KORE

Comprehensive Guide to a Successful IoT Implementation

Table of Contents

The Internet of Things (IoT) has evolved to much more than a buzzword, as GSMA forecasts the IoT revenue opportunity to be worth $1.1 trillion by 2025[8]. IoT-enabled technologies are emerging in all areas of the business world, transforming business models and enabling the creation of new products and services across virtually every industry. Organizations of all shapes and sizes are jumping to claim their piece of the IoT pie; however, only 15% of business executives considered their IoT project to be a complete success[1]. To further compound this, 66% of organizations claimed that executing an IoT solution proved to be much more difficult than expected[1]. This is largely because many businesses fail to accurately assess what they know about IoT technologies, what they have in terms of resources to execute an IoT deployment, and what is involved in implementing their IoT solution. To help organizations prepare themselves for IoT success and overcome common IoT deployment challenges, this eBook will explore seven critical steps organizations should take to efficiently get their IoT solution to market, from both a cost and speed-of-execution standpoint, and achieve the highest possible ROI.

66% of organizations claimed that executing an IoT solution proved to be much more difficult than expected[1].

Assessing Organizational IoT Readiness

Before the strategic planning process can begin for the adoption of an IoT solution, the first critical step that an organization should take is to **assess its "IoT readiness"**. By evaluating their IoT maturity level based on two main criteria – Technical Capabilities and IoT Vision – companies are equipped with the contextual information needed to generate a realistic, attainable, and comprehensive IoT strategy and are better prepared to execute against.

A company's "IoT Vision" measures the organization's knowledge of IoT technologies and how, where, and when to apply them to its business processes.

Key areas to consider when evaluating along this axis include:

- Clarity of Return on Investment (ROI) business case for implementing IoT
- Knowledge of the business application and of IoT technologies
- The level of executive buy-in to support an IoT project
- Understanding and/or clarification of the specific goals the business seeks to achieve with IoT
- The organization's level of agility for change management

As referenced in the IoT Readiness Assessment grid, a typical organization starting with some IoT experience might be assessed as "Basic" on the IoT Vision axis, whereas a business that has already deployed a Proof of Concept (PoC) IoT solution may be assessed as "Intermediate".

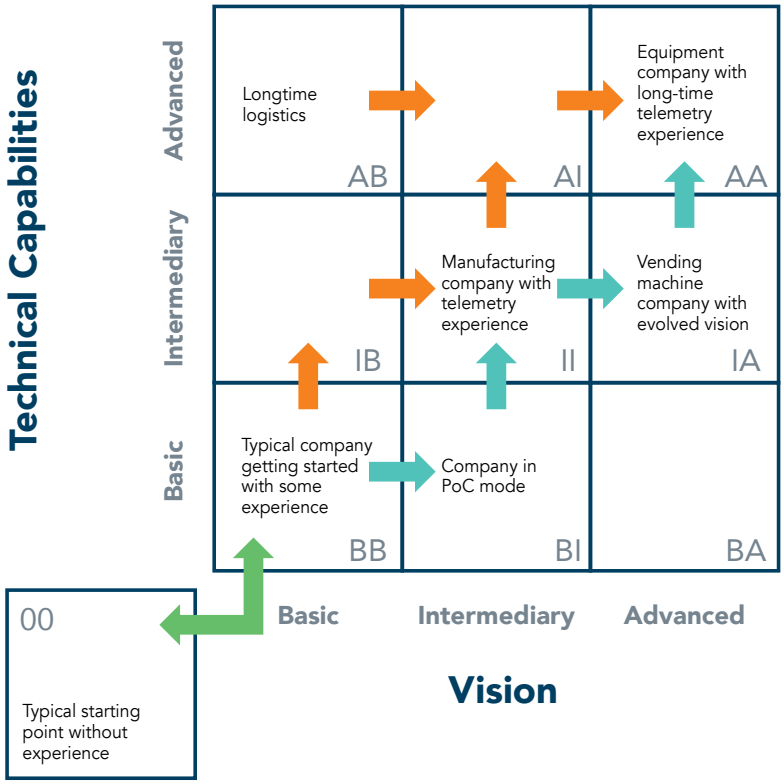
On the other axis, the organization's "Technical Capabilities" is an assessment of the technical knowledge and resources within the organization to execute on the design, selection, development, deployment, and operational management of the IoT solution. Although the most successful IoT solutions are business-centric and target-specific business outcomes, they are highly technological in nature and demand expertise to successfully deploy.

