

IoT Governance
Governance framework



Contents

Introduction	04
Background and context	05
Why do we need IoT Governance?	07
Aspects and key components of IoT Governance	08
Roles and responsibilities of IoT Governance stakeholders	10
Implementing the IoT Governance framework	11
IoT Center of Excellence	12
IoT Governance challenges related to future trends	13
Conclusion	14
References	14

Introduction



The major change that the Internet of Things (IoT) is bringing to the digital ecosystem at various levels (organizational and national) is the opening up of the discussion on how to govern the work around this new disruptor.

This paper focuses on IoT governance related issues. In the sections of this paper we will provide the context and a brief background on the emergence of IoT, discuss how IoT operations can be governed and what is needed, including the roles and responsibilities involved in IoT governance, and describe a proposed governance framework implementation as well as the future challenges facing IoT governance.

This paper is intended to showcase how IoT governance can be implemented. However, it is important to note that the IoT industry is going through rapid and major developments on a daily basis, hence agility and an open mindset are crucial for the success of any such governance schemes.

IoT is essentially a giant network of connected devices. The Joint Coordination Activity on Internet of Things (JCA-IoT) calls IoT “a global infrastructure for the information society.”

Background and context^{5,6}

In recent years, the Internet of Things (IoT) has been a buzzword in the technology space, used to refer to multiple applications and scenarios. However, let us take a step back and ask just what IoT exactly is. In simple terms, it is essentially the connection of devices to the Internet and the connection between them through sensors. These devices include everything from handheld gadgets to washing machines, coffee makers to toasters and almost any other device you can think of. According to Business Insider, forecasts predict that by 2027 there will be over 41 billion connected devices. Therefore, IoT is essentially a giant network of connected devices. The Joint Coordination Activity on Internet of Things (JCA-IoT) calls IoT “a global infrastructure for the information society”.

To understand the complexity of IoT and the pressing need to properly govern this ecosystem, it is worth looking into the components that build up this giant network of connected devices.

1. Gateways

Gateways enable the easy management of data traffic flowing between IoT devices and networks. They also translate the network protocols and make sure that the devices and sensors are connected appropriately. Gateways can also work to pre-process the data from sensors and send them off to the next layer, as well as providing proper encryption with the network flow and data transmission.

2. Analytics

The analog data that are derived from devices and sensors are converted into a format that is easy to read and analyze. The key attribute of the IoT ecosystem is that it supports real-time analysis that detects irregularities and prevents data loss or data scams to prevent malicious attacks.

3. Connectivity of devices

The main component completing the connectivity layer are sensors and devices. Sensors collect information and send it off to the next layer, where it is processed. With the advancement of technology, semiconductor technology allows the production of smart micro sensors that can be used for several applications, some of which are as follows:

- Proximity detection
- Humidity or moisture level
- Temperature sensors and thermostats
- Pressure sensors
- RFID tags, etc.

Modern smart sensors and devices use various ways to connect. Wireless networks like LoRAWAN, Wi-Fi, and Bluetooth make it easy for them to maintain connectivity (please refer to figure 1 to view the indicative layers for IoT).

4. Cloud computing

With the help of the IoT ecosystem, organizations are able to collect bulk amounts of data from sensors, devices, and applications. There are various tools that are used for the purpose of data collection that can collect, process, handle and store the data efficiently and in real time; this can be performed by using IoT Cloud.

5. User interface

The IoT ecosystem depends immensely on user interfaces, which provide a visible and physical part that can be easily accessed by the user. It is important to have a user-friendly interface to ensure a proper user and administrator experience.

The term IoT governance is still in its early stages and there are no definitive limits on what IoT governance should include, or which areas it should cover.

6. Standards and protocols

It is important to choose a platform that will enable IoT devices to interact with the system. Thus, interaction with different devices and networks with the same standard as IoT is possible. It is important to have the same protocol to have a successful interaction.

7. Database

The usage of IoT is increasing dynamically and this is dependent on data that is generated by the IoT network. The amount and type of data generated by the IoT network requires a proper data lake in place to be able to store and process the data sets generated.

8. Automation

Automated decision-making is enabled by the type, frequency, and amount of data generated by the IoT network. In addition to that, the emergence of AI technologies supports proactive predictive decision-making scenarios. Such predictive scenarios relate to user behavior and how it affects the activation/deactivation of IoT connected devices.

