




**Deloitte.**

December 2023

# Orchestrating trusted and cyber-secure smart ecosystems

**What benefits - and risks - do hyper-connected  
smart ecosystems pose for our cities?**

# Contents

 Click on each content section to navigate the document.

**1** Smart ecosystems are massive and complex **03**

**2** A smart ecosystem can include any integrated environment with digitally connected infrastructure **04**

**3** As digital and physical infrastructure converge, smart ecosystems become more vulnerable **06**

**4** Smart ecosystems face complexity due to three key factors **07**

**5** Examples of cyberattacks on smart ecosystems **08**

**6** Complexities differ based on the age and digital maturity level of the smart ecosystem **09**

**7** A “cyber-first” approach increases safety and resiliency across the smart ecosystem **11**

**8** About the Authors **17**

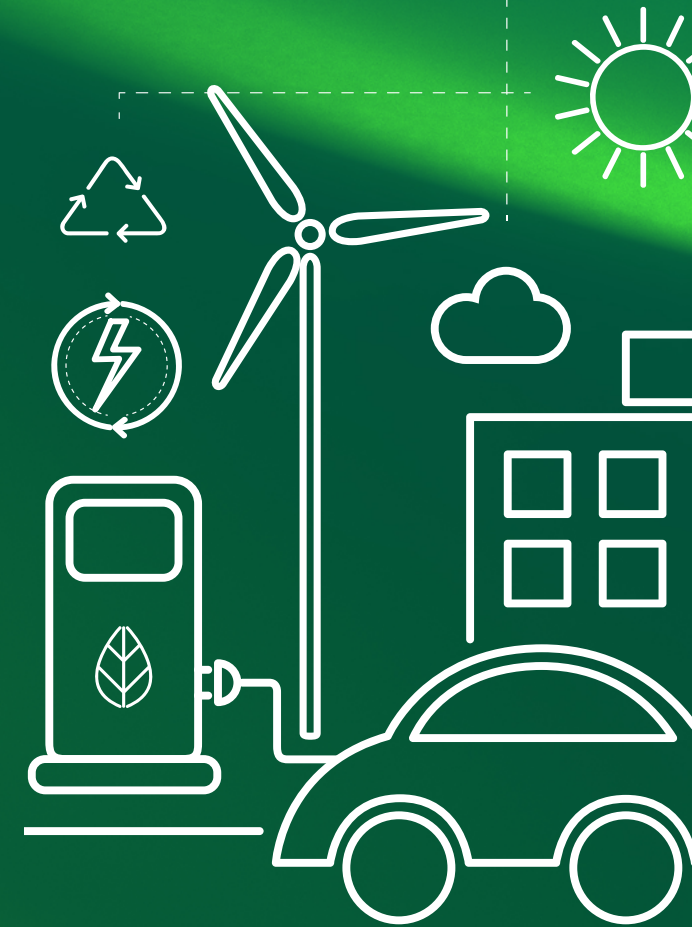
**9** Endnotes **18**

For the last couple of years, city administration ambitions and resident feedback alike have pushed in the direction of modernizing city services and creating efficiencies, as well as quality of life enhancements, through the use of digital advancements.

From meters that help households detect wasted energy use to traffic grids that help commuters better plan the flow of their trip, the interest in digital transformation is there. But once these smart solutions have been built, how can they be kept secure? How can the trillions – yes, trillions – of digital connections that form a smart city be protected from bad actors?

Cyber safety and security are paramount in any smart city. The complexity can be daunting but when a city's cybersphere is secured, new and enhanced opportunities abound for residents, organizations, and visitors.

A cyber-first approach will guide city officials in the quest to become a safe and secure smart city.



# Smart ecosystems are massive and complex.

Like most new things, they come with new challenges and unique levels of infrastructure that call for a customized form of cybersecurity.

Did you know that seven in 10 people are expected to live in urban areas by 2050? This global prediction by the World Bank<sup>1</sup> shows urban population doubling in size over the next 25 years. Wherever you are in the world, it's safe to say that rapid urbanization is persisting – and now is the time to make it sustainable and cyber-safe for a more successful future.

This expected surge in urban population will inevitably increase pressures and stresses on cities' existing infrastructure and respective resources. Cities and communities face the balancing act of efficiently using finite resources while keeping the built environment sustainable from environmental, social, and economic standpoints.

