# Foundational and emergent capabilities of IoT

December 2022

# Table of contents

# 1 Executive summary

Today's well-designed, secure and compliant internet of things (IoT) products and services possess extraordinary capabilities. But even knowing the tremendous amount of potential that exists, it can be overwhelming for IT and business leaders to develop an IoT strategy.

To begin, organizations need a strategy to focus on foundational IoT capabilities as part of their technology operating model. They must fortify the infrastructure to prepare for an influx of data, new security threats and even more complex privacy concerns. Adopting a well-thought-out organizational model, funding plan and talent strategy is important for success. This work must be done in parallel with choosing appropriate tools and aligning with overall enterprise architecture (EA).

In the long term, organizations will want to prepare for emerging and disruptive capabilities that both challenge and augment the development and evolution of IoT solutions. The emerging capabilities may require organizations to reengineer their IoT solutions.

The purpose of this paper is to review some of the foundational and emerging IoT capabilities that will help organizations develop short- to long-term plans. So, what's next for your organization's IoT strategy?

# 2 Problem statement

In an increasingly interconnected world, the commercial and industrial applications of IoT technology are poised for exponential growth. In 2021, there were more than 11 billion active IoT devices, and projections show that number will surpass 29.4 billion by 2030 [1]. While this is an exciting change for commerce, collaboration and connectivity, it also creates new expectations around data privacy, security and governance. These evolving expectations are creating unique challenges and opportunities for product developers and regulators. Along with the promise of emerging technologies (specifically IoT), futuristic leaders also realize that there is an opportunity cost if IoT is not integrated into the organization.

While most consumer-oriented IoT devices such as mobile phones and wearables are easy to develop, install and use, IoT solutions at an industrial scale warrant more planning. In addition, town planning for IoT-driven smart cities requires coordination with government authorities, solution architects and original equipment manufacturers (OEMs), as these solutions are designed to be interfaced across several civic utilities.

From an engineering standpoint, IoT is unique in its interplay between the physical and the digital world. IoT applications succeed when they work in conjunction with reliable networks and the ability to harness large quantities of data, making participation in the IoT space challenging. Developing IoT solutions requires new talent that is trained in reliability engineering, solution design, human centricity, durability and sustainability. Governance of data, maintenance and upkeep of solutions, and resilience will be key differentiators in the future, all of which require appropriate talent and leadership.

**The EY Experience: waste disposal company XYZ, trucking software [2]**

EY team combined its sector knowledge and IoT experience to put IoT at the heart of XYZ's digital transformation journey. XYZ employed radio frequency identification (RFID) tags that provided the exact weight and location of each waste bin throughout the collection route. By connecting their waste bins, containers and trucks, XYZ reduced manual effort and provided optimal routes for each driver by harnessing real-time data that XYZ shared with the city in using a secure network.

# 3 Foundational capabilities

A IoT governance and security

B Organizational model

C Enterprise architecture

Organizations new to IoT adoption can start by concentrating on three foundational areas of the IoT operating model: IoT governance and security, organizational model and enterprise architecture. Focusing on these gives the organization the opportunity to start developing capabilities that form the underlying structure for an IoT strategy. Data quality, security and privacy are primary concerns for regulators, and organizations need to closely monitor these evolving risks to structure a comprehensive IoT governance and security framework. To introduce a new IoT-driven organizational model and to fund the new roles, it's important to garner the support of stakeholders and define budget allocations. Enterprise architecture is the backbone of any IoT strategy as hardware and software are tightly integrated. Each of these three pillars is equally important and should be considered holistically to avoid operating in a siloed fashion.

## Chapter 3.A: IOT governance and security

1 Data quality

2 Security

3 Privacy

There are three key risk areas across the IoT ecosystem that have the greatest potential for harm: data quality, security and privacy.

1| **Data quality**: Data collection, analysis and applications fuel IoT solutions. High-quality IoT data also sets the foundation for other intelligent solutions. On the other hand, poor data quality can adversely impact safety-critical and mission-critical systems. As IoT devices become ubiquitous, security vulnerabilities and exploits continue to grow unchecked by current security standards. As ecosystems of IoT devices develop capabilities to infer and predict human behavior, the methods and structures of existing privacy measures are being undermined.

2| **Security**: IoT solutions typically warrant interaction between several physical devices and the network. Having multiple points of entry adds to the vulnerability of the overall ecosystem. It can take five minutes or less [3] for hackers to scan and compromise a new IoT device on the internet. Many of the IoT ecosystems today do not have robust mechanisms for software and firmware lifecycle maintenance, leaving them vulnerable to security exploits and data exfiltration and a potential conduit for botnets and other advanced persistent threats.