9. Interoperability

IoT is the latest advancement in technology where the need for development is growing and increasing with time. IoT-related technologies and devices are still undergoing rapid development and enhancement cycles without common industry standards in place as yet. As IoT works with more than one device and system, it is important to ensure interoperability across the whole IoT ecosystem.

With the rise of IoT, while we have seen an increase in convenience, it has also given rise to challenges. The most important question is how do we govern the interaction between these devices?

We believe that at a minimum, IoT governance should address a combination of IT governance, enterprise architecture governance, data management governance, and information security governance.

Governance originates from the Greek verb *kubernaein* [kubernáo] (meaning to steer, and can be traced back to early Modern England. The term was used in constitutional publications and letters where it was used to refer to arrangements of governing and ruling methods.

Currently, the term is used to describe a broader set of institutional activities for different types of institutions (Public, Private, and corporate), and it can be associated to a particular field (Environmental, Internet or Information Technology). Governance is a theoretical set of rules, actions, and processes used to stabilize institutions, organizations and communities and to ensure a persistent and stable outcome from the members of those entities.

From an information technology perspective, the term governance refers to the tools, processes, controls, and frameworks that ensure efficient and effective use of technology resources to enable an organization to achieve its goals. As IoT has emerged, along with the development of sensors that can transmit data about the status of their environment, organizations, governments and civil society institutions have become more interested in setting the right processes and frameworks to ensure that devices

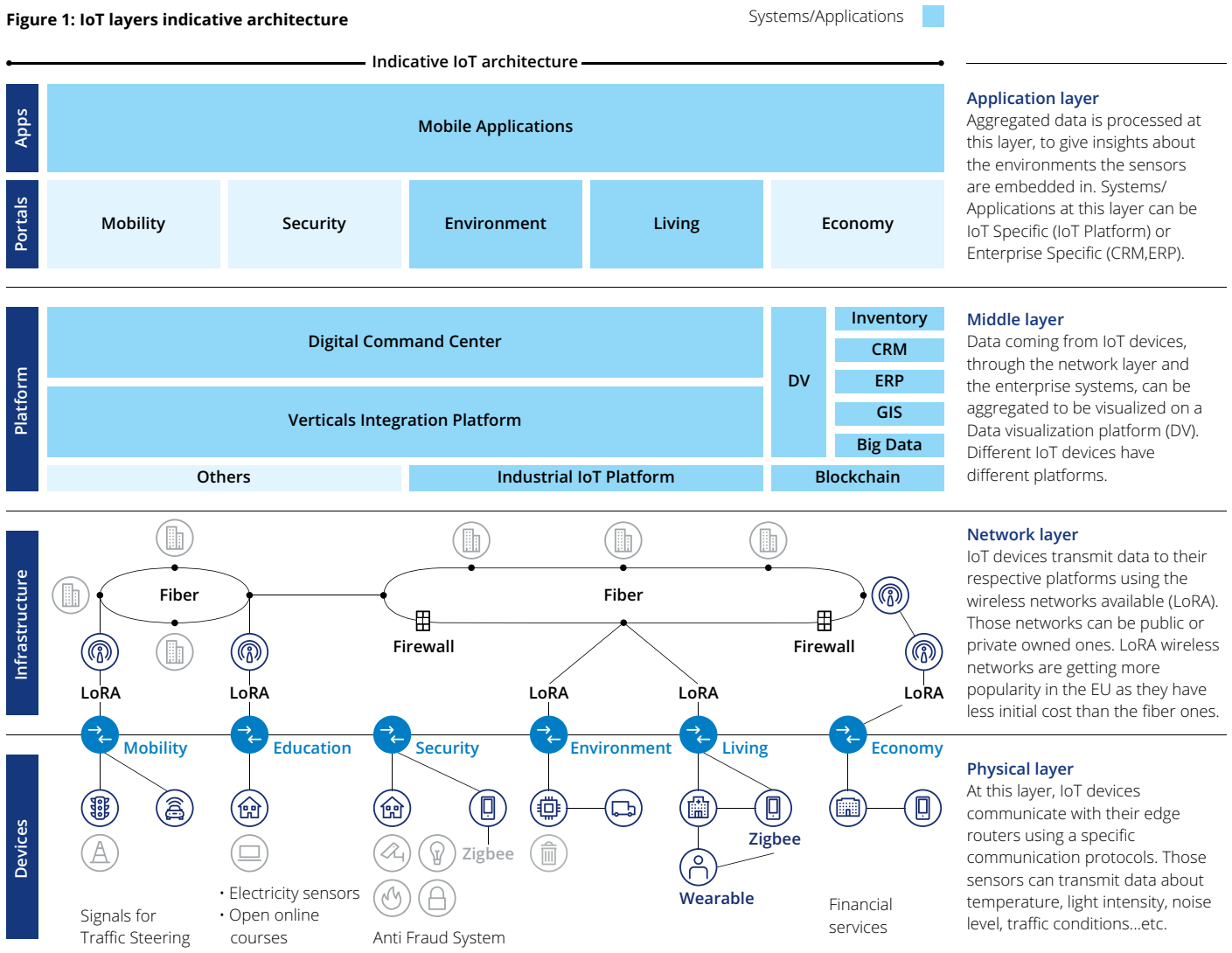
are functioning in a controlled manner and can be protected against any unlawful intrusions or intercepts.