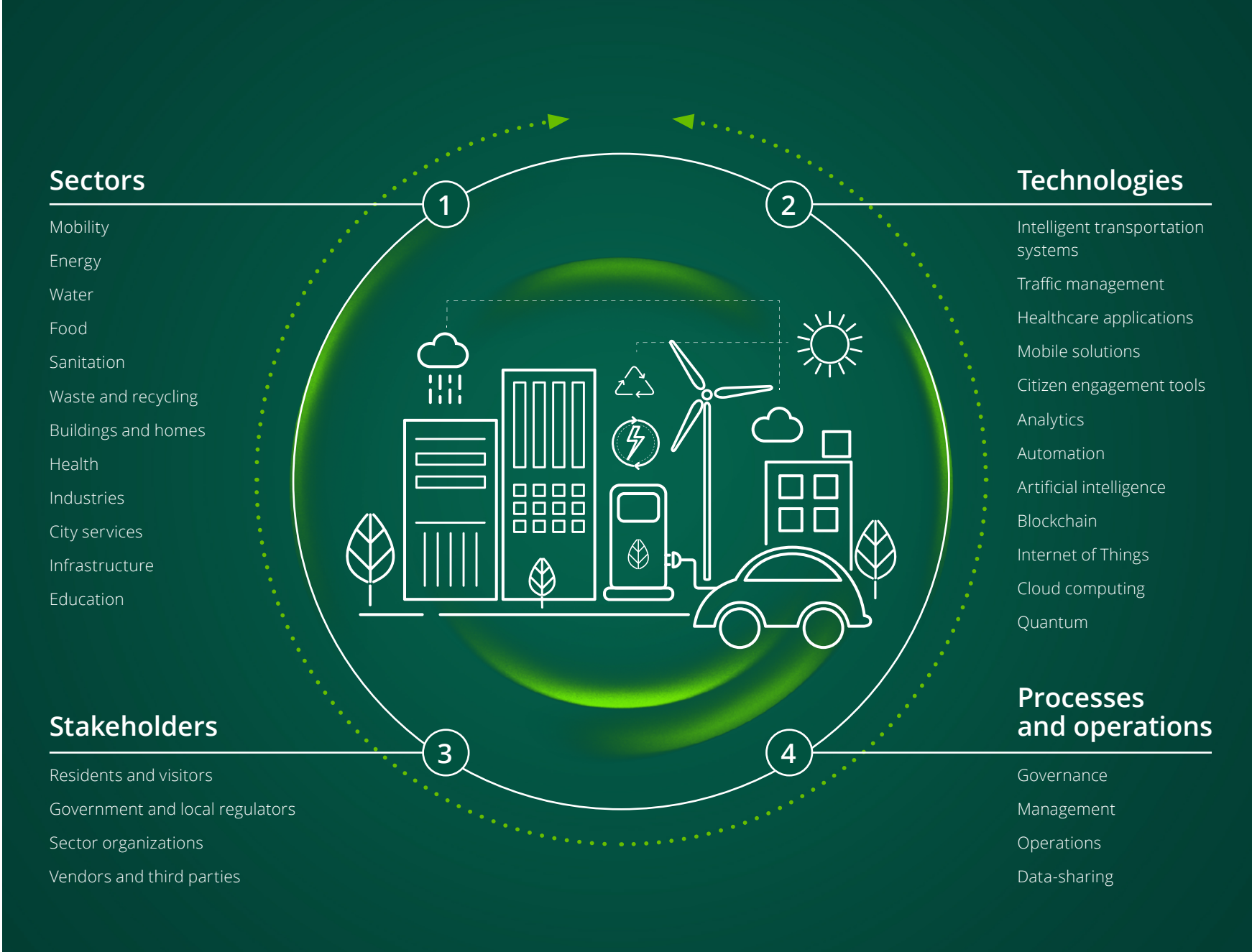
So, what can we do to prepare our cities? The smart city concept addresses these challenges. Many of us have heard of smart cities, but what makes a city “smart?”

Smart cities use digital technologies to better allocate public resources while increasing the overall quality of life. In smart cities, multiple sectors and industries come together to break down silos and slowly integrate, thus forming connected ecosystems. These ecosystems, enabled by data and technologies, use collective intelligence to optimize various functions of the city.

A smart city is one type of smart ecosystem. It involves an enormous network of digital connections where trillions of systems and devices are connected, exchanging information and controlling the physical environment by removing barriers between the cyber and physical worlds.



A smart ecosystem can include any integrated, digitally connected environment, such as a smart city, airport, transport network, power plant, or even a hospital.





Smart ecosystem developments present extraordinary opportunities for municipal leaders to improve community operations and efficiencies. However, these developments inherently introduce a myriad of information security, privacy, and regulatory challenges. Increased convergence, interoperability, and integration between information technology (IT), operations technology (OT), and the internet of things (IoT) in smart ecosystems provide avenues for bad actors to inflict significant harm – with very real and physical consequences – onto stakeholders.

Every single complexity of a smart ecosystem requires an [integrated, cyber-led approach](#); individual siloed approaches would be detrimental. Digital and physical consequences may become harsher as smart ecosystems continue to establish more digital connections, which are a fundamental and necessary driver of “smartness”.

