

Data Integrity Maturity Model (13/06/16)

		1 Unacceptable	2 Improvement required	3 Acceptable	4 Good	5 Exemplar	Contacts
Governance and Accountability	Governance	<ul style="list-style-type: none"> We have no Custodians or they are at the wrong management level. We do not know who is responsible for our dmml. We do not have the Data Management capability in staff objectives or work plans 	<ul style="list-style-type: none"> We have Custodians in place. Our Executive, National, and Local custodians are at the correct management level. We brief our Custodians on their accountability & responsibility. We do not set specific objectives to improve our data management or consider it on work plans 	<ul style="list-style-type: none"> Our Custodians actively take responsibility and accountability for dmml. We have networks across the business to manage and improve dmml. IPP objectives and/or work plans specifically include management and improvement of DMMI and processes. 	<ul style="list-style-type: none"> Our networks operate effectively and improve dmml. We look to improve our data management processes by looking at our capability, development, and resilience We base our work plans and/or objectives on dmml custodianship performance. 	<ul style="list-style-type: none"> Our networks drive dmml understanding and improvement Peer review ensures consistent objectives and drives performance improvement. Objectives are stretching and there are development actions to improve dmml. We assess and plan for future data management challenges 	
	Ownership	<ul style="list-style-type: none"> We do not know what dmml, data products, or IT systems we are accountable for. We do not understand the duplication of the data we hold. Our data is not findable Where we acquire 3rd party data we do not ensure we have a licence. We do not consider other potential corporate users of our data. 	<ul style="list-style-type: none"> We know some of our dmml, data products and IT systems (including grey IT). Our records reflect this. We have some understanding of the duplication of the data we hold. Some of our data is findable. Where we acquire 3rd party data we ensure we have a licence which may include data sharing. We occasionally consider other corporate users of the data we acquire. 	<ul style="list-style-type: none"> We know and record all of our dmml, data products, services and IT systems (including grey IT). We ensure where our data has been duplicated. Where possible we limit duplication. We look to adopt or adapt existing corporate IT applications before developing new in isolation. We ensure most of our data is findable. Where we acquire 3rd party data we build the presumption to share into contracts where possible. We ensure acquired data considers other corporate users. 	<ul style="list-style-type: none"> We regularly review and decommission our dmml, data products, and IT systems (including grey IT). We take a strategic view and use our dmml knowledge to continually improve to reflect business objectives/make decisions. We prioritise our critical dmml. We review our models against the Model Management Framework and understand where the management gaps lie We avoid data duplication where possible and store it in one location. We create metadata proactively and we have a programme to review and update. We ensure our data acquisition fulfils corporate needs. 	<ul style="list-style-type: none"> We review our models against the Model Management Framework and address any gaps in our model management practice. Our data is held once and is stored in a location where it can be obtained easily. We always create metadata for all data and our programme to review and update ensures it is all up to date. We consult widely with the business on their requirements and use of data we acquire. 	
	Security	<ul style="list-style-type: none"> Security training is rarely undertaken. We do not assess our data to check if it contains personal, confidential or sensitive data Risk Assessments are on an ad-hoc basis. 	<ul style="list-style-type: none"> Annual Security training in place but not always completed EC, NC have completed required Custodian security training. Review of data security controls sporadically undertaken. Limited impact assessment. 	<ul style="list-style-type: none"> All staff complete annual security training Data security controls are reviewed and impact assessments undertaken regularly Routine reviews of user access to priority IT systems take place 	<ul style="list-style-type: none"> The operational risks of handling and storing data are clearly understood and managed routinely 	<ul style="list-style-type: none"> Security of dmml is a high priority and viewed as a business enabler. Regular Full Business Impact Assessment is undertaken and the results guide our custodianship. 	
Line of Sight	Sharing	<ul style="list-style-type: none"> We are not aware of whom or where we share our dmml. We do not presume to share any data. We do not take steps to reduce the number of ad hoc information requests we receive. No data is risk assessed prior to sharing. We do not have an understanding of who our customers are and we do not engage with them. We develop our own solutions to share data. We do not have a plan for publishing and updating published data. None of our data is Open data. 	<ul style="list-style-type: none"> We know with whom and where we share some of our dmml. We only presume to share some data from the point of creation. We take limited steps to reduce the number of ad hoc information requests we receive. Some data is risk assessed prior to sharing. We have a partial understanding of who our customers are and do some engagement to assess their dmml needs. We mainly use the corporate data sharing platform. We publish and update data on an ad hoc basis. Some of our data is available as 1 star Open data. 	<ul style="list-style-type: none"> We know with whom and where we share our dmml. We presume to share all data we can from the point of creation. All data is risk assessed (ODRA) prior to sharing. We understand who our customers are and engage with them to assess their dmml needs. We use the corporate data sharing platform. We publish and update our data according to our agreed plan. Our data is available as 2 star Open data or higher. 	<ul style="list-style-type: none"> We regularly review our information requests and responses and to identify ways to share our data more effectively. We proactively risk assess data prior to sharing. We have a good understanding of who our customers are, we engage with them to understand their needs, plan accordingly and act on feedback. Where the corporate sharing platform does not meet our needs we look for a corporate capability rather than create our own solution. We consistently provide timely and consistent data for publishing in accordance with our plan. Our data is available as Open data and where appropriate the format is adapted for our customers. 	<ul style="list-style-type: none"> We have processes in place to ensure that our information requests are routinely monitored and a prioritised action plan is in place. We have a thorough understanding of who our customers are and we use particular methods to understand particular customer needs. We ensure that the data sharing platform meets our needs and we always use it. We share all appropriate data as Open Data using the best format for our customers We actively seek customer feedback, and review business need to improve what and how we share our data. 	
	Interdependencies	<ul style="list-style-type: none"> We do not understand what corporate objectives our data supports. We do not document how we create or use our data. We do not understand the risks to the business, including the potential for misuse or poor decisions or where we are over reliant on a sole supplier of data. 	<ul style="list-style-type: none"> We have a partial understanding of the corporate objectives our data supports. We document how we create and use some of our data. We are aware of data flow mapping and know what to map. We know where we obtain the data we use We know who uses our data 	<ul style="list-style-type: none"> We have a good understanding of how our data supports corporate objectives. We document how we create and use our data. We have data flow maps for our data and keep them up to date. 	<ul style="list-style-type: none"> We have a comprehensive understanding of how our data supports corporate objectives. The business is aware of how we've created our data and how our data is used. We have mapped most of our data and keep the maps up to date. 	<ul style="list-style-type: none"> We have comprehensively mapped our data and have resources assigned and a plan for maintenance. 	
Data Standards and Quality Monitoring	Data Standards	<ul style="list-style-type: none"> We don't review our dmml to look for common standards. Our dmml is not consistent, integrated or interoperable 	<ul style="list-style-type: none"> We have identified what standards we have in our business area but they are stored locally and not in a central place. 	<ul style="list-style-type: none"> We record our identified standards in the agreed place. Any new standards are taken from the repository and not redefined locally. We implement standards at DMMI and system creation. Standards are maintained and updated in line with business requirements 	<ul style="list-style-type: none"> Interoperability, consistency and integration with the rest of our DMMI achieved and reviewed regularly. Appropriate local standards are aligned to our shared standards in the agreed place. Standards we don't have but need have been identified. New standards are specified and published in the agreed place We publish our standards externally. Interoperability, consistency and integrated data are key to our DMMI strategy. 	<ul style="list-style-type: none"> We lead on standards specification and harmonisation for the wider scientific and environmental data communities. 	

