IoT Maturity Model for Hospitals

Manual

Internet of Things maturity model for hospitals

Manual

A guide accompanying the paper titled "A Maturity Model for IoT Adoption in Hospitals"
Authors: omitted for double-blind review
The 52nd Hawaii International Conference on System Sciences (HICSS 2021)

Mature

Table of content

Introd

Introduction

Welcome

Maturity models are mostly concerned with the performance of organizations. In this sense, organizations are the units on which the model is applied. Unit is a rather flexible denomination. It can for example be a medical unit within a hospital, but it is more often used to refer to a hospital in its entirety.

This model has been set-up with a context of the Belgian hospital and healthcare landscape, your mileage may vary when applied to different healthcare structures.

Names omitted for double-blind review
Authors

“The levels of the maturity model can be used to determine organizations’ current capabilities in the field of IoT”

Levels

Levels

Concept

The levels in a maturity model define the level of maturity an organization has in terms of IoT implementation. The levels of the maturity model can be used to determine organizations current capabilities in the field of IoT, but the levels can also provide a goal. In that way, they act as a north star for an organization to strive towards.

Initial

At the initial level, the hospital just made its first foray into IoT. Some medical equipment might be equipped with IoT capabilities, but these capabilities are not actively utilized yet.

Performed

At the performed level, hospital organizations are looking into experiments, or indeed are thinking about establishing a proof of concept (POC) or pilot program to explore new opportunities using IoT-technology.

Medical equipment, sensors or even wearables are used to enhance (or even invent new) medical processes. The IoT performance could be applied to either patients (tracking of medical measurements) or logistics (tracking of room temperature, medication temperature or location of equipment within the hospital for example).

Managed

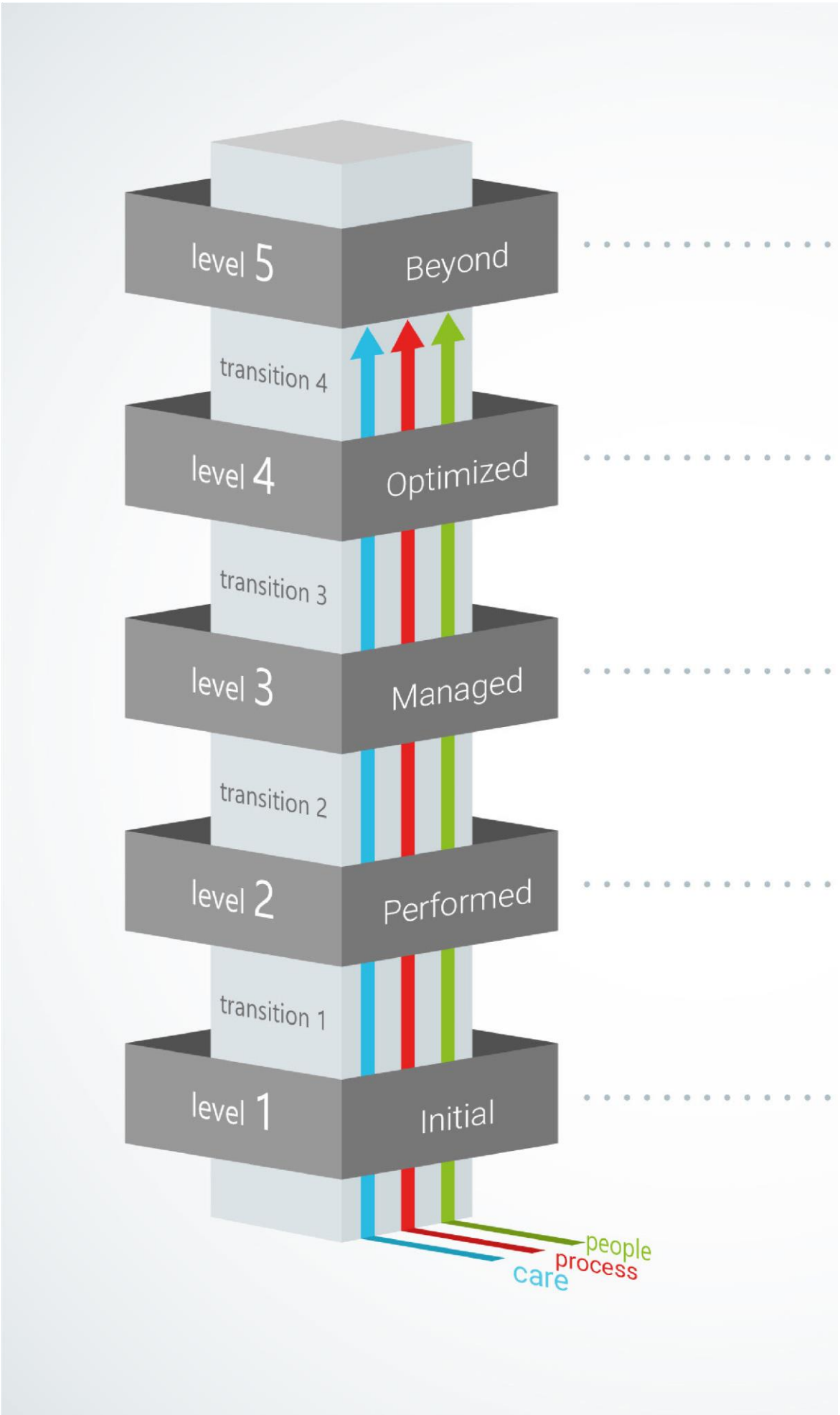
At the managed level, there is often more than one IoT project already operational in the organization. There is a focus on having foundations in place that require a level of standardization for IoT equipment and applications. In this level, there is often an agreed upon approval process which has to be followed before allowing IoT equipment to be deployed within the organization.

