KPMG

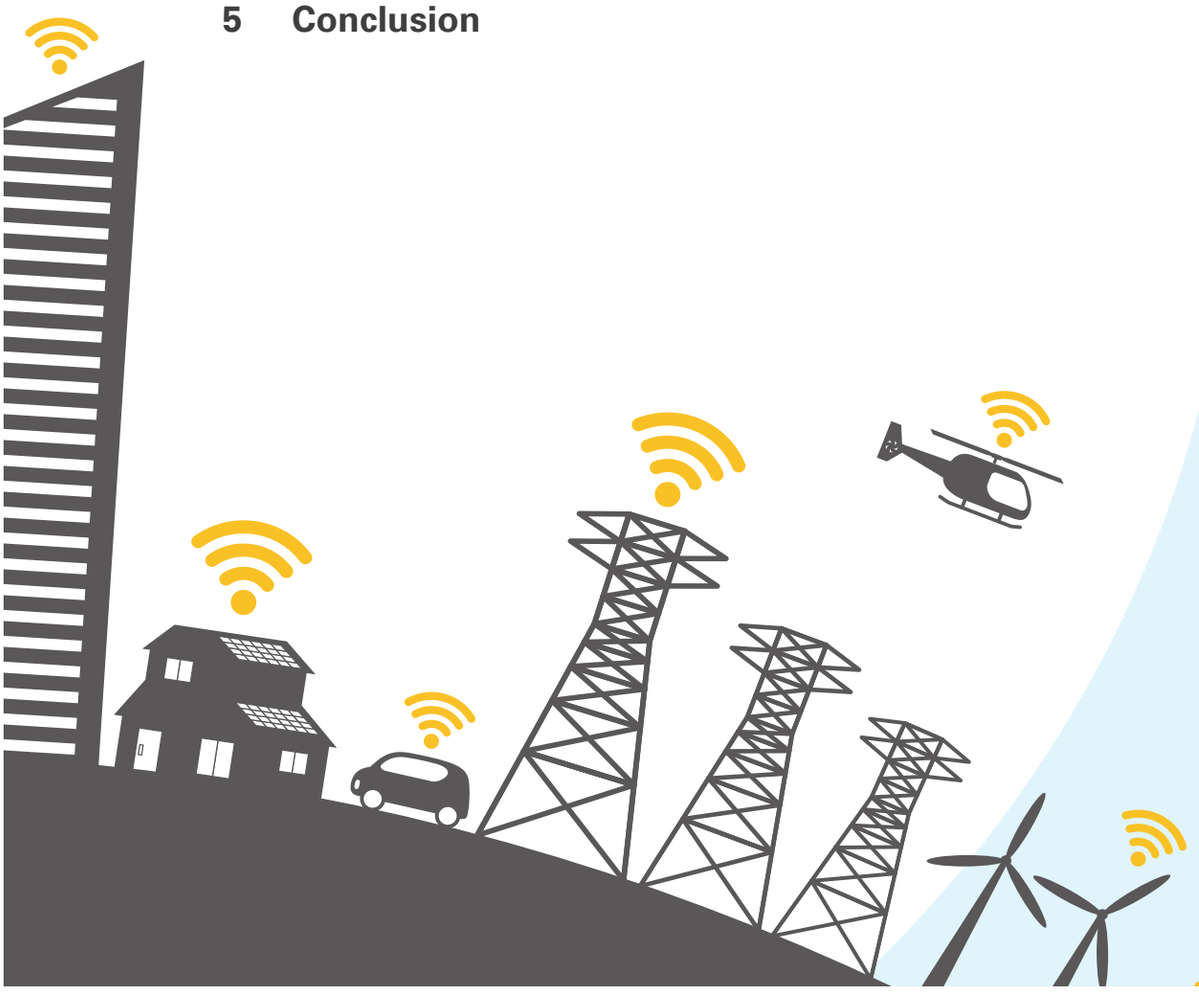
FICCI

Cybersecurity in smart cities

February 2019

kpmg.com/in

Table of contents



1 KPMG in India foreword

India is at the helm of an urban transformation with a population of almost 377.1 million[1] (~31.6 per cent) utilising urban infrastructure experiencing a wave of changes in the city services that they use. With a larger influx toward urban areas it is not only brownfield development but a large amount of greenfield urbanisation opening doors to the latest technology implementation and innovative solution interventions.

Smart City Technology has been a harbinger for ease of living, ease of governance and ease of community build up. This ease has been built into smart services through multiple junctures of process and technology which unfortunately also exposes these joints to possible misuse by miscreants. The focus in the last two to three years has been strongly on ease of digital adaption. With the growing data collected due to the digital influx, it is impertinent to step back and assess the inbuilt security in these solutions. The purpose is not only to ensure no breach of security at any level of the city service but also measures to bounce back with corrective measures in case of any mishap.

There are multiple loci for cyberattacks today due to the nature of city services layers. Earlier security of data stored in servers was paramount. However with the rise of IoT to serve city services, the focus of security is now multi folded to devices, connectivity and inter application sharing apart from data stores. This is compounded by the challenge of variety of data accumulating in huge volumes at immense velocity. This task of secure safe services can be achieved only through synergised stakeholder efforts right from Users of Services like citizens and officials, Governance bodies like the SPVs, Project managers and Implementers like the system integrators and product Original Equipment Manufacturer (OEM). The solution hence has to be a multi-pronged approach by building stringent standards without inhibiting innovation, thought through policies, transparent governance mechanisms and capacity building to avert attacks as well as recoup and harden against any outliers. This report aims at generating awareness of the challenge that lies ahead of us and the means of overcoming it.

1. Source: Website of Ministry of Housing and Urban Affairs, Government of India Urban Population : http://mohua.gov.in/cms/urban-growth.php

Ramendra Verma
Partner and Head,
Government Advisory
KPMG in India

Smart Cities is the next big digital transformation that the country is going through and to ensure that the desired benefits are provided to citizens, it's imperative to establish a cybersafe, secure and trusted environment.

Internet of Things (IoT) and smart devices are at the epicenter of establishing a smart environment, and it presents great opportunities for smart cities and innovative technology to lead the way. However, success in implementing and sustaining smart cities will take more than slick applications, connected de vices and advanced analytics; it will also require a robust approach to security, privacy and trust.

This document deliberates upon the potential challenges that key stakeholders and government agencies need to ensure are factored in while establishing smart cities to provide a safe and secure environment. The document also highlights the salient aspects of these risks which by the nature tend to be dynamic and ever changing, leading it to be a continuous process and not just a one time change.

