INTEGRATION HUB
REQUIREMENTS LIST

TABLE OF CONTENTS

1 Business Requirements

Use the response column to indicate what is applicable to the proposed solution:

- F = If the solution already has this feature Out of the box.
- M = If the solution requires minor customisation/configuration to cater for this requirement,
- D = If the solution requires major development to cater for this requirement
- TP = If the solution requires integration with another tool to cater for this requirement,
- N/A = If this requirement cannot be catered for.

Use the comment column to indicate how this requirement will be met by your proposed solution.

1.1 Functional requirements

REQ#	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
FRQ1	**Data Ingestion** The hub must support the ingestion of data from a diverse set of sources, including: • databases, • cloud services, and • streaming platforms.		
FRQ2	**Data Transformation** The hub must enable transformation of source data to meet the target system's requirements, involving processes like normalization, deduplication, and enrichment.		
FRQ3	**Data Storage** The hub must serve as a repository - able to store data temporarily or permanently.		
FRQ4	**Data Distribution** The hub must ensure that data is distributed to various systems, such as analytics platforms, data warehouses, or operational databases.		
FRQ5	**Discoverability**		

REQ#	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
	The hub must enable the advanced search capability across various data sources, including databases, data warehouse, cloud services, and analytics platforms.		
FRQ6	**Data Lineage** The hub must provide data traceability upon its lifecycle across datasets.		
FRQ7	**Data Ownership** The hub must enable the allocation of data entity ownership		
FRQ8	**Application integration** The hub must enable application integration through APIs including JSON, SOAP and REST services.		

1.2 Information Requirements

REQ#	Report Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
IRQ1	**Reports** The hub must have the functionality generate real time interactive reports and dashboards.		
IRQ2	**Notifications** The hub must have the functionality send notifications on system/user triggered events.		
IRQ3	**Analytics** The hubs must have advanced analytics and offer data insights.		

1.3 Non-Functional Requirements

Operational

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR1	Accessibility	The hub should be accessible using either Desktop and Mobile devices connecting via network cable, WIFI and/or 3G/4G/5G		
NFR2	Response time ranges	Front-end / host / back end: max 15 seconds		

1.4 Security and Privacy

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR3	Identification and authentication	Users must be assigned unique identities within the system, which clearly identifies who they are. The system must only be accessed by legitimate and authorised users including users from external entities. The system must utilise username and password to authenticate users and support. The system must be POPI compliant		
NFR4	Single sign on	System user identities must automatically be linked to Active Directory to allow single sign on to the system.		
NFR5	User Group Definitions	Role-based access control shall be used to define content and functionality applicable to users. This must be in line with the user's job function or role. Segregation of duties rules must be enforced on a system level.		
NFR6	Database Security	The database must be secured by allowing only authenticated and authorised users access to data. The database must be secured by only allowing the Web applications to access data through a service account, which forms part of Windows authentication.		

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR7	Confidentiality	Data must only be accessed by authenticated and authorised users in line with their job function or role. Data and Passwords must never be viewable at the point of entry or at any other time.		
NFR8	Data Loss (Disclosure of information about individuals or entities)	Security policies must be enabled to prevent leakage/disclosure of sensitive information to unauthorised users. Users must be trained on the functionality of the system to understand their responsibilities to safeguard sensitive information.		
NFR9	Data Encryption	All data flowing within internal and external the system must be encrypted with the latest industry standard encryption technology. All data utilised within the system must be encrypted when in storage, or in transit.		
NFR10	Data Integrity (Data Corruption)	All the information flowing within and across the system should be the same and not be altered throughout its lifecycle. The information must not be compromised during changes and must still be intact after the changes or updates.		

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
		Only authorised users must be able to edit or make changes to data.		
NFR11	Implementation and development lifecycle	Development of the system must comply with Open Web Application Security Project guidelines and ISO 27001 standard.		
NFR12	Access Reports	Reports on user access and activities must be available to monitor policy violations.		

1.5 Audit Trail

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR13	Audit trail	Enable transparent audit trail in the system, audit trails must be created for all user actions that are performed. The following information will be recorded in the audit log: • Username • Date and time of action • Field name • Before value • After value • Effective date • Source (Direct/Web/Mobile App) The audit logs are stored in a separate database		

1.6 Reliability

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR14	Availability (Percentage of time available)	100%		
NFR15	Hours of Use	• Monday to Friday: 00h00 – 23h59 • Saturday: 00h00 – 23h59		

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
		• Sunday and public holiday: 00h00 – 23h59		
NFR16	Maintenance Hours	• Sunday: 10h00 –23h59		
NFR17	Mean Time to Repair (MTTR)	• Critical: 1 hour • High: 1 hour • Medium: 1 hour • Low: 1 hour		
NFR18	Mean time to failure (MTTF)	The system timeout due to user inactivity shall be after 5min (with a warning). Upon timeout, the system must auto save and allow the user to continue from last action.		

1.7 Recoverability

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR19	Audit Trail Failure	If the audit trail function fails before the user saves updates to the transaction, the system shall be able to recover all changes made in up to one minute prior to the failure.		
NFR20	Update failure	When an update failure is detected, all updates performed during the failed session shall be rolled back to restore the data to pre-session condition.		

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR21	Roll-back	All data recovered in a roll-back condition shall be recorded for use in forward recovery under user control.		
NFR22	Safe mode	When operating after a failure the user must be informed that the application is operating in a “safe mode” and all data is available for review without update.		
NFR23	Module/Function Failure	The system shall prevent access to failed module/s while providing access to all currently operational modules.		
NFR24	Hardware failure	All hardware components of the assembly operation shall be replicated, such that failure of any one hardware component shall not render the assembly operation unavailable to end-users. It is acceptable for system performance to be poorer than normal for up to 3 business days following the failure and replacement of a piece of hardware.		

1.8 Architectural Qualities

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR25	Information retention requirements	All stored data must be backed up and archived to be available within 24 hours.		

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR26	Scalability	Ability to handle increasing volumes of data and adapt to evolving data integration needs.		
NFR27	Agility	The hub must enable real-time data availability		

1.9 Development Qualities

REF	Item	Description	Response F/M/D/ TP/NA	Detail on how your solution will meet the requirement
NFR28	Interoperability	The hub must enable hybrid seamless integration with a wide range of systems and technologies.		
NFR29	Flexibility	The hub must support various data formats and integration patterns.		