The term IoT governance is still in its early stages and there are no definitive limits on what IoT governance should include, or which areas it should cover. IoT devices are rapidly evolving in terms of their capabilities and functions, and the large-scale implementations of IoT devices is still growing. Hence, it is still not clear which areas should be addressed by any IoT governance framework that will evolve. However, we believe that at a minimum, IoT governance should address a combination of IT governance, enterprise architecture governance, data management governance, and information security governance.

Why do we need IoT Governance?

The rationale behind any governance framework is to stabilize the operations of any institution and ensure a consistent and stable outcome.

Figure 1: IoT layers indicative architecture



In the case of IoT, the IT areas affected by this new technology could be split into three: data, infrastructure, and architecture. In the same manner, the aspects of any IoT governance framework should cover these three areas. An IoT governance framework should ensure data

integrity and data security for information shared by all IoT devices in the enterprise network. It should also maintain the trusted source of information across the different layers of the IoT architecture.

In addition, the framework should ensure that all infrastructure devices, and IoT devices in particular, are well protected, physically and digitally, to prevent any unlawful intrusion or improper functioning.

Aspects and key components of IoT Governance^{1,2}

As previously mentioned, the IoT framework should cover the three main areas of data, infrastructure, and architecture. However, which aspects of these should be of higher concern to any IoT governance framework?

First is the applications associated with collecting, analyzing and monitoring the data provided by the IoT devices. At a high level, these applications should be well governed to protect the data acquired and processed by them. It should also provide controls for accessing this data, such as role-based access, for example.

Second is the platform; all platforms related to data management, application integration, and IoT device management should have a well-defined framework as to how to register/de-register IoT devices, how to collect data, how and where to publish this data, and how to interact with upper and lower layers of the IoT reference architecture.

Third is the communication. This refers to all communication between devices at the physical end up to the consumption of the collected data. The IoT framework should tap into the protocols of transporting this data across all layers and take into consideration any regulatory requirements (local and international), with the General Data Protection Regulation (GDPR) as an example.

Fourth is the IoT device itself. At this level, the IoT framework should tap into the security of the device, the monitoring of the device, intrusion detection, booting, remote control and firmware management,

and interoperability with multiple vendors' devices.

Across all these areas and aspects of IoT governance, fundamental pillars are required to execute an effective governance framework. In addition, it is important to realize the importance of IoT governance in reaching the aspired digital maturity level. The Deloitte Digital Maturity Model (DMM) is the first industry-standard digital maturity assessment tool developed in partnership with the TM forum with key contributions from other industry and subject matter experts.

First, the IoT governance framework should foster and support digital innovation; IoT adoption is still in the early stages of large-scale adoption and needs an effective IT governance approach to effectively harness its benefits. By that, we mean that a mix of agile and classical IT governance models should evolve to better cope with the fast changing and real-time nature of the IoT ecosystem.

Second, balancing the risk and compliance in the IoT framework is essential to be able to move along the curve of digital maturity. Among the Deloitte 4 dimensions of digital maturity, IoT will affect three of them (Strategy and Culture, Technology, and Operations).

