	Maturity level	0	1	2	3	4	5
	Domain	Initial	Performed	Defined	Managed	Quantitively managed	Optimized
1	Value Creation	- The Internet of Things integration is characterized as ad hoc, and occasionally even chaotic. - Few processes are defined, and success depends on individual effort.	- Value is realized on a small scale and does not support strategic objectives and activities. - The basis for sharing and exploiting the value of data is hampered by a lack of strategic vision and coordination. - There is no "wrong" data collected as the standard for what is "right" is not defined on an enterprise level.	Value is loosely defined at the enterprise level and achieved inconsistently by some local / departmental use of data.	Value is clearly defined by the enterprise and business units recognize their roles in value creation.	- Value is clearly defined by the enterprise and business units support enterprise value creation through consistent use of enterprise data definitions. - Enterprise performance scorecards are in place.	- Common enterprise-wide data and definitions are consistently used. - The transformation of data to information to knowledge to business performance is embraced as a competitive advantage.
2	Data Quality	- Data can be unstructured, as long as it is stored in some format - There is no organization-wide structure defined in how to store data	- Data quality issues are addressed reactively by business units. - Remediation addresses only immediate and known issues. - Enterprise business definitions and standards for data are not consistently understood or documented.	- There are localized efforts to approach data quality in a more rigorous manner. - Procedures to ensure data quality to a business core unit are being established. - Processes to develop standards across the enterprise may be started.	- Data quality is recognized as an enterprise issue and is being addressed though planned and coordinated efforts. - There are enterprise standards for managing data quality supported by common definitions and processes addressing root causes and ensuring that remediation addresses immediate concerns and prohibits future contamination.	- Core information is consistently managed, maintained, accessible to all appropriate parties. - Metrics for data quality exist and are actively monitored. - Information is consistently defined across the enterprise, resulting in improved effectiveness and efficiency. - Technical metadata providing traceability and transparency is mature.	- Data quality is understood and leveraged as a competitive advantage. - The use of high volumes of high quality data allows the enterprise to improve product development, pricing, and distribution, according to well defined customer segments, purchase and use patterns, as well as profitability forecasting models that consider fully allocated and variable cost approaches.
3	Security & Privacy	Security standards are neither defined nor documented, and there is little awareness or acknowledgement that such actions are needed.	Some security standards exist, though they are not comprehensive, not updated on a routinely, not easily accessible and not broadly ratified.	The required security standards exist and are comprehensive, however the resources to keep the standards routinely up-to date are lacking.	Security standards are documented, published, and easily accessible, though compliance to standards is not universally monitored, and risks associated with non-compliance are not comprehensively understood.	Security standards are documented, published, and easily accessible. Ongoing compliance with standards is measured, though measurement and analysis processes are not automated and suffer from challenges to data integrity	- Security standards are documented, published, and easily accessible. - Ongoing compliance with standards is measured via automated processes that are integrated with problem resolution and automated deployment systems. - Penalties exist for non- compliance within enterprise standards and remediation is executed in a predictable manner.
4	Data Classification / Metadata	Data is captured but simply stored for future usage without clear goals	- Data is not defined consistently within or across the organization. - There may be a low-level awareness of the concept of IoT data.	Some data is consistently defined within business units but there is no assessment of consistent or coherent use across business units or in managing or conforming data in new applications or with acquired businesses.	- Enterprise data definitions exist. - There may be inconsistencies in the quality of business, technical or operational definitions but content is granular enough to be meaningful. - Data valuation tends to be classified generically, e.g. high, medium, and low, rather discretely quantified.	- Robust data classifications and definitions exist and are uniformly understood and used across the enterprise. - Classification schemes focuses on business value of data and can be used to quantify the expected impact of an incident. - Metadata is consistently used for reporting, new product or application development.	- Classification schema focuses on business value of data and can be used to quantify the expected impact of an incident. - Output of classification is also integrated into controls framework, incidents response, reporting, and customer notification processes. - Metadata is understood as a key performance indicator for all knowledge workers.