Smart ecosystem administrators lack a holistic view of today’s cyber-risk landscape. That’s because traditional cybersecurity solutions are built to monitor a single enterprise. However, smart ecosystems, such as smart cities, have increased governance-related challenges and technical issues, in addition to multiple stakeholders and more third parties than ever before in their networks.

Unlike a traditional organization with a single point of contact for governance, the scale is entirely different for smart ecosystems. For example, a major US city collects over 500 million data events per day, ranging from smart meter details to broken streetlights.<sup>2</sup> Here, multiple disparate players come together with their own security and privacy needs based on different types of infrastructure and circumstances. However, the security for different IT, OT, and IoT governance structures need to be managed for the entire smart ecosystem.

**The complexity of a smart ecosystem requires an integrated, cyber-first approach.**

---

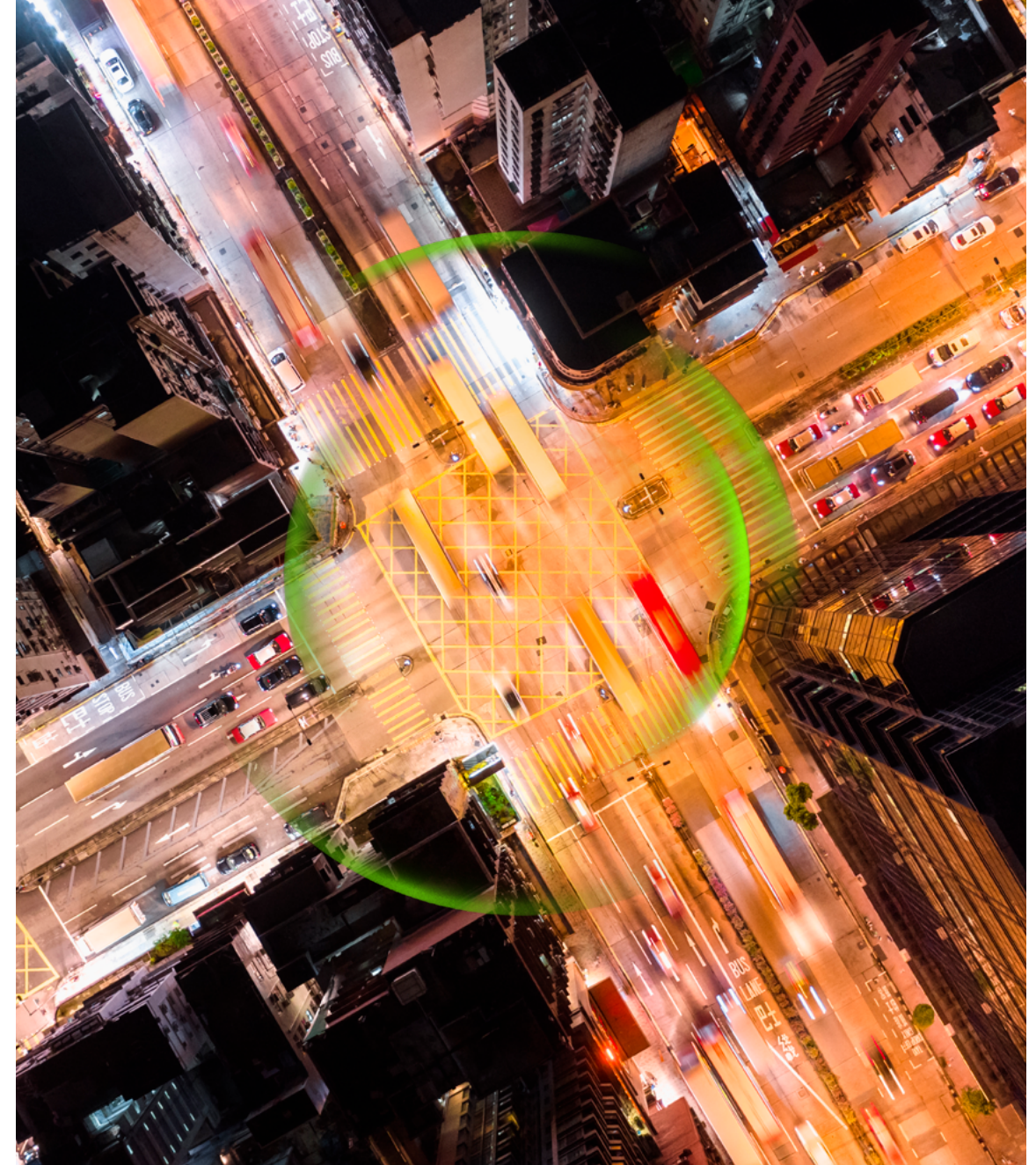
# As digital and physical infrastructure converge, smart ecosystems become more vulnerable.