Optimized

When an organization has reached the optimized level, the organization implements IoT in an efficient way. Standards and processes related to IoT are actively maintained and improved.

Beyond

When organizations have reached the ‘beyond’ level in the IoT maturity model, they have surpassed all expectations of an optimized organization and can be positioned as examples for other hospitals. Not only is the organization optimized, but it even brings added value in terms of innovation in the field of IoT in healthcare and legislation. Organizations on this level help shape the future of healthcare.


level 5
Beyond
transition 4
level 4
Optimized
transition 3
level 3
Managed
transition 2
level 2
Performed
transition 1
level 1
Initial
people
process
care


Beyond
When organizations have reached the 'beyond' level in the IoT maturity model, they have surpassed all expectations of an optimized organization and can be positioned as examples for other hospitals. Not only is the organization optimized, but it even brings added value in terms of innovation in the field of IoT in healthcare and legislation. Organizations on this level help shape the future of healthcare.
Optimized
When an organization has reached the optimized level, the organization implements IoT in an efficient way. Standards and processes related to IoT are actively maintained and improved.
Managed
At the managed level, there is often more than one IoT project already operational in the organization. There is a focus on having foundations in place that require a level of standardization for IoT equipment and applications. In this level, there is often an agreed upon approval process which has to be followed before allowing IoT equipment to be deployed within the organization.
Performed
At the performed level, hospital organizations are looking into experiments, or indeed are thinking about establishing a proof of concept (POC) or pilot program to explore new opportunities using IoT-technology.
Initial
At the initial level, the hospital just made its first foray into IoT. Some medical equipment might be equipped with IoT capabilities, but these capabilities are not actively utilized yet.