We aim to catalyse the thoughts to have a robust cyber framework and have proposed an initial framework factoring in the stakeholders along with various components and the external actors.

Atul Gupta
Partner and Head,
IT Advisory, Cyber Security - Leader
KPMG in India

1 FICCI foreword

I am happy to share with you the FICCI-KPMG report on 'Cyber Security in Smart Cities' to be released at the Urban Innovations and Future Cities Meet - Smart Cities Summit 2019 organised by Federation of Indian Chambers of Commerce and Industry.

The summit is structured to explore the disruptive technological interventions that the cities can choose to adopt in each sector of urban infrastructure and housing. The conference has also been structured to provide the much-needed platform to promote the start-up ecosystem in India.

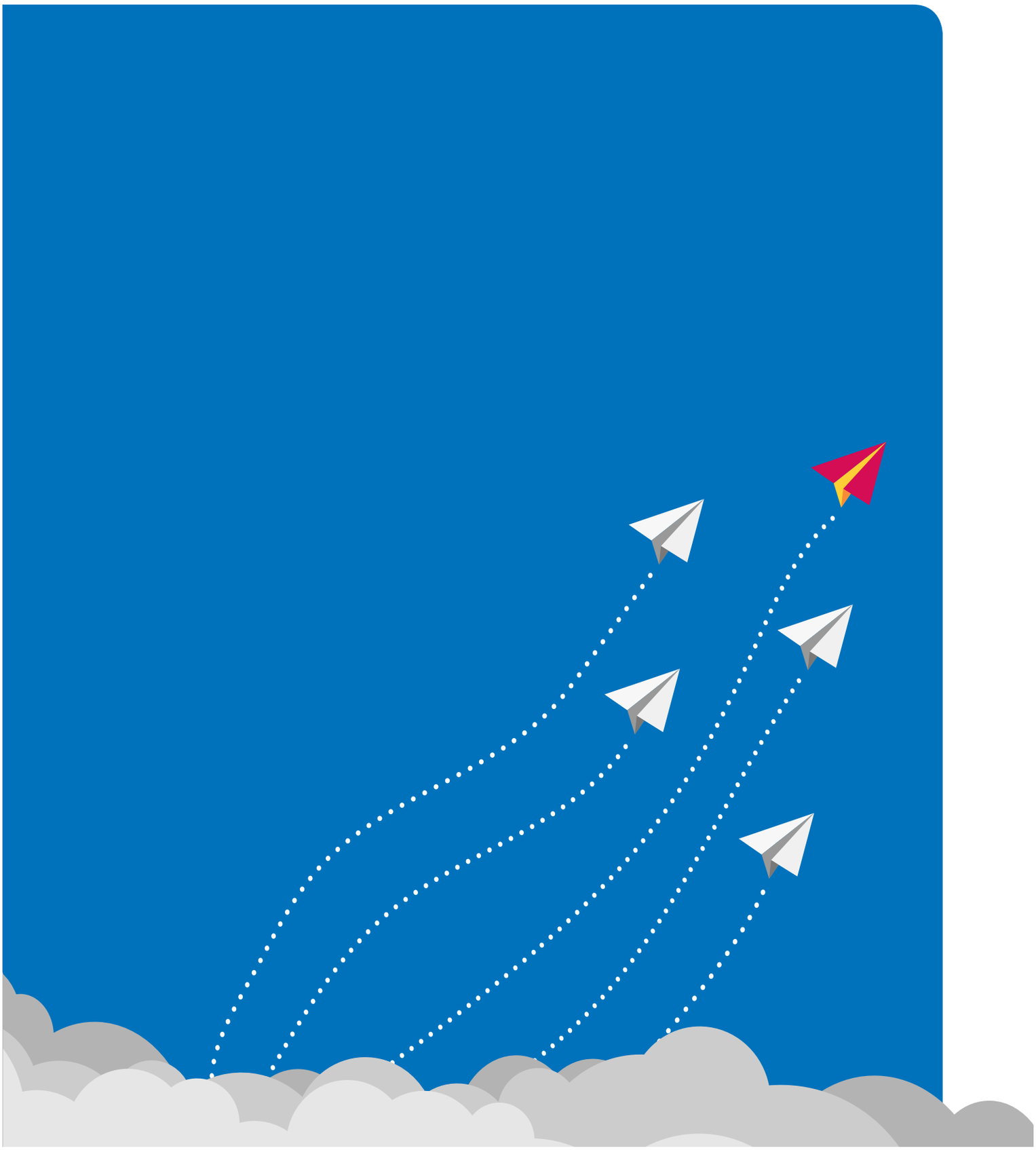
The 100 Smart Cities Mission (SCM) is one of the landmark urban initiatives by the Government of India where 100 cities have been shortlisted to be developed as "Smart Cities" across all the states and union territories, primarily through upgrading their urban infrastructure and upscaling their municipal services through effective technological interface. As a growing number of cities has begun their urban transformation, there is emerging trend of using human-centric and cloud-based technologies to automate and integrate urban services. Such technologies are resulting in significant data generation which can be further used to effective urban development.

The FICCI-KPMG report highlights the evolving trends in Smart Cities resulting in integrated device ecosystem, the data convergence and the readiness of the demand and supply side.

The report evaluates the current urban practices and emphasises the existing guidelines that may need to be relooked while designing solutions. The report also includes recommendations from policy to design to implementation to monitoring of urban projects under a standard framework.

We hope you will find this report useful.
Your suggestions and feedback are welcome.

Ajay Pandey
Chairman – FICCI Urban Infra and Smart Cities Committee, FICCI and Managing Director and CEO, Gift City



2 Smart cities

2.1 Need for smart cities

Modern day urbanisation has moved far ahead from a planned settlement to an intelligent connected settlement responsible for not only ease of living but also creating happy communities capable of leading a safe, secure life on the pillars of economic vitality and futuristic sustenance. Hence, the need of making our cities smarter and more livable is increasingly seen as a vital way to improve their competitiveness and resilience in today's resource constrained world. Local governments are at the centre of this challenge – delivering new and better services while also facing population change, economic disruption, decreasing revenues and fast-changing citizen expectations[1].

As part of this need to cater to nearly 99.6 million urban population, a total of 100 Municipalities in India are developing their Smart City Initiatives[2] to enable their overarching strategy and meet their operational and community challenges.

The reasons to develop a sustainable urban state are numerous due to the challenges[3] that the bulging population and limited resources present[4].

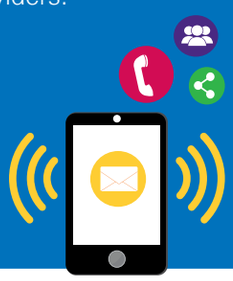
Urbanisation has a fluctuating impact on urban economy, life quality, time cost and sustainable development. The speed of urbanisation and population growth bring increasingly severe challenges to urban managers around the world.