## Let's look at the cybersecurity of smart ecosystems.


---

One of the first things we see is that digital transformation blurs the gap between the online and physical worlds, exponentially expanding the threat-attack surface. The impact of a cyberattack is no longer limited to data loss or financial loss. It can impact human life because the physical environment could also be affected.

In an attack on a water treatment plant in Florida, hackers altered the amount of sodium hydroxide in the water, which could have resulted in a serious health hazard. Thankfully, it was detected in the early stages. However, this incident highlights how cybercriminals can gain control of OT through IT systems, which could result in dire life or death circumstances such as cyberattacks that compromise hospital monitoring equipment.



# Smart ecosystems face complexity due to three key factors.

 [Click to read more about the sections](#)

When we studied the risk drivers in the hyperconnected areas of smart ecosystems, we found three key factors that create complexity, and sometimes even exacerbate it:



**Convergence:** This is where the cyber and physical worlds meet and the moment when IT systems connect with OT to blur the divide between both worlds. This exposes the OT and leaves it vulnerable to threats it didn't face when IT and OT were disconnected.



**Interoperability:** Here, we see a need for old and new systems and platforms to coexist and frequently interact. In the smart city's ecosystem, multitudes of diverse and disparate systems come together. Imagine millions of separate devices and processes with varying degrees of security maturity. Now, imagine them interconnecting and creating an inconsistent security model with gaps across the ecosystem. This would result in potential data breaches and give cyber criminals the chance to steal personal information and/or disrupt operations.



**Integration:** In a smart ecosystem, services across domains come together through IoT and digital technologies. This interconnectedness is perhaps the most fascinating aspect of a smart city, especially when you consider how integrated sectors, industries, and enabling infrastructures are. However, this interconnectedness also creates interdependencies.

An issue with one service area can quickly cascade into other areas, like dominoes, and result in essential services being degraded. It's important to understand key factors influencing the cyber-risk landscape. It's also vital to keep this at the forefront of our minds when we lay the foundations for a smart city and to use a holistic approach while mitigating risks.



1.

Convergence of IT and OT infrastructures

2.

Interoperability between legacy and digital technologies

3.

Integration and independence of sectors, processes, and technologies



# Examples of cyberattacks on smart ecosystems



## Convergence:

A petrochemical plant in Saudi Arabia entered an emergency shutdown due to Safety Instrumented System (SIS) malfunctions. SISs monitor levels of hazardous chemicals in plants and can initiate automated processes such as opening or closing relief valves. These systems were infiltrated by a threat group that had the ability to remotely reprogram the plant's operation. This was the first widely reported incidence of threat groups targeting industrial control system safety. In an attack scenario, the group could have commanded systems to ignore critical levels of dangerous chemicals in the plant, leading to injury and loss of life.<sup>3</sup>

A ransomware attack on an Alabama hospital debilitated computers and health sensors. During a birth at the hospital during the attack, nurses could not properly monitor or communicate fetal vital signs to physicians. The delivery led to severe brain damage to the baby due to asphyxiation, who later passed away after months in the intensive care unit. The attending physician is reported to have acknowledged that a cesarean section would've been performed if the staff had full access to the monitoring systems.<sup>4</sup>



## Interoperability:

A Florida water treatment plant was targeted by hackers attempting to alter the levels of sodium hydroxide in the plant's water. This could have affected up to 150,000 residents in surrounding areas. An observant engineer discovered the attackers' actions; however, the vulnerability via remote access was severe. The plant's workstations were running an outdated version of Windows 7 that was no longer supported by Microsoft.<sup>5,6</sup>

An Israeli semiconductor manufacturer, Tower, was targeted by ransomware that affected the chip maker's production floor. All operations were stopped as the company assessed the damage. A security researcher from Cybereason reported that the main issue in incidents where manufacturing systems are infected is the use of outdated operating systems. Systems are often left outdated due to concerns of self-inflicted production stoppages.<sup>7</sup>



## Integration:

The German city of Potsdam was targeted with a cyberattack that knocked out multiple public-facing portals for citizens to request information or services. These included the motor vehicle administration, registry information, and the Maerker platform, which is used to report infrastructure dangers and defects.<sup>8</sup>

Borger, a town in the Texas panhandle, reported a cyberattack that crippled the town's operations online. Services such as utility payment processing and access to archives, including, birth and death certificates, were all affected via integrated networks and systems. The attack also affected police officers, who couldn't access records they needed to do their jobs. Multiple municipalities in Texas reported similar ransomware attacks stemming from a third-party technology services contractor, with up to 20 different local governments affected.<sup>9</sup>

# Complexities differ based on the age and digital maturity level of the smart ecosystem.







The age of the environment, as well as the level of infrastructure and digital maturity, play a key role in the complexity of smart ecosystem cybersecurity.