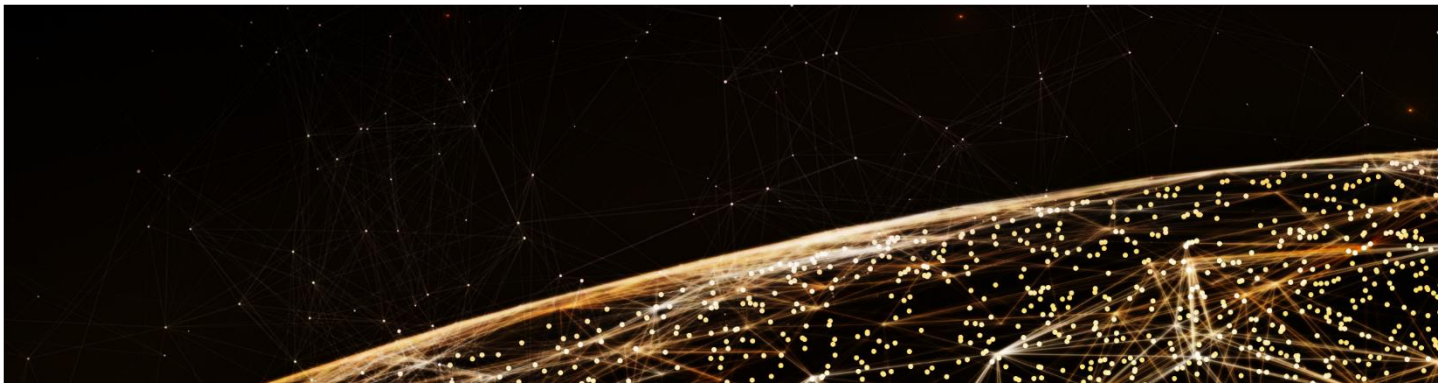
Domains

Concept

The domains that the maturity model covers are listed on the left-hand side of the maturity model, these are considered the topics that are being assessed when you measure a hospital organization in terms of IoT maturity.

Value Creation

The process by which IoT projects are assessed to maximize value creation for the implementing hospital. This value creation is often expressed as either an increase in the quality of the implanting hospital's medical care or a cost reduction in running its medical operations. Cost reduction can be achieved by example by utilizing the hospital assets in a more efficient way.



Privacy & security

Describes the policies, practices and controls used by organizations to mitigate risk and protect IoT assets. The protection of those assets can be achieved by ensuring the integrity of the software running on the devices, equipment and machines, by ensuring the generated data cannot be seen by unauthorized people and the integrity of said data remains intact.

Compliance & policy

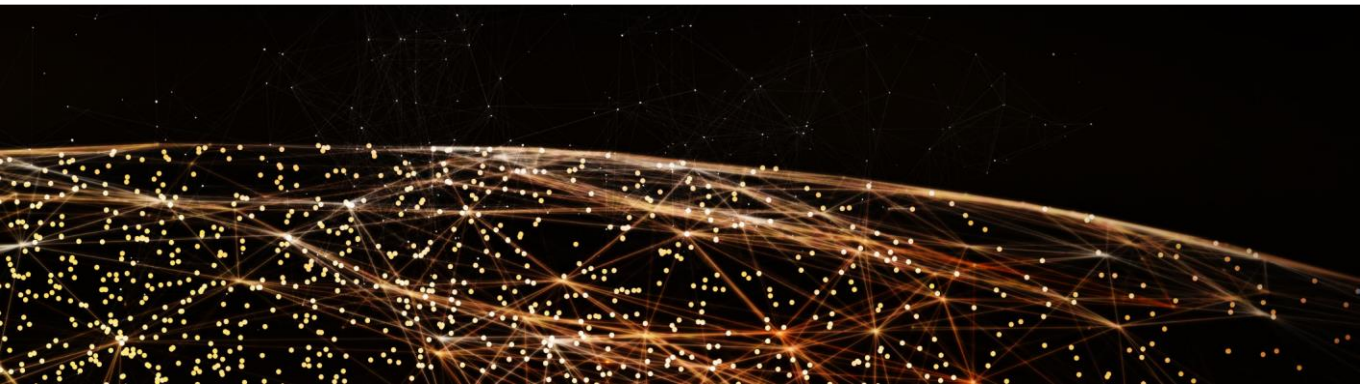
Policy is the written articulation of desired organizational behavior. This policy can be defined in such a way that it raises the quality of IoT and IT in the organization or to comply with existing legislation.

Connectivity

The domain “connectivity” measures the maturity of IoT architecture and infrastructure within the organization. A lot of technology infrastructure needs to be put in place to engage in IoT activity. For that reason, it is important to assess the maturity in this regard in an IoT maturity model.

Data governance

Data governance comprehends the steering and responsibility in terms of data within the organization. This role includes the responsibility over methods to measure, improve, and certify the quality and integrity of production, test, and archival data. The data being outputted from IoT devices can be considered metadata that bridges human and computer understanding. In this domain the role of responsibility over data is covered as well. In healthcare, a systematic policy-based approach to information collection, use, retention and deletion is a must.