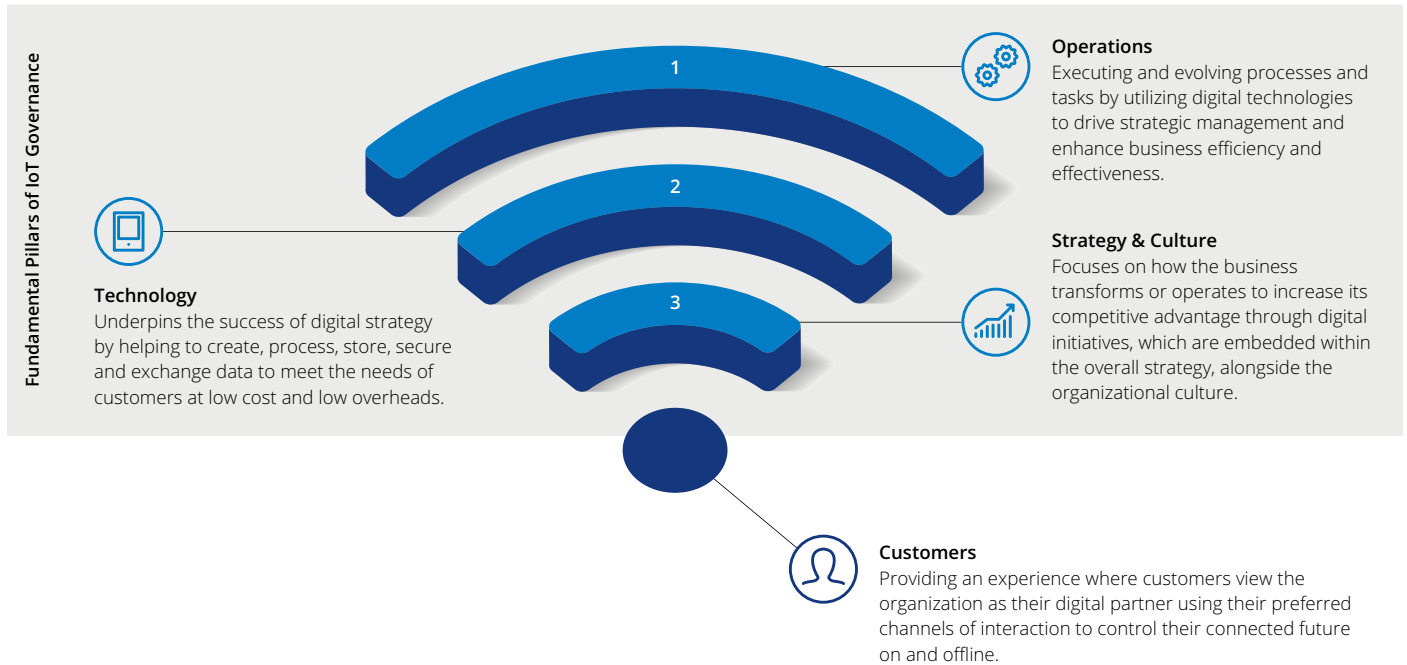
In the Strategy and Culture dimension, the framework should tap into forcing a clear adoption of the right tools and systems to run the IoT ecosystem. A well-defined IoT strategy should be part of the overall digital strategy of any organization.

The right balance of IoT investment is of paramount importance as any IoT governance framework will prove useless if the investment strategy is not well defined.

In the Technology dimension, the governance framework should ensure interoperability across the different layers of the IoT reference architecture, and this can be very specific to the organization's needs and should align with the communication standards and protocols (like periodic log transmissions, detection of anomalies, etc.) of other digital ecosystems at the organization. As part of the technology dimension, there should be a clear data lifecycle management for all data sets generated by the IoT ecosystem, given its specificity and frequency.

In the Operations dimension, the governance framework should set the rules for an integrated digital service management, workflow integration management, and a well-defined service catalogue with other IT systems. The most important aspect of the Operations dimension is the real-time insights and data analytics; as mentioned, the specificity and frequency of the IoT data implies a high level of correlation control points, time-related rules to account for data loss, and data-trust checkpoints for data sources. Finally, a well-defined automation scheme of all relevant resources in the IoT ecosystem is crucial for any successful IoT governance framework.

Figure 2: IoT Governance Pillars mapped to the Dimensions of the Deloitte Digital Maturity Framework



Third is the need for a distributed and balanced authority over all matters related to the IoT system. The distributed nature of IoT systems implies a distributed responsibility and accountability matrix in the organization. The amount of data generated by this system implies a balanced authority over those data sets.

The aspects of IoT governance are not far from those of digital governance, in fact, IoT governance should be part of any digital governance framework any organization wishes to pursue.