		1 Unacceptable	2 Improvement required	3 Acceptable	4 Good	5 Exemplar	Contacts
	Data Quality and Confidence	<ul style="list-style-type: none"> We do not consider data quality when creating data We do not measure or report on the quality of our data or plan to take actions to improve. We do not consider the confidence that we have in our data and information. Key staff do not have the right skills to ensure data is fit for purpose or understand or recognise the impacts of poor quality data 	<ul style="list-style-type: none"> We have reactive processes in place after data creation to control data input There is some data quality monitoring and reporting but it is largely ad-hoc, reactive or audit based and leads to reactive data cleansing, not focusing on root causes. Key staff are trained to the correct level to reactively manage data quality and understand the importance of quality data to their own work We can define the confidence we have in our data and information qualitatively. 	<ul style="list-style-type: none"> We have proactive measures in place at system/ data creation to control/ monitor quality and identify areas to improve. We carry out proactive data quality monitoring guided by the purpose of our data, share our data quality results and confidence levels with our stakeholders and focus on proactive actions to improve our priority datasets. Key staff are trained to the correct level to proactively ensure data is fit for purpose, know what acceptable quality is, understand the confidence in our data and know the impact on other business areas. We can define the confidence we have in our data and information quantitatively and we help others to understand it. 	<ul style="list-style-type: none"> Our data creation/acquisition programmes define the quality and confidence needed for our purposes and actively manage the use and improvement of the data we acquire that is not fit for purpose We have ongoing data quality monitoring, reporting and improvements programmes for our priority datasets making best use of our tools We have programmes identifying areas where we have poor confidence and we are following actions to improve. Data quality is recognised and supported with skilled staff who have time to ensure data is fit for purpose, and we have evidence based confidence in our data 	<ul style="list-style-type: none"> Monitoring data quality is an integral part of our dataset and systems design, evidence based risks and opportunities from data quality form a key part of our data management and decision making and all data quality issues are dealt with at source We build data quality and confidence best practice into new systems, datasets and reports. Defining, improving and communicating confidence in our data and information is business as usual. Share data quality and confidence best practice within the business area and with others. 	