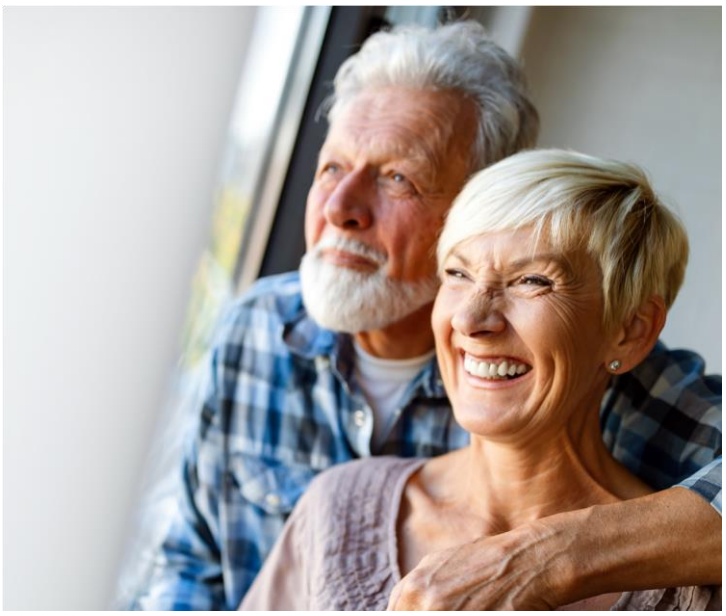


Organizational culture

Organizational culture describes the level of mutual responsibility between business, IT, medical units and management. It describes how open an organization is terms of innovation and employee participation.

Monitoring

Monitoring is a term, coming from the healthcare quality assurance domain. It stresses the importance of measuring your results against a baseline. That baseline can be predefined in a model by a recognized body, comparison internally within the different medical units or even benchmarking against other hospitals in neighboring countries or even globally.



Governance

Governance describes the quality control discipline in which the organization has clear demarcation of responsibilities assigned to different teams within the hospital. These teams ensure custodial care of data for asset enhancement, risk mitigation, and organizational control. They also set up the organizational processes for monitoring and measuring the data value, risks and efficacy of governance.

MATURITY MODEL FOR I

	Domain \ Level	1 Initial	2 Performed
WHY?	Value creation	Internet of things is considered an immature, novelty technology, not mature enough to provide aid or added value in healthcare in a reliable way.	The Internet of Things integration is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort. There is no "wrong" data collected as the standard for what is "right" is not defined on an enterprise level.
	Privacy & Security	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. The integration that is planned to happen is being verified by the IT security department on security risks and requires approval before deployment. The IoT equipment can demonstrate compliance with international standards, such as ISO 22301 for business continuity management, ISO/IEC 27001 for information security management, and ISO/IEC 27018 for data privacy in the cloud.
	Compliance & Policy	The IoT regulatory, legal and rights related challenges are not being explored and unknown to the hospital. It would therefore be risky to engage in IoT activity.	The regulatory limits in terms of IoT are explored and taken into account for the project. Policies are defined and enforced at the departmental level.
WHAT?	Connectivity	The architecture currently in place is insufficient to accommodate for a pilot IoT implementation.	The initial investment or budget for upgrading infrastructure is made or taken into account using real-life simulations: Cost of design, equipment, installation and maintenance is taken into consideration. Tracking and monitoring infrastructure is limited to the scope of the business case. The existing eco-system is taken into consideration when applying a business case.
	Data governance	It is understood that data will be an important aspect of IoT and will be a driver for key decisions in the value-chain. Data is currently not actively extracted and/or captured from the (medical) equipment and the ability to do so is not a deciding factor in choosing equipment.	There are trials or experiments capturing data from sensors or medical equipment. A standardized storage structure is not a focus in this level. The manner of handling the sensitive data is taken into account and meets all regulatory standards. The organization has identified processes where data is created or acquired. There is low-level awareness of the concept of IoT data.
HOW?	Organizational culture	The basis for sharing and exploiting the value of IoT is hampered by a lack of strategic vision and coordination. New techniques and features in terms of IoT are overlooked by the organization and not maintained.	Collaboration is happening in a limited scope, required for some projects to succeed. New IoT features are being implemented ad-hoc by upgrading medical equipment or software packages who use it. There are some people within the organization that are aware of new techniques out of interest. There is an IoT/data resposible being assigned within the unit the projects takes place in.
	Monitoring	There is no monitoring happening in terms of IoT.	Medical units are being monitored and compared internally against each other in terms of IoT implementation and progress.
	Governance	There are no organization-level standards for identifying IoT assets or establishing clear accountability for those assets. There is no idea on how IoT usage would need to be reported about, therefore there are no standard reporting processes. Management's ability to understand the data consistently across the organization is limited.	Clear accountability for information assets is implemented on a limited (unit or project) basis. Accountability is viewed as and assigned to IT departments. Formal patient notification processes exist and are followed, for all Data Breaches, according to GDPR guidelines. High-level reporting processes exist; however, these do not provide assurance or improvements in consistent reporting quality. Strategic analysis is limited or limited in effectiveness as a result.