Population

- India's total population is close to 1.21 billion (as census 2011).
- Urban population reached about 377.1 million (~31.6 per cent).

Communication

- The escalation in demand for communication has posed challenges to the construction of urban network infrastructure and the network operation and maintenance capacity of providers.



Transportation

- Urban traffic congestion has led to high time cost.
- The average travel speed across the 154 cities studied indicates that the average speed in Indian cities is 24.4 km/hr. (as WB Report).
- On average, travelers in Delhi, Mumbai, Bengaluru, and Kolkata spend 1.5 hours more on their daily commutes than their counterparts in other Asian cities during peak traffic times.
- Among foreign cities, the average commute time in New York is also over 30 minutes.

Healthcare

- Over 60 per cent death caused by Non-communicable in India (as WB report).
- Over 70 per cent expenditure on healthcare goes from patient's pocket. The rest is probably paid by Government or Insurance companies.
- Nearly 1.7 million Indian's death caused by heart diseases every year. (as WB report).

Education

- The need to align network, training institutions and education resources.
- Lack of Quality of education due to limited learning resources for teachers.

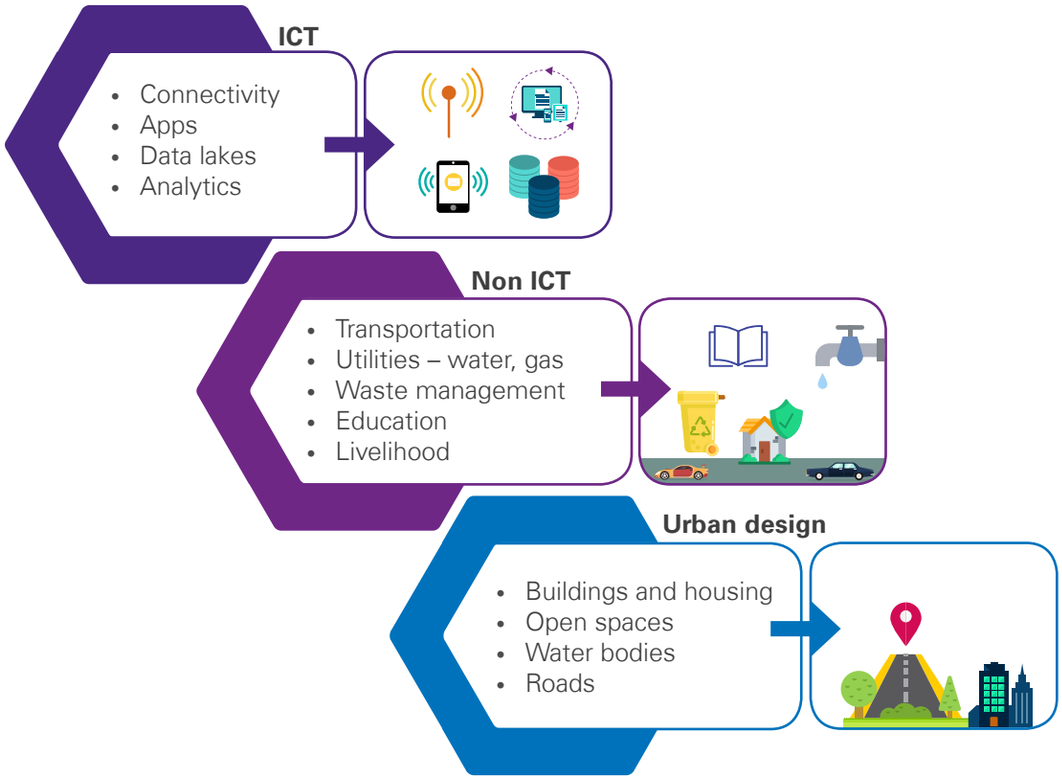
1. Source: KPMG Australia Report Mar 2018 - The Smart City Data Challenge.
2. Source: Website of Smart City Mission, Ministry of Housing and Urban Affairs, Government of India - http://smartcities.gov.in/content/
3. Source: A report on "Traffic jams in just four Indian cities cost $22 billion a year" at www.qz.com.
4. Source: A report of Indian Council of Medical Research "News Update 21 TO 28 September" https://www.icmr.nic.in/sites/default/files/ICMR-NEWS-UPDATE-21-28-September.pdf

The sheer vastness of urbanisation challenges makes it essential that proactive measures that are smart in nature be taken up to ensure a healthy and evolving society. With local bodies grappling with large scale urbanisation challenges, it is imperative to derive a model that is evolving and sustainable utilising technology as backbone to support and innovate changing needs. Hence the rise of the so called 'Smart Cities'.

2.2 The embodiment of smart cities

Smart Cities today is a model that has augmented civil infrastructure with a digital arm converting city assets into services with a view to improve urban living standards and reduce the environmental impact of growing populations. As the world moves from an era of traditional infrastructure to smart infrastructure there is a build up of synergy and innovation between ICT, Non-ICT and Urban initiatives.

Smart city model



The model of a smart city has to ensure a build up of city infrastructure that allows a resilient architecture. This can be articulated as the 4M needs of a Smart City

- Mobilised
- Monitored
- Managed
- Measured.

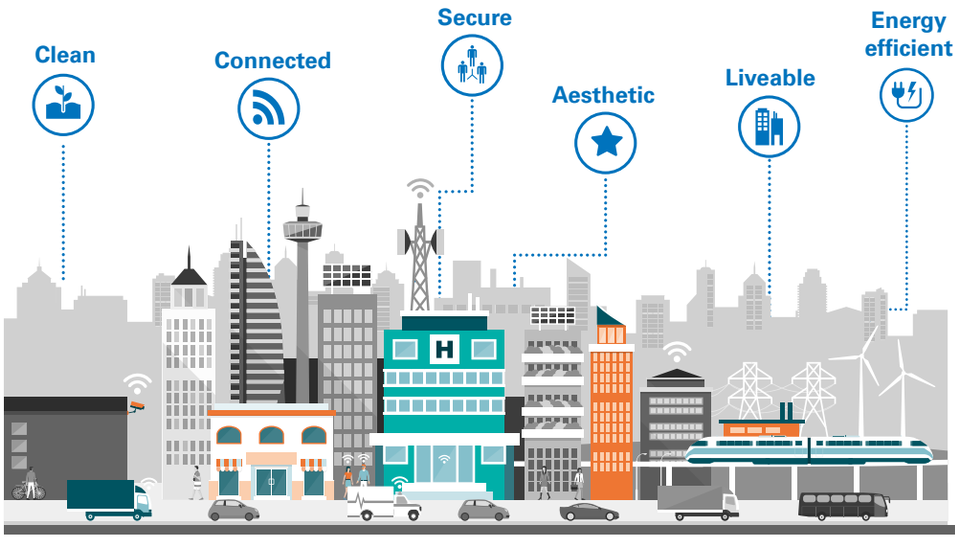
What do Smart cities embody

Smart cities represent civil infrastructure augmented with a digital arm churning humongous amount of data that can be utilised in a safe and secure mechanism for smartness maturity