Governance is a theoretical set of rules, actions, and processes used to stabilize institutions, organizations and communities and to ensure a persistent and stable outcome from the members of those entities.

Roles and responsibilities of IoT Governance stakeholders^{2, 3}

IoT architect

The IoT architect defines an end-to-end IoT solution architecture. The IoT architect is responsible for defining the IoT platform strategy and the integration of all solution components based on the IoT platform. The IoT architect also establishes standards and guidelines for the development, deployment, and management of the IoT solution.

Security architect

The security architect supports the IoT architect in defining the security solutions by analyzing data, infrastructure, and application security requirements. Moreover, the security architect designs, plans, and implements secure coding practices and security testing methodology, and performs security audits.

IoT developer (in case of IoT development)

An IoT developer is responsible for the development and implementation of all related IoT applications/tools for data collection and data analytics.

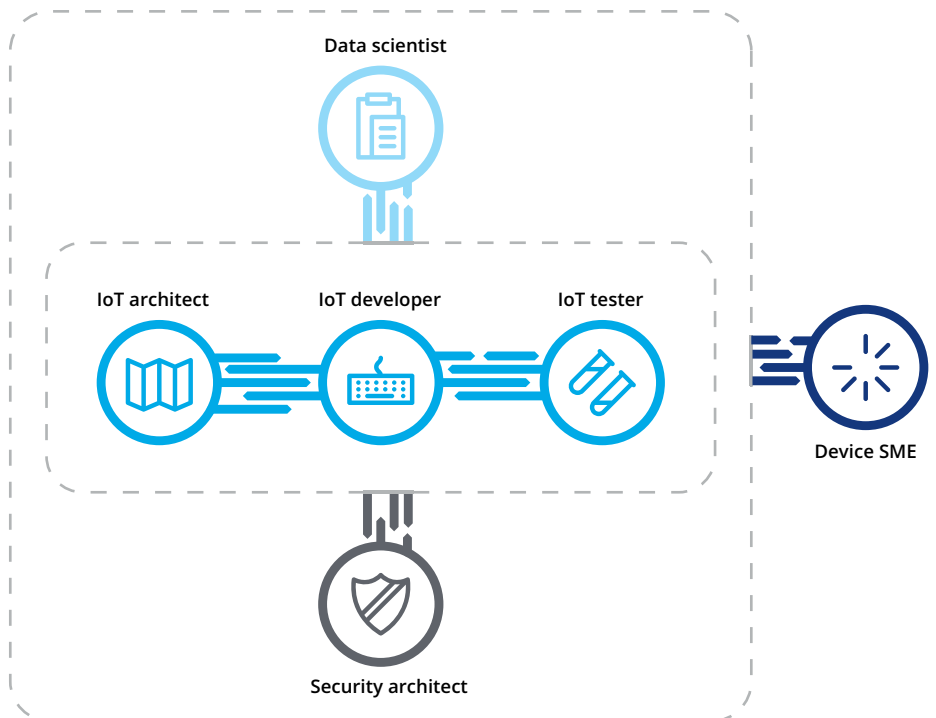
IoT tester (in case of IoT development)

The IoT tester is responsible for testing the developed solutions including the overall solution in addition to security tests.

Data analyst

Data analysts define plans and strategies related to data collection, models, mapping, and reporting.

Figure 3: IoT Governance roles and responsibilities



Device SME

The SME finalizes device/product specifications based on data collection requirements and the IoT solution architecture. The device SME also helps in choosing the right devices/products for the IoT solution and works with the IoT architect and infrastructure architect to set up communication networks that connect IoT devices/products. The device SME is also a key participant in finalizing device management policies and principles, including device/product physical security and cybersecurity.

Implementing the IoT Governance Framework

The real question that follows the formulation of any framework is how to implement this framework. Moreover, the most important question is, does a typical IT governance framework implementation suffice for IoT governance implementation? The straight answer to this question will be no, and the reasoning behind this is the nature of the IoT ecosystem and the need for agile and adaptive governance methodology. The implementation of an IoT governance framework can be divided into four major steps:

First, collect your organization's IoT ecosystem requirements. This involves deciding which controls should be in place to direct investments in IoT systems, and what the organizational goals and KPIs are that need to be tracked in relation to IoT projects. The values of the IoT strategy should be defined and the relative controls set in the IoT governance framework.