OT IMPLEMENTATION IN HOSPITALS

3 Managed	4 Optimized	5 Beyond
Value is realized on a small scale and does not support strategic objectives and activities. Value is loosely defined at the enterprise level and achieved inconsistently by some local / departmental use of data.	Value is clearly defined by the hospital and medical units recognize their roles in value creation. Common organization-wide IoT-data and definitions are consistently used.	The usage of IoT as a tool to obtain information and knowledge different aspects within the hospital, as well as to provide comfort and care to patients, is embraced. The technolog reached commodity status and is often iterated upon to furth medical care in their daily activities.
Security standards are documented, published, and easily accessible, though compliance to standards are now universally monitored, and risks associated with non-compliance are comprehensively understood. 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. Software running on the medical and IoT devices are regularly being verified to ensure the integrity of the data being sent.	Security standards are documented, published, and easily acce Ongoing compliance with standards is measured via auto processes that are integrated with problem resolution and auto deployment systems. Penalties exist for non- compliance hospital standards and remediation is executed in a predi manner.
There is a person or team within the legal department actively maintaining knowledge about IoT and data-specific legislation. The legal body verifies additional IoT projects (about to be) implemented in the hospital. There are some common criteria and policies around IoT and its data classification. Some formalization of board approved policies is in place, but enforcement may be inconsistent or lacking.	The hospital has adopted a collaborative approach to IoT policy discussion. Since IoT is a challenging area for policymakers, bringing together the expertise on the topic with the development of policies, accelerates the evolution of internal policies. 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 ad of compliance or regulatory mandates. To mitigate the rapid p IoT technology surpassing regulatory frameworks, the h promotes internet and IoT with legislative bodies. The organiza able to proactively address emerging trends related to Inter Things as the global business environment.
Connection architecture is defined, basic infrastructure is in place to ensure a consistent, reliable method to track assets and personnel within the hospital. There is careful consideration for what assets are worth tracking and the investment is made to cover that. The hospital is willing to make investments to improve IoT infrastructure and aid the medical units with their IoT projects.	There is an extensive infrastructure installed all-around the hospital, making future IoT implementation cost relatively inexpensive.	The hospital makes recurrent investments in the IT an infrastructure allowing to lower the project budgets for ne projects.
The application is in a pilot phase, capturing data within a narrow hospital unit. Procedures to ensure data quality to the core unit are being established and applied to the whole unit. Some data is consistently defined within hospital units but there is no assessment of consistent or coherent use across hospital units or in managing or conforming data in new applications. Data management processes are mature but may not address key data quality, data enrichment, or data aggregation / consolidation opportunities. Organization has defined approval processes for data creation, acquisition and destruction. Critical data quality considerations are known. Technical metadata providing traceability and transparency is mature.	Organization has routine approach to data creation and acquisition. Data quality is recognized as an organizational issue and is being addressed though planned and coordinated efforts. Data definitions exist. 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. 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. Organization has defined processes for migration, reuse, transformation, aggregation and consolidation. Metrics for data quality exist and are actively monitored. Information is consistently defined across the enterprise, resulting in improved effectiveness and efficiency.	Robust data classifications and definitions exist and are uni understood and used across the enterprise. Classification sc focuses on business value of data and can be used to quanti expected impact of an incident. Metadata is consistently us reporting, new product or application development. Data quality are routinely identified and remediated. The use of high volu high-quality data allows the hospital to improve according t defined patient segments as well as forecasting models that co improved recovery rate as well as cost approaches. Output o classification is also integrated into controls framework, inc response, benchmarking, and patient processes. Hospital under data as a corporate asset and seeks opportunities to enhan quality and use of data for operational purposes. Data quality are anticipated and addressed proactively.
Collaboration across organizational units is encouraged and co-creation is fostered. There is limited awareness about the IoT evolutions throughout the organization. New IoT features are implemented when the added value is highlighted within a project. Wihtin the hospital management level, there is a resposible for IoT, having expertise on decision-making level.	Management is transparent with their employees about IoT implementation and thus changes to the processes. Employees feel heard by management and ideas and concerns are taken seriously. New techniques that seem interesting to the organization are being documented for future exploration or implementation. A full, collaborative IoT team is in place synchronizing between legal, management, IT and the inidividual medical units.	Risk taking and pursuing change is encouraged and reward empower those who adapt. The organization is able to proa address emerging trends related to Internet of Things as the business environment and associated risks continue to evolve. is an active culture of experimentation with new IoT features in environment. Once deemed successfully tested, the result considered by the management. Continuous improvement is e by quantitative feedback from the process and from piloting inno ideas and technologies.
The hospital has a unified way to measure its IoT quality up against other hospitals around the world, a process named benchmarking. The hospital performance is lower compared to public hospitals within the country or in neighbouring countries.	The hospital is on equal level with hospitals within the country or compared to neighbouring countries when measured using a unified methodology.	The hospital is a significant leader compared to comparable hospitals within the country or beyond. It sets example in terms integration and has novelty applications implemented.
The concept of IoT/Data Stewardship is emerging, at a localized or unit level. The role of Business Information Steward in managing information content, and the relationship with IT roles as custodians of medical information is understood. Roles within the unit areas and IT are being labelled "IoT/Data Stewards", the focus of the roles is "IoT data". There is a clear view on how to retrieve (audit) logs and what information they contain. Regulatory compliance drives such efforts, so reports are more informational than strategic. The need for consistency in approach and Executive level strategies and roles are emerging. Business Executives are engaged in developing and enabling a more strategic approach to Internet of Things.	IoT 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 IoT. A business model for accountability of data, associated standards and guidelines is in place and endorsed at the Board level. 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.	Stewardship roles, structures, and processes have enable organization to optimize the value of its information assets by en that information is aligned with business strategy, enabling a planned and coordinated approach and increased sharing of ass unnecessary duplication of effort. Comprehensive, conf reporting processes and monitoring is integrated into organiz standards. Output of reporting is understood and leverage strategic purposes and provides an accurate and comprehensive of enterprise performance.