Properties of Smart city

- Create a smart sustainable urban structure
- Implement smart solutions over traditional infrastructure
- Introduce efficient city management

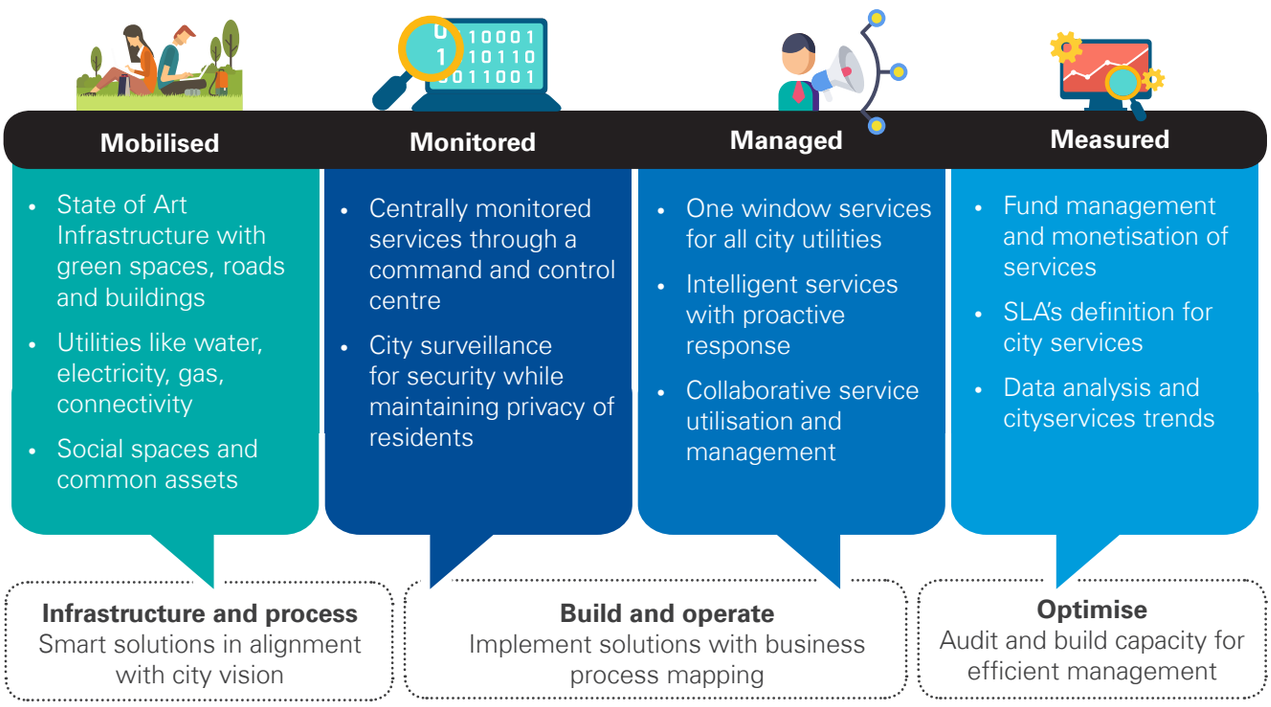
4 M's of Smart city denotation



1. Mobilised
2. Monitored
3. Managed
4. Measured.

The 4M concept details the steps that a smart city needs to take, to ensure that the city is progressive towards building a smart infrastructure.
The smartness of a city has to be directed towards creating the necessary parameters of livability during its complete lifecycle.

Smart city features and services



The city vision must capture the identity of the city and play a major role in mobilising the need and planning of city needs. The solutions that need to be mobilised have to be in synch with the demands of various stakeholders like citizens, governance bodies, implementers and operations support.

A well planned city requires the services to be monitored to ensure security, transparency and ability to react to known and unknown events. Services require checks and balances to ensure fair usage and productive utilisation.

Governance is the core of city management and is enabled further in a smart city through smarter solutions and aids to ensure smooth flow of processes. A managed city ensures a synergistic approach to improve livability.

Finally the evolution and improvements in urban lifestyle is determined through the process of measurement of outcomes of city smartness. The means to improve and innovate evolves out of quantifiable and measurable KPIs governing a city.

2.3 Epicenter of smartness in cities – Data

The realm of a Smart City today is an interconnected mesh of social, community and personal lives brought together by intelligent means powered by innovative technology that could be devices, data processing or simply connectivity. The need and availability of technology to ease the utilisation of civic amenities as digital services has created a new challenge to harness and build upon – Data.

Data today is being collected in great Volumes, Variety and Velocity from various smart city services. This data which is a monetisable asset needs safe and secure handling to ensure that it is rightly used and shared for effective governance and not compromised. It is thus critical to understand the threats and challenges to secure data at all levels starting from the source of generation, to motion of data, to storage of data and finally sharing of data for effective use.

> ***Security of Data collected in huge Volumes, Variety and Velocity is imperative for confidence in utilisation of smart city services***

3 Cybersecurity for smart cities

3.1 Building technology-centric smart solutions

India has embarked on the journey of building 100+ smart cities that aims to have nearly 40 per cent of India's population and contribute to 75 per cent of India's GDP by 2030[1]. These smart cities will be driven by smart solutions powered by state of the art technologies. Some of the smart solutions include:

E-governance and Citizen Services, such as

- Citizen engagement, public information and grievance management
- Electronic service delivery
- Surveillance, monitoring and crime control

Smart urban mobility

- Intelligent and integrated traffic management systems
- Smart parking
- Intelligent and integrated multi-modal transportation systems

Smart waste management

- Waste recycling, reduction and re-use through conversion to energy, fuel and compost

Smart healthcare

- Smart patient health management and healthcare services
- Data based public health intercessions and infectious disease surveillance, care search and scheduling
- Remote patient monitoring and telemedicine

Smart water management

- Monitoring water sources and water distribution systems for optimising water resource usage, ensuring water quality and minimising leakages

Smart trade and economy facilitation centers

- Digital business licensing and permits
- Digital land use, building registration and permits