5	Information Lifecycle Management	Lifecycle management is not taken into consideration while puchasing and/or implementing IoT solutions.	- Organization has some recognition of data lifecycle management. - Organization has identified processes where data is created or acquired.	- Organization has routine approach to data creation and acquisition. - Data management processes are mature but may not address key data quality, data enrichment, or data aggregation / consolidation opportunities.	- Organization has defined processes for data creation and acquisition as well as migration, reuse, and transformation. - Critical data quality considerations are known.	- Organization is managing data across the known lifecycle including creation, acquisition, migration, reuse, transformation, aggregation, consolidation, and destruction. - Data quality issues are routinely identified and remediated.	- Organization understands data as a corporate asset and seeks opportunities to enhance the quality and use of data for business purposes. - Impact analysis is a routine consideration in data creation or other development efforts within the information ecosystem. - Data quality issues are anticipated and addressed proactively.
6	Policy & Compliance	A policy is known, maybe even written down, but not applied all the time.	Policies are defined and enforced at the departmental level.	There are some common criteria and policies around information classification.	Some formalization of enterprise level (Board Approved) policies is in place but enforcement may be inconsistent or lacking.	- Formal enterprise policies are adopted, implemented, and driven down through the organization. - Policy compliance audits and feedback loops are in place.	- Policies are proactively designed, developed and adopted in advance of compliance or regulatory mandates. - These are configured as a method for guiding enterprise behaviour as a competitive advantage.
7	Organizational Awareness (New feature implementation)	New techniques and features in terms of IoT are overlooked by the organization and not maintained.	- There are some people within the organization that are aware of new techniques out of interest and mention them sometimes. - They are probably not being implemented, but there is some awareness.	New techniques that seem interesting to the organization are being documented for future exploration or implementation.	New features are being implemented once they become a "late majority" feature by which upgrading commercial software packages who use it.	There is an active culture of experimentation with new features in a test environment. Once deemed successfully tested, new features might be implemented.	- The organization is able to proactively address emerging trends related to Internet of Things as the global business environment and associated risks continue to evolve. - Continuous improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.
8	Stewardship	Data output might be used sometimes in some reports, but there is no consistent, defined method.	- Clear accountability for information assets is implemented on a limited or localized basis. - There are no organization-level standards for identifying information assets or establishing clear accountability for those assets. - Accountability is viewed as and assigned to technology / technology resources.	- The concept of Data Stewardship is emerging, at a localized or tactical level. Roles within the business areas and IT are being labeled "Data Stewards". - The focus of the roles is "data" and this at the IoT level. - The need for consistency in approach and Executive level strategies and roles are emerging.	- A business model for accountability of data, associated standards and guidelines is in place and endorsed at the Board level. - The role of Business Information Steward in managing information content, and the relationship with IT roles as custodians of business information is understood. Business Executives are engaged in developing and enabling a more strategic approach to Internet of Things.	Business Information Stewards are establishing IM programs across the organization, and organizational structures are in place to ensure consistency in practice, compliance with Data Governance standards, and ongoing investment in Internet of Things.	- Stewardship roles, structures, and processes have enabled the organization to optimize the value of its information assets by ensuring that information is aligned with business strategy, enabling a more planned and coordinated approach and increased sharing of assets vs. unnecessary duplication of effort.
9	Audit & Reporting	- No standard reporting processes exist. - Management's ability to understand the data consistently across the enterprise is limited. - The quality of consolidated financial or performance reporting is suspect.	There are some people in the organization who set up the system. They are able to retrieve (audit) logs.	- High-level reporting processes exist, however these do not provide assurance or improvements in consistent reporting quality. - Data is not conformed and strategic analysis is limited or limited in effectiveness as a result.	- Comprehensive and consistent reporting processes exist supported by adherence to conformed enterprise data definitions. Reporting requirements are integrated into organizational processes and the data management lifecycle. - Regulatory compliance drives such efforts so reports are more informational than strategic.	- Comprehensive, conformed reporting processes and monitoring is integrated into organizational standards. - Output of reporting is understood and leveraged for strategic purposes and provides an accurate and comprehensive view of enterprise performance. - Formal customer notification processes exist and are followed, for all Data Breaches, regardless of whether or not such action is legally required. - Focus of notification is on protecting interests and well-being of organizational customers with a long-term view of building sustainable relationships.	- Comprehensive, conformed reporting processes and monitoring is integrated into organizational standards. - Output of reporting is understood and leveraged for strategic purposes and provides an accurate and comprehensive view of enterprise performance. - Reporting also supports security standards, data classification, control assessment, incident response, and reporting processes. - Formal customer notification processes exist and are followed, for all data breaches supporting internal and external interests and impacts are factored into planning forecasts.