Assessment

Concept

To asses a hospital on the maturity model, an assessment sheet has been included. It serves as an initial guideline in your path to assessing the IoT maturity of a hospital.

This assessment sheet has been constructed in Microsoft Excel and includes various data validation parameters and formulas to ease the result generation of such an assessment.

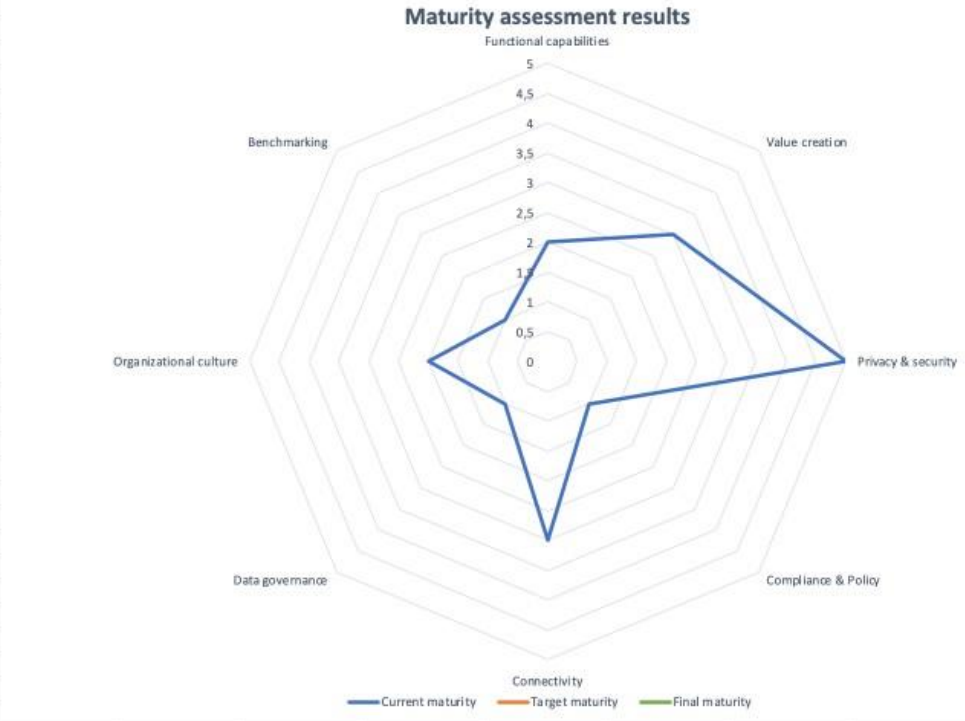
Results

The results page in the worksheet presents a clear overview of the different domains handled in the multiple tabs of the worksheet. The calculations are made and presented in the table in the top part of the page. Underneath, the user finds a spider chart visualizing the domain scores and highlighting discrepancy between them.

For every domain, the user is able to select whether it is applicable (Yes/no) to the organization and provide a weight (0,5; 1; 2 or 3) for it to count towards the weighted average maturity score. With the exception of 'Functional capabilities', all the scores are retrieved from the other sheets in the assessment document.

Maturity model assesment results

	Current maturity			Target maturity			Final maturity		
Measuring date									
Domains	**Applicable**	**Weight**	**Score**	**Applicable**	**Weight**	**Score**	**Applicable**	**Weight**	**Score**
Functional capabilities	Y	1	2	Y	1		Y	1	
Value creation	Y	1	3	Y	1	0	Y	1	0
Privacy & security	Y	1	5	Y	1	0	Y	1	0
Compliance & Policy	Y	1	1	Y	1	0	Y	1	0
Connectivity	Y	1	3	Y	1	0	Y	1	0
Data governance	Y	1	1	Y	1	0	Y	1	0
Organizational culture	Y	1	2	Y	1	0	Y	1	0
Benchmarking	Y	1	1	Y	1	0	Y	1	0
		Total	1		**Total**	0		**Total**	0



Functional capabilities

The assessment of functional capabilities is a topic in the assessment model reserved for the measurer's subjective perception of the organization. There could by underlying reasons why an organization could be considered more, or less, mature compared to what the objective scorecard is able to provide. It is important to have the same assessor measuring the functional capabilities of the organization in the 'current' maturity and 'final' maturity at a later stage.