Let's take a closer look at cities. Some are ancient, established thousands of years ago. Other cities find themselves at a crossroads where old meets new, and some cities are being built from scratch with the latest strategies and technologies. There are cities that were the first at their time to modernize, but now have aging technology that needs to be upgraded or integrated with new technology.

The varying degree of digital modernization with the integration of disparate technologies requires the holistic application of a cybersecurity framework across the ecosystem. The table below provides some examples of urban circumstances and their cybersecurity implications. The examples are not exhaustive, and more than one circumstance could apply to a city.



# Examples of urban circumstances for cybersecurity

Urban Circumstance	Description	Implications	Challenges
Ancient	Cities established thousands of years ago with layers of historical infrastructure	Digital modernization and cybersecurity woven into a deeply historical infrastructure, rather than rebuilding the infrastructure	 Convergence  Interoperability
Contemporary	Cities built in the last 200 years that are newer and often planned using contemporary urban planning concepts	Technology and cybersecurity infrastructure methodically added to grid systems	 Convergence
Starting from scratch	Cities at the initial development stage	Cybersecurity introduced and included right from the initial conception phase	 Integration
Merging	Cities merging with other nearby cities into one continuous urban and industrialized area, called a conurbation	Many disparate entities come together with different levels and needs for cybersecurity; vigilant coordination required	 Interoperability  Integration

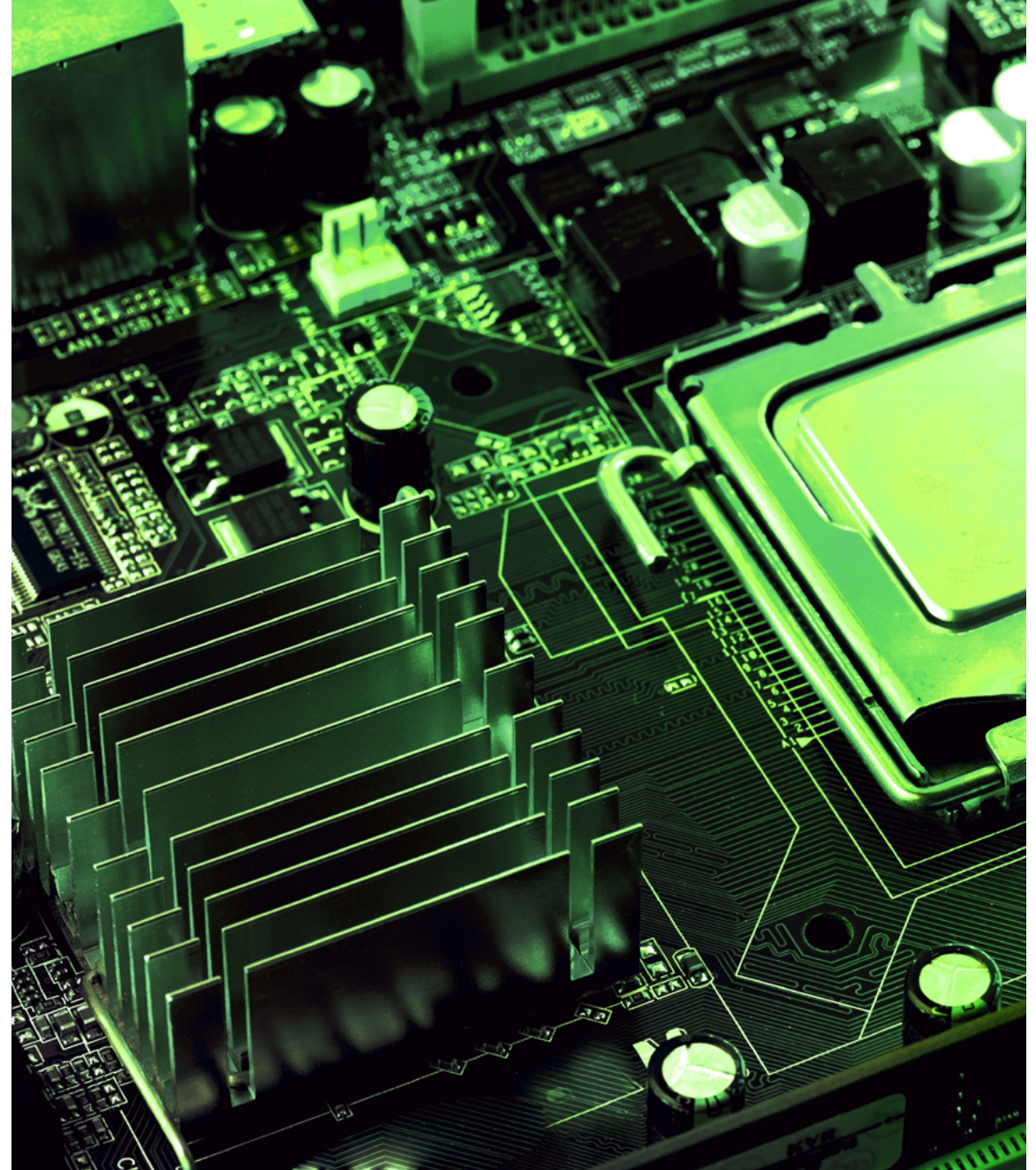
# A “cyber-first” approach increases safety and resiliency across the smart ecosystem.