Key areas to consider when evaluating along this axis include:

- The level of internal IoT expertise or skill sets
- The level of traditional technology/IT capabilities related to the IoT project
- Any technology partnerships and alliances that exist currently

Referencing back to the IoT Readiness Assessment grid, a typical organization starting with some technical experience might be assessed as "Basic" on the Technical Capabilities axis, whereas a business with years of logistics technology experience may be assessed as "Advanced".

When conducting an IoT readiness audit, it is important to tap into all departments within an organization to paint the most holistic picture possible and yield the most accurate results. By determining specific, attainable goals, identifying potential obstacles, and thoroughly understanding IoT potential early on, businesses can hop on the fast track to the implementation of a successful IoT solution.



Source: Gartner

IoT Strategy Development

An organization's IoT strategy will dictate the specific details of how and when targeted business goals will be achieved through the implementation of an IoT solution. Leveraging the results of the IoT readiness assessment as a backdrop, the IoT strategy will delve deeper into the specific components and timelines for IoT solution deployment, **providing a framework** for the business to work against. For the highest chances of success, an IoT strategy should be thorough, covering all aspects of business process selection, architecture, technology selection, organization, design, and governance – end-to-end.

Each IoT strategy should begin with the identification of targeted business processes to which the IoT solution can be applied to enable transformation of how a business is run. This information allows organizations to better understand where – globally – these processes take place, which back-end systems the processes are integrated with, and how secure these processes must be, etc., thus guiding many of the strategic decisions that will follow, such as:

- IoT network architecture
- IoT device requirements
- Procurement and sourcing strategy
- IoT partner selection
- Pilot solution(s)
- Solution deployment schedule
- IoT governance

As the details of the IoT strategy begin to fall into place, it is critical for businesses to establish an IoT solution organization and an IoT solution governance to ensure the correct steps are being taken for the strategy to progress as outlined, and to ultimately yield the business results that are expected of the IoT solution implementation.

Each IoT strategy should begin with the identification of targeted business processes to which the IoT solution can be applied to enable transformation of how a business is run.

IoT Security Evaluation

According to a recent study by HP Security, up to 90% of IoT devices collect some kind of personal information. Even further, the number of data breaches in the United States jumped 29% over the course of 2017[3]. It must be understood that **IoT security is paramount to the success** of any IoT solution. The required level of added security measures is directly proportional to the importance and sensitivity of the data and systems that the IoT solution will access. IoT security can be split up into three main "layers", and **best practices should be actualized across all of them** to alleviate risk associated with IoT security issues:

I. Device Layer

The device layer in IoT security relates to the endpoint device that connects to and allows for collection and transmission of data from the physical "thing" in an IoT solution. In order to properly secure an IoT solution on the device layer, organizations must be sure that both the physical properties (i.e. metal casings to prevent SIM card theft), as well as software properties (i.e. firmware, operating systems, applications running on the device) are protected. In regards to software properties, potential security issues should be considered throughout the design process to ensure the firmware can be updated, safeguarding the device from unwanted access and configuration changes. From a software standpoint, there are a number of measures businesses can take to help lock down their devices. Some examples include:

- Use of secure booting to ensure only verified software can operate on the device
- User authentication and authorization to ensure proper access control
- Regularly updated, secure device firmware to avoid unintended network or application usage

It is important to note that some IoT devices are small in size with limited memory and processing resources to support advanced security features. In these instances, organizations should consider cloud-based IoT security solutions.

II. Communications Layer

The communications layer in IoT security relates to the network connectivity technology that enables the device to send and receive data. To properly secure the communications layer of an IoT solution, organizations must consider implementing infrastructure-centric solutions, as well as data-centric solutions.

Network infrastructure security is typically verified with an organization's network connectivity provider(s). Some critical questions that businesses should be asking connectivity providers during the partner selection process include:

- What encryption methods and firewall technologies are used by the network provider?
- Is there an Intrusion Prevention System (IPS) in place?
- Are all servers and network components within the organization's network updated with the latest security patches and updates? Is there a process in place to apply new patches and updates in a timely manner?

In regards to data-centric IoT security measures, best practice solutions revolve around data encryption. Encryption protects IoT data from being accessed and read as it passes through different networks, including the public Internet. **Site-to-site Virtual Private Network (VPN) solutions** as well as data signing solutions are a few examples that ensure authenticity and integrity of transmitted data.