Second, design the IoT governance framework. This involves setting the governance groups (their number and mandate), keeping in mind the need for a distributed responsibilities schema to cope with the scattered nature of the IoT ecosystem. The next step would be making sure that the framework covers all areas and aspects related to IoT governance. After that, there should be a scenario analysis for the use cases for the controls and checkpoints defined in the governance. The final step in this phase would be creating a repository for all attributes related to this governance framework for future reference and review.

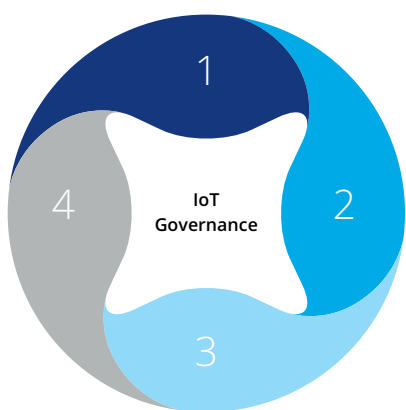
Third, implement and operate the IoT governance framework. After the IoT governance framework has been approved by the organization and communicated to the relative stakeholders, the implementation phase takes place. At this stage, the focus will be on the following:


- Setting up the needed governance

- bodies if they do not exist already
- Building and enriching the needed culture and shift in priorities associated with implementing the IoT governance framework
- Implementing the processes, controls, and associated roles and mechanism to support the work of the governance bodies
- Implementing the change management processes that currently exist at the organization
- Integrating the IoT governance framework with the organization technology/digital governance framework


Fourth, evolve and maintain the IoT governance framework to cope with the nature of the IoT ecosystem. This will take into consideration changes in the IT organization operating model, the progressive cultural shift in the IT department to adapt to IoT, and the change in the organizational goals and strategies.

Figure 4: Steps to implement IoT Governance framework




- 


1 Collect IoT ecosystem requirements

 - Understand the organization's IoT strategy
 - Decide on the controls of IoT investment
 - IoT projects KPIs
- 

2 Design IoT Governance framework

 - Set the Governance groups
 - Ensure all aspects of IoT governance are covered in the framework
 - Scenario analysis and use cases verification
 - Create a repository of all attributes related to the Governance framework
- 

3 Implement and operate IoT Governance framework

 - Setup the relative governance bodies
 - Build the proper culture
 - Implement the defined processes, controls, and associated roles
 - Implement the change management process
- 

4 Maintain and evolve IT Governance framework

 - Monitor change in the organizational goals and strategies
 - Adjust the IT operating models to cope with the needed changes
 - Build the cultural shift needed to continuously evolve the IoT governance framework

IoT Center of Excellence⁴

A dedicated IoT center of excellence (CoE) will form an essential element to enforce governance within an organization and ensure that the enterprise is moving towards a common goal. A CoE can help navigate the various business and technical complexities that may face an organization. Therefore, the function of a CoE can vary according to the needs and nature of an organization. The functions could be defined by what is practically achievable or functionally desirable.

An IoT CoE must be aligned to the goals of the organization, and where it is driven by strong leadership, a clear vision and the necessary tools to work with the relevant stakeholders. It could be the driver of enforcement and ensure that a level playing field is set across the organization.

To ensure governance, the CoE could enforce the adoption of a reference architecture that meets the different organizational needs. The CoE could be entrusted to define the technological standards for all IoT projects and initiatives across the organization. It could also promote the adoption of best practices and develop a strategy to manage the IoT platform and device vendors. In large organizations, it could help facilitate communication and coordination between various stakeholders, including business and IT. With visibility on all IoT projects, it could be the single point of contact to ensure that the appropriate experts, skills and resources are being deployed to

An IoT governance framework should ensure data integrity and data security for information shared by all IoT devices in the enterprise network.

achieve the stated objectives. To ensure alignment to organizational/project goals, the CoE could also be entrusted to review deliverables to ensure alignment to the larger goals of the organization.

Critical success actors:

- The establishment of a CoE that is aligned to the aspirations of the organization.
- The goals and objectives are clearly defined as a CoE can perform multiple functions depending on the organization's needs and goals.
- A clearly defined strategic roadmap and KPIs to measure the performance of the CoE to ensure its alignment with stated objectives.
- The CoE must also have the appropriate leadership and operational skillsets to ensure optimum success and delivery.
- It is agile enough to adapt to any change in circumstances and be able to evolve.