## What can we do to make sure our smart cities are safe and resilient?

---

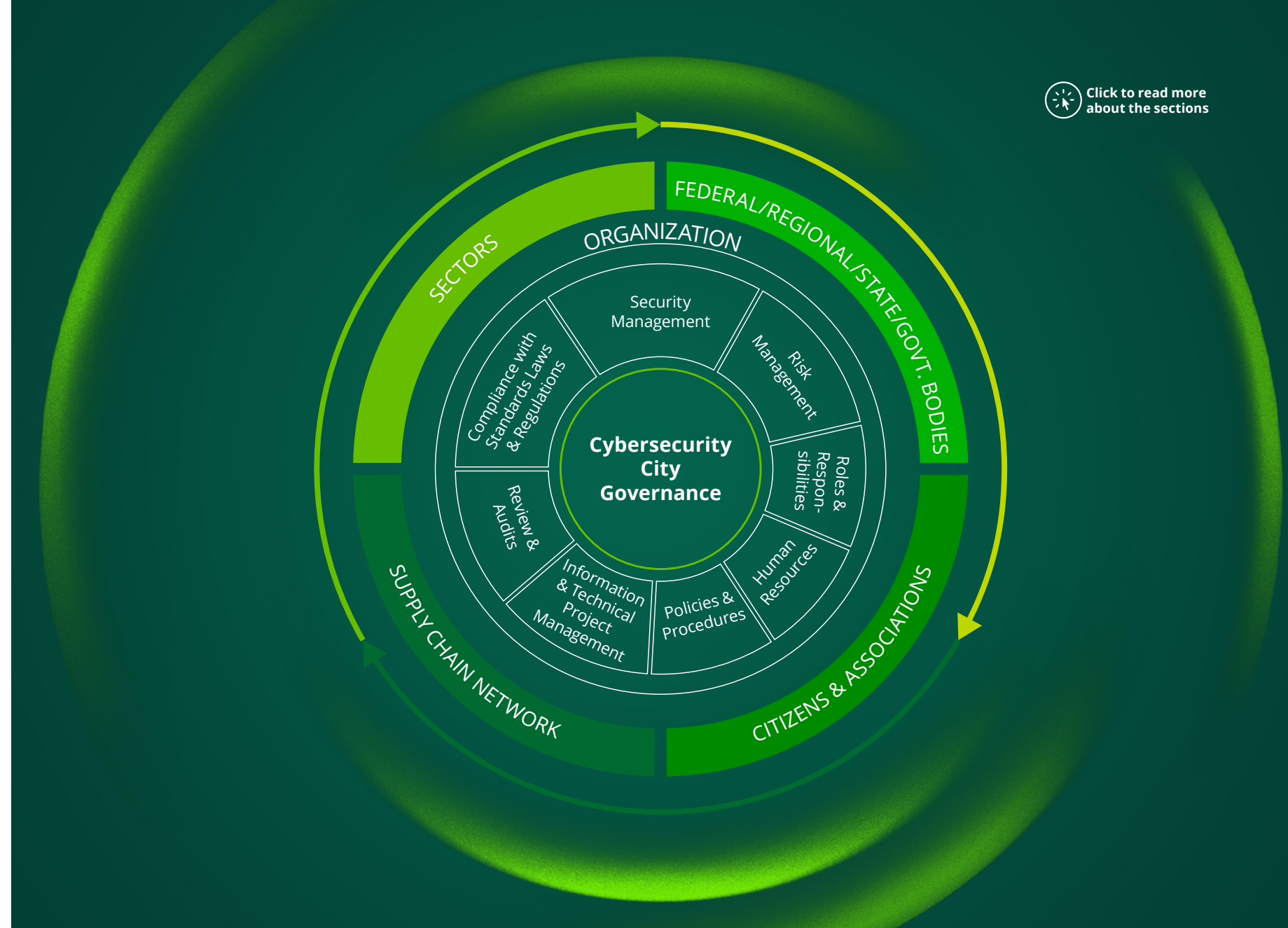
Cybersecurity for a smart city’s hyperconnected environment requires a holistic view of the entire ecosystem. This includes greater scrutiny on the ecosystem’s individual components and services and their influence on each other.