III. Application Layer

The application layer in IoT security relates to securing the application and databases at the heart of the solution. As with the other layers, application security should be considered throughout the development process to protect web, mobile, and cloud components. Best practices to protect this part of the IoT solution include:

- Code analysis tools to automatically inspect source code and identify potential security flaws
- Timely, automated application updates to quickly and efficiently update applications to protect against new virus attacks or other emerging security risks
- Key exchange solutions that enable secure updating of IoT application security keys, even over public networks
- Certificate enrollment solutions to provide each IoT device with a unique identifier, and to verify this identifier before enabling access to systems or networks

Additionally, organizations should implement threat management in order to ensure the availability and integrity of their solutions. Because the world of technology is ever evolving and hackers are constantly improving their attacks, businesses need to ensure that they thoroughly understand their IoT solutions' behavior patterns so they can quickly detect and respond to anomalies. The best way to accomplish this is by implementing monitoring systems across all elements of the IoT solution that notify security teams when a change in device or application behavior is detected.

Network Connectivity Selection

All IoT solutions require network connectivity to function, and the IoT is powered by a broad range of network technologies that facilitate the transfer of data among devices and systems. When designing an IoT solution, organizations must select the option that works best for their unique business requirements. Network technologies can be categorized in three main areas – Personal Area Networks (PAN, i.e. NFC, Bluetooth), Local Area Networks (LAN, i.e. WiFi, ZigBee), and Wide Area Networks (WAN, i.e. Cellular, Satellite) – all of which vary greatly in capabilities related to bandwidth, mobility support, battery life, and throughput, among many others. Among WAN technologies, which account for the majority of B2B IoT solutions, cellular connectivity is the most widely selected network technology with an estimated 450 million cellular IoT connections active in 2017[4].

As the latest "evolution" of cellular networking, 4G LTE is quickly becoming the technology of choice for IoT deployments and GSMA predicts it will account for 53% of total global connections by 2025, up from just 29% in 2017[5]. Organizations must understand that **LTE is not a single technology** but a range of technologies that fall under the LTE umbrella. Different "categories" of LTE, as they are referred to, have been designed for specific purposes, with specific levels of performance, and specific device architecture requirements. The increased adoption of LTE for IoT is made possible by the release of new, **low-power (LPWAN) LTE technologies** that have been specifically created to support the rapid growth of IoT.

Designed to **replace legacy 2G and 3G cellular networks** for IoT, low-power (LPWAN) LTE technologies such as NB-IoT and LTE-M are lower power, lower bandwidth LTE variants that provide the longevity of traditional LTE categories (i.e. Category 1 or Cat-1, Category 4 or Cat-4) at a much lower cost, with much longer battery life, and much lower power consumption. Common benefits of IoT solutions deployed on LPWAN LTE networks include:

- Very low power consumption with some applications boasting a battery life of 10 or more years
- Low cellular module costs leading to low device unit costs
- Indoor and outdoor coverage in previously unreachable locations
- Scalable technology with ability to support large number of devices over a wide geographic area
- End-to-end secure connectivity and support for authentication appropriate to the IoT application
- Long-term network technology solution

In addition to the aforementioned licensed, low power LTE technologies, there are also a number of proprietary LPWAN network options that operate in **unlicensed spectrum** such as Sigfox and LoRa. When using licensed spectrum, operators must apply for and obtain a license from the FCC to own and operate spectrum in exchange for connectivity that is 99.999% interference-free. Unlicensed spectrum does not require any special permit or license to operate, but if multiple providers are operating in the same area, unlicensed connections may be subject to interference[6].

Prior to the emergence of NB-IoT and Cat-M1, unlicensed networks were the only LPWAN solution for new IoT solutions requiring lower power, longer range, and longer battery life. Although the market is shifting towards licensed network technologies, there are still certain geographies and use cases where unlicensed connectivity is an adequate solution. The superior choice for network connectivity is dependent on each business' unique requirements. Key elements and specifications for businesses to consider when selecting a network technology are as follows:

	LTE Cat 6	LTE Cat 4	LTE Cat 1	LTE Cat-M1	NB-IoT	Sigfox	LoRa
Bandwidth	40 MHz	20 MHz	20 MHz	1.4 MHz	200 kHz	100 Hz	125 kHz
Battery Life	Days	Days	5 years	5-10 years	10+ years	10+ years	10+ years
Throughput	DL: 300 Mbps UL: 50 Mbps	DL: 150 Mbps UL: 50 Mbps	DL: 10 Mbps UL: 5 Mbps	1 Mbps	250 kbps	100 bps	290bps - 50kbps
2-Way Data Tx	Full Duplex	Full Duplex	Full Duplex	Full or Half Duplex	Half Duplex	No	Class Dependent
Security	3GPP (128-256bit)	3GPP (128-256bit)	3GPP (128-256bit)	3GPP (128-256bit)	3GPP (128-256bit)	16 bit	32 bit
Scalability	High	High	High	High	High	Low	Medium
Mobility Support	Full	Full	Full	Connected & Idle mode	Idle mode	No	Yes
Location Support (LBS)	Yes	Yes	Yes	Needs GPS	Needs GPS	No	Yes
Voice Support	Yes	Yes	Yes	Yes	No	No	No
Module Cost	$50+	$40	$20-25	$10-20	$5-10	$2	$12
Common Use Case	Virtual Doctor Applications	WAN Primary, WAN Backup for Healthcare Clinics	Diabetes Management Applications	Personal Emergency Response (PERS)	Age-in-Place Applications		
Availability	**Future 2018**	**Now**	**Now**	**Now**	**2nd Half 2018**	**Now**	**Now**

IoT Device Selection

The IoT device is directly related to the underlying technology of an organization's IoT solution, as it must support the desired network technology, application, security requirements, etc. A key element in ensuring this happens is determining the proper device standard, as there are varying protocols available in the marketplace that are designed to support different functionalities. Device standards, for example, can range from MQTT, which is a simple messaging protocol designed for constrained devices with low bandwidth requirements on high-latency networks, to Lightweight M2M (LWM2M), which is a device management protocol designed for remote management of sensor networks, M2M devices, and related service enablement. Selecting the correct device standard will directly correlate to the device's ability to support desired applications and other technologies.

Once device standards are understood and selected, **businesses essentially have two options:** purchase an off-the-shelf device that meets your IoT solution requirements, or build a proprietary device from scratch. Although each option has distinct advantages, organizations must understand that the decision to build a custom device will be more time consuming. Resources will need to be dedicated to addressing a number of items ranging from module evaluation and selection, to industrial design, to mechanical engineering, to **device certification** – just to name a few.

Some key considerations when making a decision to build or buy include:

- Potential size and scale of the IoT solution deployment
- Availability of funds for upfront expenditure
- Importance of owning intellectual property
- Importance of brand fortification
- Speed-to-market requirements
- Availability of technical resources for engineering support
- Potential device certification requirements

Typically, building makes more sense for companies that are going to market as "IoT companies" and have a core competency in IoT technology. These types of businesses have the internal expertise needed to execute the build, and the value of bringing a unique device to market outweighs the possible challenges of delayed time-to-market or large financial investment.

On the flip side, buying typically makes more sense for companies that are using IoT solutions as "consumption" products that are not being offered downstream to end-users but are being implemented to improve internal operations or processes. These types of businesses generally do not have the internal resources required to design and build an IoT device from scratch, and therefore the upfront investment in off-the-shelf devices is worth it.

Regardless of the decision, it is most important for the selected device to support the application that will power an organization's IoT solution, as well as provide adequate levels of security based on the results of the IoT security assessment.

IoT Solution Lifecycle Management

Once an organization has evaluated and selected their technologies and has successfully designed, developed, and tested their IoT solution, it is critical to understand that the IoT project is not yet complete and the IoT solution will require ongoing deployment, operational management, as well as sustainment and support efforts to maximize ROI realization. There are a host of business processes that must be defined to ensure the entire IoT solution lifecycle is properly taken into consideration. This area of IoT solution implementation can be broken down into three sub-areas: deployment (also known as forward logistics), operational management, and sustainment and support (also known as reverse logistics). In order to efficiently get an IoT solution to market, maintain the health of the solution, and properly adapt to any IoT solution issues or updates, businesses must plan for these ongoing processes.