3| **Privacy**: Perhaps the greatest threat posed by IoT devices is a new risk to privacy as vast amounts of data are collected and the varying manufacturers and users of IoT systems exist within an ecosystem. Companies must consider how to both make their connected devices more resilient to cyber threats and attacks and how to protect the privacy of users and their personal information.

2018
GDPR act

2019
ETSI guide

2020
US IoT cyber act

2021
PIPL act

The legal landscape of privacy protection regulations is continuing to evolve. Following the well-known GDPR act of 2018, several laws have been passed to protect consumers' privacy.

In 2019, the European Telecommunications Standards Institute (ETSI) released a technical specification guide for "Cyber Security for the Consumer IoT" marketplace to provide a framework for best practices around the security of consumer IoT devices. [4]

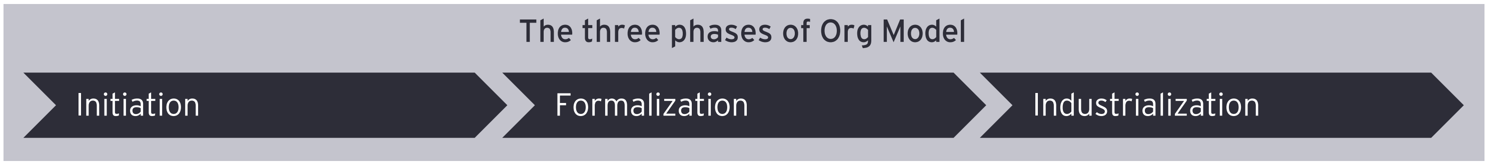
In 2020, the first US IoT Cybersecurity Improvement Act was signed into law and the US' National Institute of Standards and Technology (NIST) released guidelines for data protection called the Foundational Cybersecurity Activities for IoT Device Manufacturers. [5]

In 2021, China enacted a Personal Information Protection Law (PIPL) mandating that firms that collect IoT data must get prior consent to obtain the data and can choose to refuse services to consumers who elected to opt out of having their information used. [6]

As these laws have only been enacted in the last few years, we should expect that the landscape will become increasingly complex. Organizations need to adhere to IoT policies that can scale for global growth and adhere to the nuances of differing regulations across the world. To monitor and manage the risks posed by IoT, it will be necessary to create:

- New standards for interoperability and lifecycle maintenance
- New regulations and innovation to manage the risks to privacy
- Strong enterprise and ecosystem data governance to manage data quality

## Chapter 3.B: Organizational model


The three phases of Org Model

Initiation

Formalization

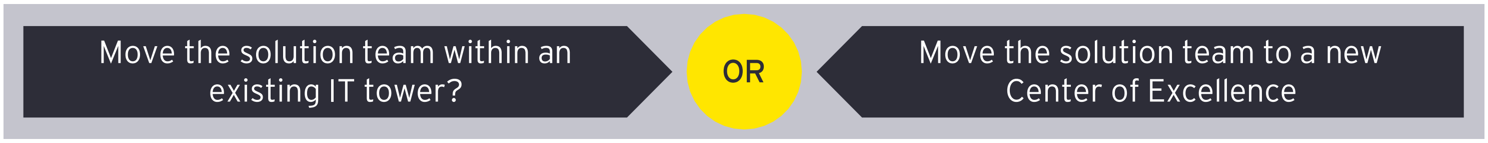
Industrialization

A good organizational design requires strategic placement of talent for solution development and adoption across three phases: Initiation, Formalization and Industrialization. Equally important is a strategic plan for how funding models will evolve as the organization matures through each phase.

The vision for how the organization will evolve and mature over time is developed in the **Initiation** phase. The focus of this phase should be on empowering talent to experiment and create rapid prototypes that can quickly show value or be discarded to make room for further experimentation. The team is generally made up of a small, dedicated group of motivated full-time employees who start with the goal of developing two to four prototypes that solve a market problem.

During Initiation, the funding typically comes from the budget of the Chief Information Officer (CIO) as part of innovation and capex budgets. The IoT innovation team is empowered to think outside the box and be more creative in solution design. In this phase, some measures of success are the number of use cases identified and analysed, prototypes or features developed, and product owners who have adopted the prototype solution for beta testing in a real market setting.

To encourage experimentation and adoption, a good practice is to keep innovation "free" for the product owners. Since it is not allocated in department budgets, there is no cost of failure. This enables the IoT innovation team to collaborate with the product teams and think more deeply about the challenges, opportunities and roadmap of the product. As the organization evolves (i.e., Initiation > Formalization > Industrialization), so does the method of funding.


Move the solution team within an existing IT tower?

OR

Move the solution team to a new Center of Excellence

As the prototypes evolve, they begin to **Formalize** within the organization, and the decision must be made whether to move the solution teams into a specific product tower or develop a Center of Excellence (CoE). In specific product towers, the use cases (i.e., prototypes) are narrow in scope. The advantage of this option is that it keeps the team focused on managing its own budgets, roadmaps and talent for IoT. In addition, early integration with an existing product tower allows the IoT innovation team to receive feedback from established customers and to make targeted improvements in future iterations.