The “cyber-first” framework combines cyber controls throughout the smart ecosystem lifecycle, from the planning phase involving conceptualization and requirements determination, then moving into the integration/implementation phase of construction, and finally concluding in the operation phase.



A cyber-first approach increases safety and resiliency.

[Click to read more about the sections](#)



# Cyber-first phase 1: Planning

---

The cyber-first approach for securing smart ecosystems begins with the planning phase. During this phase, an environment is chosen for transformation into a smart ecosystem.

Then, assessments of existing infrastructure security and privacy are conducted to understand the environment's current state; applicable project standards and regulations are determined and cybersecurity and privacy target states are defined.

At the end of this phase, a high-level project roadmap is drafted to guide the project forward and bridge the gap between the assessed current state and desired target state. The activities of this phase form the foundation upon which critical infrastructure is designed, built, and integrated.

Planning components:

- **Cybersecurity assessment of the connected infrastructure:** Risks are identified and evaluated in alignment with regulatory requirements while conducting an audit of existing infrastructure.
- **Target state design and roadmap development:** The roadmap for developing the smart ecosystem's cybersecurity program is created, including the development of resiliency frameworks and plans.
- **Governance, risk, and compliance (GRC):** The smart ecosystem security and privacy governance model is created, including secure procurement and the development of policies and procedures, third-party risk management, and a communication framework to align security and device management.
- **Asset identification and classification:** Classification criteria and categorization of IT and OT assets are defined based on a rating of potential impact severity. A risk/criticality classification of IT and OT assets based on the impact rating is also applied.

---

## Case study: Smart cities from scratch

---

Smart cities that are being developed and built from scratch offer the opportunity for cybersecurity to be a key concept included right from the initial conception phase. New smart cities can incorporate cybersecurity strategies and learnings for city leadership, citizens, visitors, and other stakeholders in the initial design to continuously evolve cybersecurity and data privacy concepts based on user feedback.

### Opportunities:

- **Cyber strategy roadmap:** Creating the cyber strategy roadmap in the planning phase
- **Community learning program:** Developing a program to foster innovation in the community through education, collaboration, and awareness for continuous improvement

# Cyber-first phase 2: Integration/implementation

---

Once the planning phase is finished, the integration/implementation phase can begin. Here, smart ecosystem project teams focus on building out architectural and high-level operational components for the security and privacy program within the smart ecosystem.

Then the project roadmap drafted during the planning phase is revised to include more granular activities. These include creating a digital asset inventory, selecting and implementing digital identity, identifying data protection tools and processes, determining vulnerability management and threat-intelligence solutions, and constructing robust training and awareness programs. Project teams then can perform a baseline security risk assessment for the newly connected infrastructure.

Throughout this phase, it's essential to align each component with the applicable standards and regulations determined in the planning phase. Integration/implementation components:

- **Security architecture and roadmap:** Security architecture of the smart ecosystem is created. This includes developing the security technology operating model, service catalog, security library, and the roadmap for security technology implementation.
- **Digital identity:** Smart ecosystem identity solutions are developed to verify identities of integrated systems before granting access to ecosystem data.
- **Data protection:** Controls around data encryption, privacy, storage, transfer, and more are implemented to align with regulatory requirements
- **Vulnerability management:** This process is established to identify, classify, prioritize, remediate, and mitigate vulnerabilities in the smart ecosystem infrastructure.
- **Threat-intelligence platforms:** Monitoring requirements are planned, identified, and mapped, and enhanced infrastructure is designed and implemented.

---

## Case study: Tunnels and bridges

---

Deloitte supported the [Pennsylvania Turnpike Commission](#) (PTC) in modernizing the mile-long Tuscarora Mountain Tunnel, one of the four tunnels providing passage for drivers as they traverse the 360-mile-long road through the Appalachian Mountains. The commission not only faced typical civil engineering challenges, but it also had to manage a host of cybersecurity risks directly related to a complex web of connected devices deployed throughout the tunnel.

The project required the deployment of connected environmental sensors that measure and report on tunnel conditions, temperature, and levels of carbon dioxide and other gases; automated ventilation, lighting, and video detection systems; and a control system that collects data and enables remote monitoring, among other devices and systems.

With so many physical devices now part of the tech stack, the commission knew they needed to take a farsighted, preemptive approach to cybersecurity. The engineering and security teams decided to tailor and use prescriptive cybersecurity standards typically used in power grids.

