes but is not limited to race, gender, sex, pregnancy, marital status, national, social or ethnic origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, birth of person, education background and history, financial history, employment history, criminal history, email address, physical address, location **information**, mobile numbers, online identifiers (e.g. cookies or IP addresses), biometric **information**, an identifying number or symbol, the personal opinions, views or preferences of the person, the opinions of another individual about the person, the name of the person if it appears with other personal data relating to the person or if the disclosure of the name itself would reveal **information** about the person, correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence.
Physical Data Model	Physical Model is a representation of how a data model will be implemented using a specific technology, or the actual implementation represented through software artefacts like code (which is preferable in a DevOps context).
Physical Records	The original paper copy, printout, or any **record** that can be read without the use of a computer or other electronic device.
Qualitative data	**Qualitative Data** are measures of 'types' and may be represented by a name, symbol, or a number code.
Definitions	

Quantitative data	**Quantitative Data** are measures of values or counts and are expressed as numbers. **Quantitative data** are data about numeric variables (e.g. how many; how much; or how often).
Record	Records are **information** about facts, events, transactions or opinions, which is created, received, or maintained by or on behalf of Absa Group Limited (including those generated, processed or stored by third parties or customers) in carrying out its activities. In general, these are the **information** which are created and stored as a result of Absa's business dealings and activities.
Relevant Record	Records which must be sourced, created, retained, and managed in a manner that are compliant with specific legal, regulatory, or business requirements (e.g. operational business purposes, demonstrate policy compliance). Records that are considered relevant are identified in Country Retention Schedule(s) which also prescribes the period for which these records should be retained.
Retention Period	The period a relevant data and record/s is required to be retained for Legal and Regulatory purposes.
Source System	A **Source System** is any system or file that captures or holds data of interest. Data is extracted from a source system to send to target systems for further use. In integration terminology this may also be called a **Data Provider** or **Interface Provider**.
Taxonomy	A **Taxonomy** is a classification or categorisation of concepts (or things). It contains formal naming and definition of these, but is generally limited to a hierarchy or grouping rather than describing all relationships between them. Taxonomies help us to organise and locate things.
Technical Lineage	**Technical Lineage** is a subset of the broader **Business Lineage** and pertains only to the integrations and data movements between the systems but has a higher level of detail (akin to the difference between a conceptual and a logical data model). It is preferred that technical lineage be accomplished through self-documenting code and frameworks (such as spline), and not re-written in a separate artifact.
ABSA Data Owner	Defining clear operational data ownership and accountability for critical data with Data Owner(s) appointed for each business domain. The Data owner must be a senior, permanent staff member who can effect change within the business and set priority of work undertaken in line with the business strategy. Where appropriate, the Data Owner may appoint Data Stewards as their delegates who will have day-to-day operational responsibility over the data. The Data Owner's accountability extends across the Data, Information and Records management life cycle as well, defining what data is critical, ensuring that data quality is well defined and implemented in their area. In addition, they or their delegates serve as the key point of contact for operational issues with their data which are encountered in other areas.

APPENDIX A

Table A: ABSA Information Classification schema

Classification Level	Unrestricted (Level 1)	Internal Only (Level 2)	Confidential (Level 3)	Secret (Level 4)
Definition	The 'Unrestricted' classification applies to information which is already in the public domain, or information for which unauthorised public disclosure would have no significant negative impact or consequences for Absa, its customers or its business partners.	The 'Internal Only' classification applies to information related to Absa internal operations or communications which is of general relevance to all employees and appropriate for distribution throughout the organisation. Such information would not typically have any significant negative impact if disclosed to unauthorised personnel but could provide knowledge of Absa' internal operations which may not be appropriate for non-Employees members.	The 'Confidential' classification applies to information which is proprietary to the organisation or related to a sensitive or specific business process and is not appropriate or necessary for viewing by all employees. Such information may have a negative impact if it were disclosed to unauthorised personnel both internally and externally. Personal and financial customer information is classified as 'Confidential' by default (although some less sensitive customer information or individual customer records may be classed as 'confidential' dependent on the requirements of the Information Owner or risk assessment - see the Absa Data Privacy Policy for further details).	The 'Secret' classification applies to information for which unauthorised disclosure (even within the organisation) may cause serious financial or reputational damage, significant loss of competitive advantage, or lead to regulatory sanction or legal action.
Examples	• Absa marketing materials. • Job advertisements. • Public announcements. • Content of Absa publicly accessible web sites. • Publications	• Organisation policies. • Internal announcements. • Employee names and internal phone directories. • Job functions. • Employee handbook. • Newsletters. • Internal Communications.	• New product plans. • Client contracts. • Organisation charts. • Employee contact lists. • Audit reports. • Legal contracts. • P&L reporting. • Sensitive Customer / Client information including financial and personal. • Strategies • Vulnerability Assessments. Performance Appraisals	• Profit forecasts or annual financial results (prior to public release). • Information on potential mergers or acquisitions. • Strategic planning information. • Performance and compensation information specific to individuals. • Sensitive customer/client information including financial and personal data. • Exco Minutes. • Crypto keys.
Hard Copy Information and Removable Media (Physical)				
Description: *Includes all printed documents and data storage media used to store Absa' Information such as CDs, backup tapes and removable devices.*				