Connectivity assessment

			Current			Target			Final			
Identifier	Question	Answer	Applicable	Weight	Score	Applicable	Weight	Score	Applicable	Weight	Score	Comments
CON-1	Do you own the connectivity layer?		Y	1		N	1		N	1		
CON-2	If you do not own the connectivity layer, what SLA's are agreed with your connectivity provider?		Y	1		N	1		N	1		
CON-3	How reliable is the message transmission?		Y	1		N	1		N	1		
CON-4	What type of sensors are in use in the hospital?		Y	1		N	1		N	1		
CON-5	What communication protocols are used for IoT within the organziation?		Y	1		N	1		N	1		
CON-6	Do your IoT devices communivate uni- or bidirectional to the gateway?		Y	1		N	1		N	1		
CON-7	What technology is in place to communicate from the devices to the IoT gateway?		Y	1		N	1		N	1		
CON-8	What technology is in place to communicate from the gateway to the data aquisicion platform?		Y	1		N	1		N	1		
CON-9			N	1		N	1		N	1		
CON-10			N	1		N	1		N	1		
CON-11			N	1		N	1		N	1		
CON-12			N	1		N	1		N	1		
CON-13			N	1		N	1		N	1		
CON-14			N	1		N	1		N	1		
CON-15			N	1		N	1		N	1		
				Current maturity	0		Target maturity	0		Final maturity	0	

Domain Scorecard

By assessing each domain individually, the assessment can highlight the weaknesses of the organization and provides an investment focus to lift the organization to a higher level.

A domain scorecard assists the assessor of the IoT maturity level with some example questions that should be answered while assessing the organization.

Similar to the results page, the assessor indicates whether the question applies to this organization, provides a weight and finally scores the performance on the specific question.

The most notable difference is the ability to provide a written text answer, as well as comments to trace the source of information for this assessment.

2021