### Project highlights:

- **Proactive cybersecurity:** Enabled farsighted planning of critical virtual-physical infrastructure and proactive cybersecurity in the design, with OT for future design efforts
- **Cyber communications:** Enabled cybersecurity collaboration between PTC operations, design, engineering, and construction teams and standardized change management processes for the cyber-physical space

# Cyber-first phase 3: Operation

---

As the smart ecosystem begins transitioning into the third and final phase, the operation phase, administrators focus on creating resiliency to operate safely, strengthen customer trust, and boost stakeholder value.

This phase includes bolstering cybersecurity support and managed services, continuously undertaking threat evaluation and monitoring, and constantly identifying opportunities for security and privacy improvement.

Operation components:

- **Managed threat-evaluation services:** This involves audit readiness and technical evaluation, manual review, automated vulnerability scanning, and continuous/early detection of threats. These services will allow users to prioritize and address threats within ongoing processes.
- **Secure operations center:** Smart ecosystem cybersecurity incidents are monitored, analyzed, and resolved on a continuous basis. Consolidated, consistent monitoring allows for incident resolution in real time.
- **Threat intelligence:** Private, public, and regulatory entities are coordinated for threat intelligence through a central and secure platform to cooperate on threat mitigation.
- **Recovery and resiliency:** Processes and procedures for business continuity management, disaster recovery, data back and recovery, and incident response are monitored and continuously evaluated. This helps reduce the ecosystem's vulnerability to losing valuable data and functionality in the instance of an incident, such as a cyberattack, natural disaster, or system outage.

---

## Case study: Contemporary cities

---

Contemporary cities can take the opportunity to find convergence between their legacy systems and the opportunity to modernize and operate with cybersecurity infrastructure. Deloitte is supporting cities and infrastructure entities around the world for Identity Access Management (IAM), Privileged Access Management (PAM), Data Protection services, Application Security, Infrastructure Security, Threat Intelligence, Threat Hunting, and Vulnerability Management. The “Digital Identity by Deloitte” solution can transform a city’s workforce identity governance, access management, and privileged access controls, which helps enhance safety, resiliency, and citizen trust.

### Opportunities:

- **IAM roadmap:** Empowers stakeholders to visualize and map cyber IAM in the short- and long-term
- **Proven implementation design:** Implementation of a standardized IAM solution that removes bottlenecks and improves user experience





Take action!

Rapid urbanization is here to stay for the foreseeable future. City officials across the globe can embrace this reality and create spaces and places that are safe and ready for the opportunities and risks inherent in today's blended virtual-physical worlds.

Deloitte is poised to help city leaders secure the future, smartly. Please email any of the authors on the [next page](#) if you would like to inquire about evolving into, and safeguarding, a smart city.

# About the Authors



Click to view  
biographies

## **Acknowledgements**

The authors would like to thank Peter Wirnsperger and Paul Beverley for reviewing and contributing ideas and insights and Deepali Kochhar, Rita Machado, Harris Block, Tanner Brooks, and Larissa Dorn for key contributions during the research and development of this project.

# Endnotes

1. The World Bank, "[Urban Development](#)," accessed August 17, 2023.
2. Merritt Maxim and Salvatore Schiano, [Making Smart Cities Safe and Secure](#), Forrester, 2021, p. 4.
3. Samuel Gibbs, "[Triton: hackers take out safety systems in 'watershed' attack on energy plant](#)," The Guardian, December 15, 2017.
4. TrendMicro, "[New Critical Infrastructure Facility Hit by Group Behind TRITON](#)," April 11, 2019.
5. Kevin Poulsen, Robert McMillan, and Melanie Evans, "[A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death](#)," The Wall Street Journal, September 30, 2021.
6. Casey Crane, "[Hacker Breaches Florida Water Treatment Plant, Adds Lye to City's Water Supply](#)," Security Boulevard, February 16, 2021.
7. Lee Mathews, "[Florida Water Plant Hackers Exploited Old Software and Poor Password Habits](#)," Forbes, February 15, 2021.
8. Meir Orbach, "[Israeli chipmaker Tower confirms cyberattack forced it to shut down systems](#)," Calcalist Tech, September 6, 2020.
9. Sergiu Gatlan, "[City of Potsdam Servers Offline Following Cyberattack](#)," Bleeping Computer, January 24, 2020.
10. Jake Bleiberg and Eric Tucker, "[Holy Moly!: Inside Texas' Fight Against a Ransomware Hack](#)," Bloomberg News, The Associated Press, July 26, 2021.
11. Samuel Gibbs, "[Triton: hackers take out safety systems in 'watershed' attack on energy plant](#)," The Guardian, December 15, 2017.
12. Samuel Gibbs, "[Triton: hackers take out safety systems in 'watershed' attack on energy plant](#)," The Guardian, December 15, 2017.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL ( also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s more than 450,000 people worldwide make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

2023. For information, contact Deloitte Global.

Designed and produced by 368 at Deloitte. J31276