Smart energy management

- Smart metering, smart grids and management of power
- Smart and efficient channelising of renewable energy
- Energy efficient and green buildings

Smart skill development centers

- Personalised education and online training programs
- e-career portals

1. Source: Smart Cities Mission Statement & Guidelines, Ministry of Urban Development, Govt. of Indiainsurance contracts leadership team , KPMG International Standards Group, July 2017

Smart cites in India

Smart energy management
Advanced Metering Infrastructure (AMI) with two way communication and meter data management system

Smart healthcare
Remote patient monitoring and telemedicine

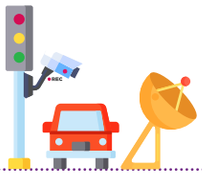
Smart trade and economy facilitation
Online portal for issuing digital license to businesses

Smart skills development center
Online portal to impart job oriented training programs

Smart waste management
RFID tracking of vehicles bio-methanation, waste to-energy decentralisation waste processing

E-governance and citizen services
Smart apps based citizens engagement, public information and grievance management and electronic service delivery

Smart urban mobility
Covering dynamic signal synchronisation, Automatic Number Plate Recognition (ANPR) cameras, license plate recognition camera, red light violation detection system and radar based speeding detector built on the surveillance camera network



Smart surveillance:
surveillance network consisting of CCTV, fixed box and mobile transport cameras at different locations, to capture high resolution read-time images with facilities for wireless and wire connectivity download

Smart water management
SCADA, 'smart metering,' advanced leaked detection, online quality monitoring

These smart solutions are powered by combination of heterogeneous enabling technologies such as Ubiquitous Network Connectivity, Sensor Networks, Smart Cards, IoT-based devices / wearable devices (using narrowband or long range, lower power wireless communication technology), autonomous systems at physical device level, integrated with intelligent mobile apps, cloud computing, open data and advanced analytics powered by new age AI solutions. These enabling technologies reduce the cost of gathering information for structured analysis. With large volume of useful data analysed into structured data patterns, the city councils, governments and the residents of smart cities can collectively work to channelise and optimise existing infrastructure and resources.

3.2 Cybersecurity – A necessity

IoT provides significant advantages, but it comes along with associated cyber risks. As the government gets more and more familiar with the benefits that IoT can deliver – specifically for smart cities – key concerns around security, privacy and trust are likely to grow[2]. A comprehensive understanding about the cybersecurity threats that these technology brings is being still worked upon, but its rapid adoption is exposing potential security breaches.

2. Source: KPMG TL - "Security and the IoT Ecosystem"

> ***IoT-based devices provide significant opportunities and it is imperative to have them operate in a secure environment to realise all the benefits***

Smart cities are facing a deluge of cyber-attacks affecting availability of smart city infrastructure, continuity of services and misuse of personal data / privacy. Some recent attacks include[3]:

23/12/2015 – Ukraine Power Grid
Attackers compromised three energy distribution companies systems, affecting 30 substationsand leaving 230,000 people without electricity.

16/03/2016 - Kemuri Water Company
Attackers changed the levels of chemicals used to treat water, and the data of 2.5 million utility customers was compromised.

25/11/2016 - San Francisco Municipal Railway
Ransomware attack on systems.

7/10/2017 - Dallas
Attackers activated 156 emergency sirens around midnight, leading to public chaos and thousand of calls to 911 helpline.

11/10/2017 - Sweden Transport Administration Systems
Distributed Denial of Service (DDoS) affected system to monitor trains, road traffic leading to traffic chaos and delays.

18/11/2017 - Scaramento Regional Transit Systems
Ransomware attack deleted 30 million files.

22/03/2018 - Atlanta Municipal Systems
Ransomware attack on city systems, leading to outage across various city systems.

01/07/2018 - Department of Homeland Security, US
Russian hackers compromised the networks of multiple U.S. electric utilities and put attackers in a position where they could have caused blackouts.

3. Source: Forbes tech council – listing of cyberattacks; and CCIS report on Significant Cyber Incidents since 2006

These cyber-attacks have highlighted the pervasive impact to entire smart city ecosystem and have underpinned the requirement of having robust cybersecurity setup.

There are multiple reasons attributed to these attacks, and some of the key factors include:

a. Inadequate security governance structures to provide strategic inputs and directions for managing security transformation programmes for such large smart city initiatives and ensuring stakeholder commitment to cybersecurity requirements.

b. Inadequate security requirements planning and implementation of technology and network architecture of smart city solutions, leading to attackers being able to exploit system design vulnerabilities, implant malware and carry out attacks (DoS, data exfiltration, etc).

c. Increased attack surface due to lack of standardisation on security standards across smart/ connected devices. Most of the communication protocols for capturing and relaying data is not secured and the sensor layer remains insecure to data snooping, sniffing and man in the middle attacks.

d. Inadequate and infrequent security assessment and testing of devices, network, applications (mobile / web) and data exchange interfaces for identification and remediation of security vulnerabilities. Additional complexity and difficulty in security patch deployment on heterogeneous devices and legacy systems.

e. Lack of identification of crown jewels and sensitive personal data within the smart city ecosystem that requires additional security safeguards for ensuring adequate security is provided to sensitive data.

f. Security monitoring controls are unable to cover all smart devices and have adequate use case scenarios for monitoring the security events / incidents across devices, network and applications within the Smart City ecosystem.

g. Inadequate cyber incident response capability to detect and respond to cyber-attacks and minimise potential impact.

3.3 Cybersecurity – Key Components

There is need to ensure that the challenges which the IoT devices and other smart technology brings upon, is adequately addressed. Following are the key components which need to be addressed upon:

- Establishing minimum baseline for security standards
- Establishing Security, Privacy and Trust in ecosystem
- Driving cybersecurity across Smart Cities value chain

3.3.1 Need for Standards

Given the pervasiveness of IoT and the sensitivity of the systems and data, there is a clear need for IoT regulations and standards[4]. However, there are concerns about the speed to market at which IoT-based solutions are being released and standards are being established.

> ***Development of industry standards will be an important step to driving IoT adoption in smart cities. Indeed, it is often not until generally accepted standards are set that most new innovations truly achieve mainstream adoption.***

4. Source: KPMG TL - "Security and the IoT Ecosystem"

Given this context, it's imperative for smart cities, regulators and other stakeholders to come together and establish minimum baseline standards for security.

The Hypercat consortium in the United Kingdom is a great example of technology companies, government and business coming together to develop standards for the application of IoT in Smart Cities space[5]. The Hypercat consortium supports adoption of IoT technologies for smart solutions by:

- Developing a new standard for secure IoT interoperability.
- Enabling IoT devices to securely connect over web.
- Providing assistance to innovators to apply ideas / use cases into global businesses.

