IBRS | ANALYSIS INSIGHT JUDGEMENT

Data Maturity Model

Maturity/ Qualifier	1 Initial	2 Managed	3 Defined	4 Quantitatively Managed	5 Optimised
Systems & Resources	Business case for data tools and data team is in development or is delayed/postponed.	Business case approved, procurement and recruitment in progress.	Data systems being released into production. Decommissioning legacy systems in planning.	Data systems and relevant processes have been embedded into BAU. Decommissioning of legacy systems underway.	Data systems and resources have a roadmap with approved funding. Legacy systems have been decommissioned.
Governance & Compliance	No formal data custodian identified. Few controls over data release, change, storage or usage. No record of what data is used for what reporting. No records management framework.	Most data requests are formalised. Some record of who has access to what data. Records management framework in draft, some elements in use.	Consistent data naming conventions adopted for in-house application development. Records management framework released and being rolled out.	Data governance practices and processes approved and enforced. All data released under goes approval and validation. Register of data released.	Data working parties established across the business.
Master Data	Multiple single sources of financial, customer and operational business data exists. No EM repository in place.	Master data and sources have been identified and system owners identified. Master data schema under development.	Central EM repository in place. Master data and schema has been documented no change control in place.	Master data and schema has been documented and approved. Change control in place for all existing systems.	Master data impact analysis is part of procurement process for new systems.
Data Security	Data classification, sensitivity and access policies in draft or not existent. Poor encryption. Data not encrypted at rest, in transit or in processing.	Data classification, sensitivity and access policies approved and released. No system enforcement – reactive processes. Some data encryption.	Data Access is defined by role/function and not by person. Change to access formalised. Some SIEMs, DLP processes in place.	Data access change requests formally managed. Proactive data access management in place. Automated access control to sensitive data. Data encrypted at rest, in transit and at processing.	Data Security roadmap with approved funding. Data security embedded into staff onboarding process.
Data Quality	Majority of data sources have not been cleaned. Data on input not consistent. No uniform formatting standards. Little data validation.	Master data records have been cleansed for active records. Data validation on input ad hoc and not enforced. Formatting standards have been documented but not enforced.	Data validation on input widely implemented. Data formatting standards widely adopted. Data uplift on client records.	Data standards applied to historical records. Data standards applied to paper inputs.	Data standards applied to Procurement process for ICT.
Data Visualisation & BI	Multiple CSV reports used across the business. No central analytics or visualisation capability. Inconsistent data interpretations across the business.	Rationalisation of CSV reports in progress. Analytics or visualisation capability in procurement/ setup. Multiple reports from different business units interoperates the same data in different ways.	Central analytics or visualisation capability in use for core reports. Inconsistent data interpretations across the business. Data team in place.	Predictive analytics in use to help optimises decision making to ensure best actions are taken to maximise business value.	Analytical insight optimises business processes and is automated where possible.