Table B: ABSA Information Classification scheme handling requirements throughout the information asset lifecycle

Classification Level	Unrestricted (Level 1)	Internal Only (Level 2)	Confidential (Level 3)	Secret (Level 4)
Labelling	• Not required.	• Not Required.	• All hard copy information containing 'Confidential' information must carry a prominently displayed classification label on the cover page, and a visible classification label on every page of the document (e.g. in the header or footer of the document.) • All removable storage media/devices containing 'Confidential' information must be labelled and marked accordingly, e.g. CDs must be marked with a permanent marker etc. All removable media must be labelled with the highest classification of any information residing on it.	• All hard copy information containing 'Secret' information must carry a prominently displayed classification label on the cover page, and a visible classification label on every page of the document (e.g. in the header or footer of the document.) • Wherever possible, removable media is not to be used to store or distribute 'Secret' information. If it must be used all removable storage media/devices containing 'Secret' information must be labelled and marked accordingly (as per 'Confidential' information) and additional controls must be in place (see handling, storage and distribution requirements).
Handling and Storage	• No restrictions.	• Secure workplace practices such as a clear desk policy, must be followed. Information must be stored out of sight when not in use and only provided to other Absa Employees unless authorised by the Information Owner.	• Physical documents and removable media must be stored securely, in accordance with the "need to know" principle, when not in use for long periods, for example, overnight. • Printed documentation must be retrieved from printer trays, fax machines or photocopiers. • Only store 'Confidential' information on removable media for as long as it is explicitly required.	• Physical documents and removable media must be stored securely, in accordance with the "need to know" principle, when not in use. • Printed documentation must be retrieved immediately from printer trays or photocopiers. • 'Secret' information stored on removable media must be protected with appropriate additional technical controls (e.g. using Absa approved encryption mechanisms).
Retention	• No specific requirements (although Employees are encouraged to dispose of this information as soon as practical).	• No specific requirements (although Employees are encouraged to dispose of this information as soon as practical, and at least annually, except if directed otherwise by the Business Unit Retention Schedule or Information Owner).	• Retain in accordance with the documented region/Business Unit specific retention schedules.	• Retain in accordance with the documented region/Business Unit specific retention schedules. • 'Secret' information is more likely to be subject to legal or regulatory requirements so retention requirements and processes must be reviewed regularly (at least annually) to ensure they are current.

Classification Level	Unrestricted (Level 1)	Internal Only (Level 2)	Confidential (Level 3)	Secret (Level 4)
Distribution	• No restrictions.	• No specific restrictions, although information should be review for appropriateness before distributing externally (if in doubt check with the Information Owner). • Must obtain approval from the Information Owner.	• No restrictions for internal mail. • For external mail (e.g. being sent by courier or local postal service), do not mark the classification on the envelope. • For fax, ensure the address is confirmed, accurately entered and confirm immediate receipt. Each page of the document must be clearly numbered, in a format that includes the total number of pages.	• Use care when sending 'Secret' documents internally or externally. Only send to authorised named individuals and address the information accordingly. Obtain approval from the Information Owner before sending documents and follow any additional distribution controls they specify. • For internal and external mail, mark the classification on an inner envelope. This inner envelope must then be placed in an unmarked outer envelope. • Use recorded delivery for 'Secret' Information delivered by external mail. • 'Secret' information must not be sent via fax. • Maintain a record of data storage media containing 'Secret' information which is sent outside of the organisation (e.g. to authorised Third Parties)
Disposal	• No restrictions.	• Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder. • Delete information on removable media when no longer required.	• Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder. • Magnetic media (e.g. disks and tapes) that are no longer required must have the magnetic surface removed and cut into small pieces. • Optical media (e.g. CDs) must be scored with an abrasive material and, where practical, broken into pieces. • If re-usable media. Then all 'Confidential' data must be deleted /overwritten when no longer required and before re-use. • 'Confidential' data must be securely disposed of in accordance with supporting data disposal procedures	• Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder. • Magnetic media (e.g. disks and tapes) must have the magnetic surface removed and cut into small pieces • Optical media (e.g. CDs) must be scored with an abrasive material and, where practical, broken into pieces • If re-usable media. Then data must be securely overwritten when no longer required using an Absa approved secure deletion solution. • 'Secret' data must be securely disposed of in accordance with documented data disposal procedures, including recording the successful deletion of the information.