Establishing minimum baselines standards will go long way in addressing the need of having safe and trusted environment. Some of the key areas where these standards need to be available should include – authentication and authorisation, cryptography, auditing and alerting, patching and updates, security configurations and having no backdoors, and security by design.

3.3.2 Security privacy and trust in ecosystem

The solution ecosystems deployed in smart cities need to address three key concepts that enable valuable user experience: security, privacy and trust.

- Security – This is an ever evolving risk and with the complex ecosystem required in smart cities the challenge on having adequate security increases multi-fold. In order to deliver a safer and more secure environment, it's key to adopt a 'Security by design' approach while deploying the various technology components[5].
- Privacy – Smart cities shall capture large volume of data which is specific to residents/ citizens and the value of this data is immense in today's digital world. This brings upon a key element to ensure that the privacy of data is maintained adequately, which is not only limited to having confidentiality, but also having granular data access controls. Unlike security, privacy is difficult to 'embed' into a solution or product and needs to be appropriately designed.
- Privacy isn't just about protection of individual / user data, it's also about how individuals / users allocate rights to their data and how that information is shared and used among the large ecosystem established in the smart city.
- Consequently, it's imperative to have "Privacy by Design" supported with a robust framework to ensure that adequate privacy measures are built in smart cities.
- Trust – this is an area that has been least frequently debated upon. This implies establishing an 'ecosystem' which enables stakeholders to have adequate trust and integrity across the inherent technology that fuels the smart cities. This will be critical in adoption and enhancement of value being provided through incremental use case scenarios for implementation in Smart Cities[5].

5. Source: KPMG TL - "Security and the IoT Ecosystem"

> ***Stakeholders and individuals in smart cities should always understand what technology is being utilised, what data is being captured, where it is being stored, who has access to it and what mechanisms are in place to protect it***

> ***Trust requires secure design such that there is adequate protection of ecosystem devices, communication channels and infrastructure that underpin the smart cities – but also addressing regulatory needs, policy compliances, ensuring data privacy and building trust with users and stakeholders***

3.3.3 Driving Cybersecurity across the value chain

Success in establishing Cybersecure Smart Cities will require the stakeholders to establish a sustainable value chain and the enabling ecosystem to be secure.

Smart cities will see multiple service providers and third party suppliers getting embedded in the value chain and it will be pivotal to ensure that all these entities need to demonstrate security capabilities. The value chain will constantly grow and shall not be limited to device manufacturers to infrastructure service providers, to telco companies or data warehousing facilities[6].

The suppliers will be required to gain accreditation or submit to audits and assurance examinations. Thus building Cyber Assurance and Cyber Resilience into the ecosystem will be critical in building the overall 'Cyber Confidence' and 'Trust' in smart cities.

> ***Smart cities need to ensure they are looking at entire value chain and not only at individual components – security is only as strong as the weakest link***

6. Source: KPMG TL - "Security and the IoT Ecosystem"

4 Frameworks to establish cybersecurity

4.1 Cybersecurity standards and practices by global knowledge bodies

Cybersecurity has been a major focus across multiple knowledge bodies in the world. There have been concerted efforts by knowledge bodies to enhance the existing cybersecurity standards and bring consistency in security practices. Considering the shortage of specialist cybersecurity skills in managing, implementing, assessing and governing security technologies and controls, the standardisation of security practices and abundant guidance from knowledge bodies significantly reduces the risks of oversight while implementing security controls and processes.

There are multiple global security standards that are relevant in context of underlying technologies used in smart cities:

- NIST[1]: National Institute of Standards and Technology (NIST) had launched Global City Teams Challenge (GCTC) Program for collaboration and the development of standards in the smart city sector. Alongside, they have introduced an international technical working group IOT-Enabled Smart City Framework. The framework provides a simple-to-use analytical tool for early investigation of smart city applications. NIST has also developed a framework for Cyber Physical Systems. The Framework provides a taxonomy and organisation of analysis that allow the complex process of studying, designing, and evolving CPS to be orderly and sufficiently encompassing.
    - ISO: ISO has defined a number of standards to provide cities with an overall framework for defining what "being smart" means for them and how they can get there. These include:
    - ISO 37100, Sustainable cities and communities – Vocabulary
    - ISO 37120, Sustainable development in communities – Indicators for city services and quality of life
    - ISO 26000, Guidance on social responsibility
    - ISO 17742, Energy efficiency and savings calculation for countries, regions and cities
    - ISO 39001, Road traffic safety (RTS) management systems
    - ISO 39002 (under development), Good practices for implementing commuting safety management
    - ISO 24510, Activities relating to drinking water and wastewater services
    - ISO/IEC 30182, Smart city concept model-Guidance for establishing a model for data interoperability
    - ISO/IEC 21972, Information technology – An upper level ontology for smart city indicators
    - ISO/IEC 27550, Information technology – Security techniques – Privacy engineering
    - ISO/IEC 27551, Information technology – Security techniques – Requirements for attribute-based unlinkable entity authentication
    - ISO/TS 37151, Smart community infrastructures – Principles and requirements for performance metrics.
    - ISO/TR 37152, Smart community infrastructures – Common framework for development and operation.
- In the Indian context, The Ministry of Housing and Urban Affairs (MoHUA) has already taken initiatives in terms of creating the cybersecurity model framework for smart cities.

Also, Ministry of Science and Technology has formulated the National Data Sharing and Accessibility Policy (NDSAP) which calls for proactive sharing of data by different government agencies, both at the national and sub-national levels, in standardised human and machine-readable formats.

In 2018, India took a step towards Data Protection through its Personal Data Protection Bill that includes obligations like transparency, record keeping, appointing a data protection officer and timely notifications of the breaches.