IoT Solution Deployment (Forward Logistics)

To avoid delayed time-to-market or unforeseen difficulties in transitioning an IoT solution from Proof-of-Concept (PoC) to production, organizations should consider the following critical disciplines:

IoT Solution Operational Management

Once an IoT solution has been launched, many organizations, especially those new to IoT, may not fully grasp the level of resources required to support the IoT deployment as it grows. To avoid future management and scalability issues, organizations should consider the following critical disciplines:

IoT Solution Sustainment and Support (Reverse Logistics)

Even the most successful IoT projects are prone to issues or failures that may be beyond the organization's control (i.e. **carrier network sunsets**) and require continuous adaptation and support to maintain a healthy implementation. To alleviate these challenges, organizations should consider the following critical disciplines:

Whether organizations choose to manage these processes internally or partner with an IoT provider to provide **IoT endpoint lifecycle management** services will all depend on the level of IoT expertise, speed-to-market schedules, and resource availability as dictated by the business' IoT strategy.

IoT Solution Optimization

Once an IoT solution has been implemented, organizations should be continuously monitoring the effectiveness of the deployment to understand the current value it is delivering, and to make the adjustments needed to derive greater, quicker value realization for downstream customers. Continuous monitoring and analyzation of network, device, and application performance provides the baseline information needed to prepare and prioritize IoT solution updates. For example – if a particular IoT device is experiencing slow network performance, organizations monitoring their networks will be enabled to better understand if the issue is the result of carrier outage or coverage, or if the issue lies within the device itself.

Organizations can also increase the effectiveness of their IoT solution(s) and create added value by leveraging the data collected via their IoT devices. A recent study estimates that the amount of data currently being processed in the digital universe could fill a stack of 128GB iPad Air devices that would reach a height of 158,000 miles – that is approximately two thirds of the way to the moon[7]. The data collected via IoT solutions is arguably the IoT's greatest differentiator, providing businesses with massive amounts of information that was previously unavailable.

By taking data analytics beyond the functionality of the IoT solution, organizations can leverage the data collected by IoT solutions to extract valuable business intelligence, **improve operational efficiencies**, or even **introduce new services** that are relevant or adjacent to current offerings. For example – a medical device manufacturer of MRI machines that has implemented an IoT solution to monitor and track device usage during testing can now extend the IoT solution to production models, enabling hospitals to pay for the machines in an OpEx "per image" model, as opposed to an expensive, upfront capital expense. This IoT data-enabled "as-a-Service" business model enables the manufacturer to penetrate new markets, catering to providers with smaller budgets. Another example might be an organization that has implemented an IoT-enabled fleet tracking application to simply track the location of a vehicle, but leverages IoT data analytics to monitor driver behavior, increase fuel efficiencies, and implement preventative maintenance practices.

Conclusion and Next Steps

The IoT ecosystem is highly complex, and each organization's journey to an impactful IoT solution implementation will be unique to their business processes and IoT goals. With that said, it must be understood that even the most experienced IoT companies should not attempt to "go it alone", as a recent survey from Cisco found that the most successful organizations engage their IoT partner ecosystems at every stage of IoT solution planning, development, deployment, and management. The right IoT partner should be a trusted advisor with deep IoT expertise and a technology-agnostic approach. By selecting a partner that provides solutions and services spanning the entire IoT implementation process (i.e. consultative services, IoT devices and/or device certification services, network connectivity, IoT endpoint lifecycle management services, etc.), businesses are enabled to alleviate risks, avoid common challenges, and benefit from a streamlined and simplified IoT solution.

About KORE

KORE is a pioneering leader and trusted advisor that helps deliver transformative business performance from IoT solutions. We help customer organizations of all sizes navigate the complexities of IoT and improve execution, so they can focus on operational and business results. Our IoT expertise and experience, global reach, independence, and deployment agility accelerate and materially improve our customers' return on their IoT investments.

Learn how KORE can simplify the complexity of IoT to ensure a successful IoT implementation.

Sources

1. https://newsroom.cisco.com/press-release-content?articleId=1847422
2. https://www.gartner.com/imagesrv/research/iot/pdf/iot-275309.pdf
3. https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881
4. https://www.statista.com/statistics/671216/global-m2m-and-nb-iot-connections-forecast/
5. https://www.gsma.com/mobileeconomy/#techmigration
6. https://blog.oneringnetworks.com/the-difference-between-licensed-v-unlicensed-spectrum-for-fixed-wireless
7. https://www.versatek.com/blog/how-much-data-will-the-internet-of-things-iot-generate-by-2020/
8. http://www.itpro.co.uk/internet-of-things-iot/31218/iot-revenue-opportunity-to-exceed-1-trillion-by-2025