A CoE could perform any of the following functions within an organization to ensure governance from an IoT perspective:

- Review project technology and architecture decisions

- Assist the business department with budgets and business cases
- Drive ideation aligned to business stakeholders
- Advise businesses on IoT opportunities and emerging trends
- Establish IoT requirements and contribute to the development of IoT strategy
- Recommend technologies, vendors and architectures
- Drive and participate in IoT security assessments
- Disseminate knowledge and best practices across the organization where relevant
- Create technology demonstrators
- Facilitate IT/operational technology (OT) integration

IoT Governance challenges related to future trends

The first challenge facing the future governance of IoT is the increasing number of different connected devices; this requires a great deal of complex solutions to accommodate the heterogeneous connection of devices along with the size of the connection, where the implementation of protocols and algorithms of all devices has to be efficient. Data protection and anonymity is another factor threatening security that must be addressed in order to keep users' data secure.

Below are the major trends expected to present challenges for IoT governance:

Data governance

Big data platforms are usually made for supporting the demands of large-scale storage and for performing the investigation which is required to extract the full advantages of IoT. This is the new IoT trend that we are facing and will see in the near future on a largescale. The heterogeneous nature of these platforms and devices will raise major challenges for adopters and implementers as well.

Privacy rights

Wearable devices are being used by the healthcare sector, and will see steady development. However, can you imagine all these medical devices using Cloud and storing their images for intelligent systems? This will raise the question of data privacy among citizens and government regulators.

Security breaches

As the IoT ecosystem spans different layers, the ability to protect each layer from intrusions and hacking becomes a complex process. The fact that the number of physical devices is increasing in large numbers, puts tremendous pressure on organizations and regulators to protect these devices, both physically and digitally.

As mentioned, data protection is a major issue when questioning IoT adoption by citizens and governments. The heterogeneous nature of IoT devices, IoT platforms, and data generated from these devices requires standardized communication and data aggregation layers.

A dedicated IoT center of excellence (CoE) will form an essential element to enforce governance within an organization and ensure that the enterprise is moving towards a common goal.

Conclusion

IoT is changing rapidly and becoming increasingly complex. While its existence is a clear disruptor, its widespread and complex nature requires good governance. An IoT implementation involves multiple components and stakeholders as well as the coming together of multiple internal and external entities related to the organization. The governance of IoT has to be approached in a multi-dimensional fashion by looking at different aspects, such as the various layers and components involved in IoT, the pillars of governance,

the roles and responsibilities, and the various ways in which such governance can be implemented and how IoT is likely to change even more in the future. A holistic approach of this nature will help organizations and nations maximize their benefits while minimizing the risks of IoT implementation.

References

1. Dayal, "IoT Ecosystem Components: The Complete Connectivity Layer", May 28, 2018
2. Gantait, Patra, Mukherjee, "Defining your IoT governance practices", Jan. 19, 2018
3. Serbanati, Rotondi, Vermesan, Baldini, "IoT governance, Privacy and Security Issues", Nov. 14, 2014
4. Jones, Wallin "How an IoT Center of Excellence Can Help CIOs Deliver Better IoT Solutions", July 27, 2017
5. Newman, Peter "THE INTERNET OF THINGS 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue", March 6, 2020
6. IBM "Defining your IoT governance practices", January 19, 2018

Authors



Bhavesh Morar
Partner – Consulting
Dubai
bhamorar@deloitte.com



Yousef Barkawie
Partner – Consulting
Dubai
ybarkawie@deloitte.com



Rajesh Balakrishnan
Senior Manager – Consulting
Abu Dhabi
rabalakrishnan@deloitte.com



Mohammad Khasawneh
Manager – Consulting
Dubai
mkhasawneh@deloitte.com



Jassim Bangara
Manager – Consulting
Abu Dhabi
jbangara@deloitte.com



Hussam Abu Baker
Consultant – Consulting
Abu Dhabi
habubaker@deloitte.com

Deloitte.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche (M.E.) LLP ("DME") is the affiliate for the territories of the Middle East and Cyprus of Deloitte NSE LLP ("NSE"), a UK limited liability partnership and member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL").

Deloitte refers to one or more of DTTL, its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL, NSE and DME do not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories, serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 300,000 people make an impact that matters at www.deloitte.com.

DME would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

DME is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides audit and assurance, consulting, financial advisory, risk advisory and tax, services through 27 offices in 15 countries with more than 5,000 partners, directors and staff.