1. Source: NIST (www.nist.gov or https://pages.nist.gov/GCTC). This is a program run by NIST.

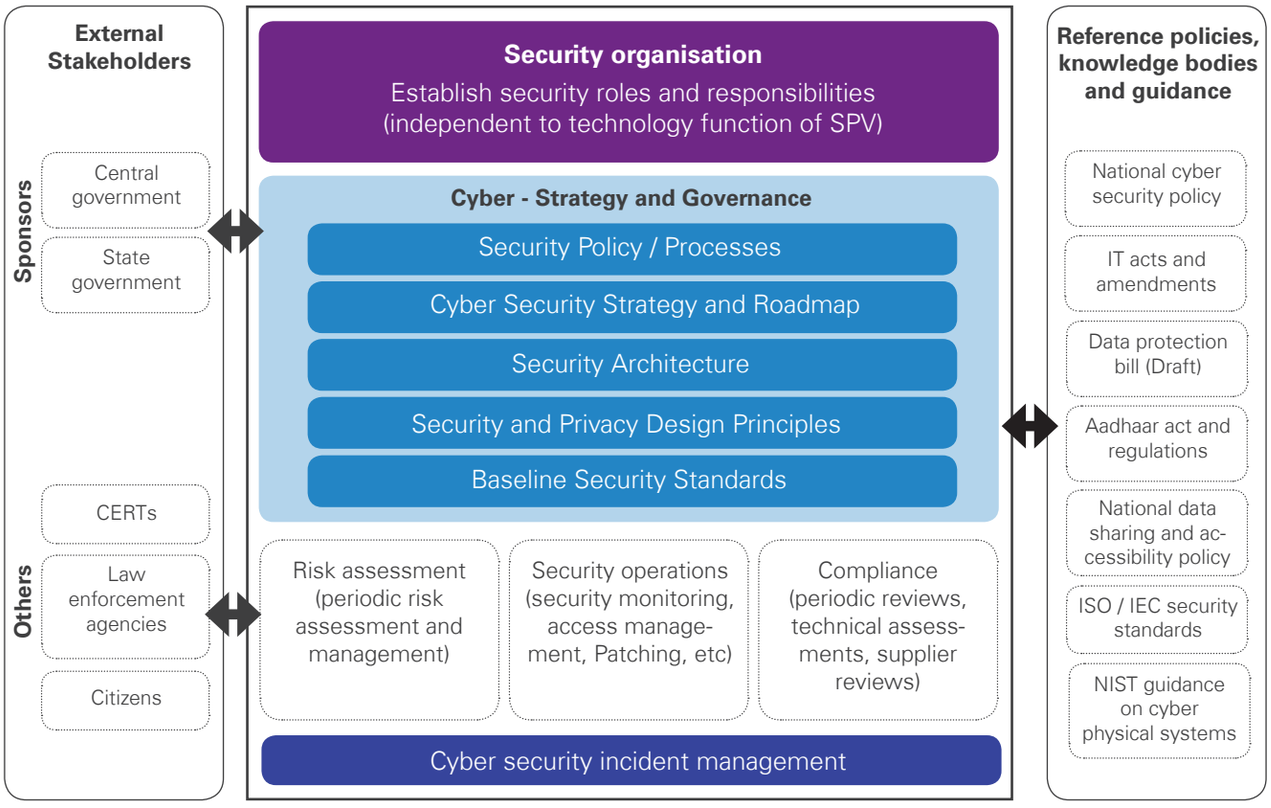
4.2 Framework from the India context

The Ministry of Housing and Urban Affairs (MoHUA) has created Smart City Special Purpose Vehicle (SPV) to plan, implement, manage, operate, monitor and evaluate the Smart City development projects.

It is imperative that SPVs may consider establishing an effective governance mechanism for protection of smart city infrastructure to manage the cyber risks. The problems of cybersecurity governance are unique and evolving and they cannot be dealt with traditional approach.

For establishing secure and resilient smart cities, a standardised cybersecurity framework comprising of the following can be adopted:

Smart city cyber security framework



A robust cybersecurity framework requires collaboration across all the key stakeholders yet maintaining independence

Recommendations for SPV:

- Formalise a cyber-security governance structure with well-defined roles and responsibilities of cybersecurity team and third party security services organisation supporting smart city infrastructure and security operations.
- Establish clear reporting relationships for monitoring security performance KPI's.
- Define a comprehensive cybersecurity policy and processes to govern and manage IT and OT security ecosystem within smart cities.
- Formalise cyber-security strategy and identify security initiatives that need to be implemented for smart cities. Prioritise the initiatives to address critical cyber risks.
- Adopt 'Security and Privacy by Design' principle where the security concepts are built into hardware and software from the developmental stages to the "end of life."
- Create a 'Defense in Depth' approach for designing and implementing security solution architecture. This should lead to a succession of barriers that an intruder must overcome to gain access to systems and increases the cost/ effort to carry out cyberattacks.
- Establish baseline security controls and standards for implementing and operating smart city solutions.
- Periodically perform cyber risk assessment and comprehensive cybersecurity reviews of smart city assets and underlying critical technology infrastructure to assess and align cybersecurity posture. As new smart technology are introduced across the cities, there will be emergence of new cyberthreats and attacks, targeted towards various stakeholders of a smart city. Therefore, there will be need to periodically educate stakeholders on the security measures that are required to be followed.
- Establish cyber security review plan covering entire smart city ecosystem (covering people, process, technology, third parties, etc.) and conduct periodic cybersecurity audits and reviews to ensure compliance to cybersecurity policies and regulatory requirements.
- Evaluate and deploy adequate behaviour based automated security operation control system that can assist in handling and mitigating real-time security threats. Implement cyber analytics systems (leveraging the power of machine learning, artificial intelligence, data visualisation and automation controls) to detect, prevent and respond to advanced cyber-attacks.
- Establish a cyber-incident response structure and a specialised security incident response team. The team needs to be adept at performing appropriate countermeasures in case of attacks or service recovery in case of system failures. An automated cyber incident response can enable SPV to investigate and orchestrate action across different security products, to remediate a cyber-threat.

5 Conclusion

As we continue to seek technology-centric smart solutions for smart cities, there is a need to realise that these solutions would have their own set of security limitations. Thus, smart cities might become attractive targets for large scale cybersecurity attacks that will have a pervasive impact on the entire smart city ecosystem and the residents of smart cities.

It is critical for smart cities to keep pace with the cybersecurity needs and build a cyber-resilient and trusted environment across the entire value chain.

Based on the analysis provided in this report, the key measures to be established may include:

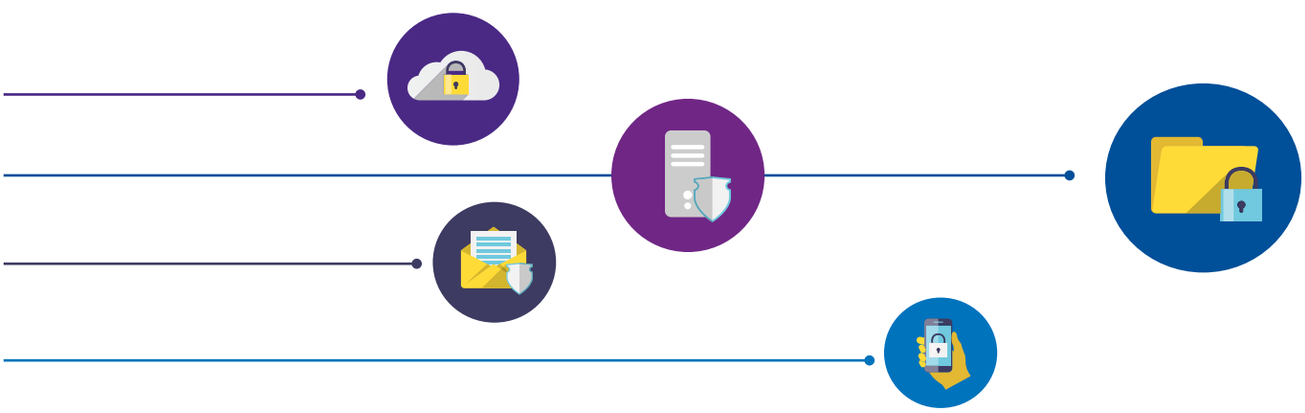
1. **Establishing a formal cybersecurity framework:** A formal guidance based on a well-defined cybersecurity policy and a structured security organisation with clearly defined roles and responsibilities will be really important for governing the cybersecurity posture and reducing the cyber risks.

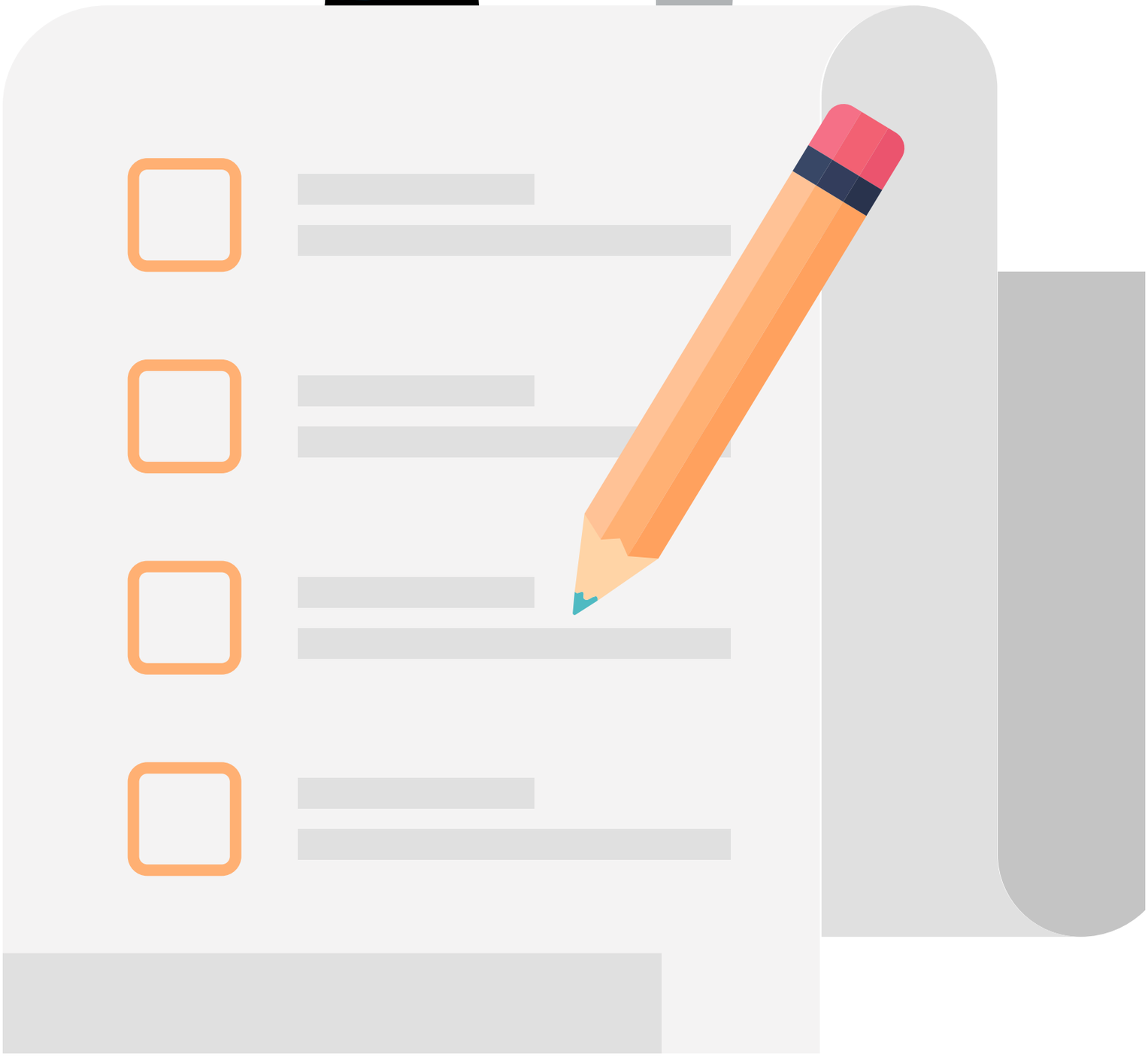
2. **Security must be built-in from the ground up:** Stakeholders and users in smart cities ecosystem will expect security to be built into the system; technology architects should follow an 'always-on' principle that provides high levels of control with appropriate fail-safes.

3. **Security should be deployed in integrated form across value chain:** Smart cities should carefully evaluate their third party suppliers, identify qualified partners, and invest in integrating security, privacy and trust across the ecosystem.

4. **Establish cyber resilient and trusted environment:** Resilience and trust will be established through validation of cyber practices, ensuring compliance and consistent engagement with smart city stakeholders and citizens. This will enhance cyber confidence of citizens and stakeholders on smart city functioning.

5. **Engage across industry, knowledge bodies and regulatory groups to standardise security measures:** Collaboration will reduce ambiguity and accelerate the ability to implement secure products and services within sustainable smart cities ecosystem.





KPMG in India contacts:

Nilaya Varma
Partner and Leader,
Markets Enablement
T: +91 124 669 1000
E: nilaya@kpmg.com

Ramendra Verma
Partner and Head,
Government Advisory
T: 91 120 3868703
E: ramendra@kpmg.com

Atul Gupta
Partner and Head,
IT Advisory, Cyber Security - Leader
T: +91 124 307 4134
E: atulgupta@kpmg.com

FICCI contact:

Neerja Singh
Director and Head - Infrastructure,
FICCI
T: +91-11-2348 7326
E: Neerja.singh@ficci.com

#KPMG josh

Follow us on:
kpmg.com/in/socialmedia

Printed in India. (059THL_0219)