The second option, developing a CoE for IoT, is recommended for use cases (i.e., prototypes) that are broader in scope. The objective of a typical COE would be to enable IoT solutions within several products and services across the organization. Broad IoT use cases typically allow portfolio leads to move towards interoperability, data gathering and synthesis across various products. Upon successful adoption of the CoE's IoT solutions with one to two product portfolios, more demand gets generated within the organization. The expansion of the CoE model relies on the demand and adoption by other product owners, which requires significant coordination of time, resources and budgets.

As prototypes succeed and product owners see value in the adoption of IoT solution(s), the product owners can start to budget for scaling and maturing the solution. Depending on the scope of the IoT solution (i.e., specific IoT product tower vs. IoT CoE), the IoT solution can either move toward generating its own revenue (i.e., become a product tower) or rely on a chargeback funding model for the CoE. A chargeback model enables the IoT team to fund its activities and grow in line with adoption levels of its solutions.

If the product/portfolio owners are confident in the value of the use case, they can decide to fund the IoT capability 100% moving forward. This would allow them to systematically prioritize features and direct the IoT efforts in alignment with their product strategy. At the same time, the IT organization can continue investing in identifying newer use cases and garner more support from leadership based on the evidence of past successes.

Given that IoT applications vary by industry, some IoT CoEs may fall under the purview of the Chief Technology Officer (CTO) vs. that of the CIO. IoT solutions inherently involve physical and digital components, thus it is important to identify capabilities that go across the offices of the CTO and CIO. Stakeholders with experience and knowledge of enterprise capabilities are better suited to be a part of the IoT CoE. The IoT CoE should comprise individuals from varying backgrounds such as business, sensor technology, legal/compliance, reliability engineering, facilities management and others involved in developing and implementing the solution.

Office of the Chief Information Officer (CIO)

vs.

Office of the Chief Technology Officer (CTO)

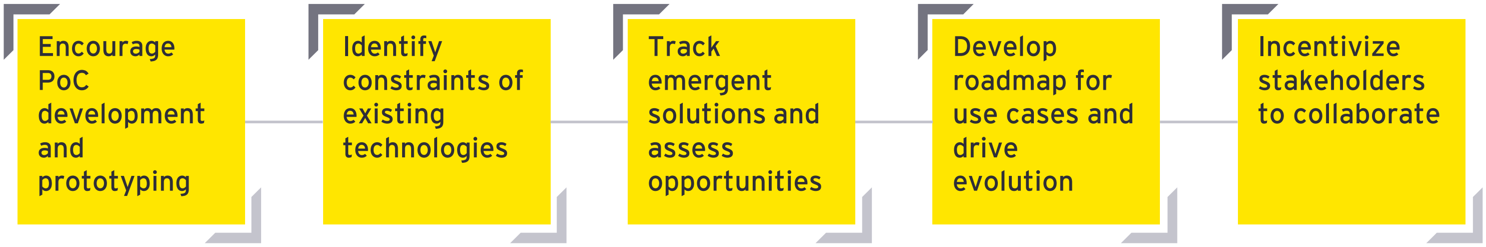
The ultimate design objective is to ingrain IoT into the culture and strategy of the organization. In the **Industrialization** phase, the identification of IoT use cases, development of IoT capabilities, management of talent and adoption of IoT solutions should ultimately become routine within the organization.

There are several initiatives that may help mature IoT capabilities and increase their adoption:

- Recruit talent internally and incentivize employees and business leaders to participate in employee-led innovation and idea generation
- Identify, onboard and empower change agents and champions across the organization who will take an interest in understanding existing IoT capabilities, proactively identify gaps within the product portfolios and help develop solution designs
- Develop, maintain and publicize collateral for internal awareness of success stories, capabilities, trainings and seminars
- Upskill existing non-IoT talent and improve IoT adoption

In one such example, the IoT innovation team collaborated with facilities management to install sensors in conference rooms to check real-time occupancy status and provide availability updates via Outlook and the room reservation application. This both provided a new capability for the facilities team as well as placed a visible IoT application in front of every office employee to promote IoT presence in the workplace.

## Chapter 3.C: Enterprise architecture and tooling considerations



Encourage PoC development and prototyping

Identify constraints of existing technologies

Track emergent solutions and assess opportunities

Develop roadmap for use cases and drive evolution

Incentivize stakeholders to collaborate

During early IoT adoption, proof-of-concept (PoC) development and prototyping should be built upon existing enterprise technical capabilities. Equally important is the focus on solution design and user centricity. Balancing the constraints of existing technology and the evolving needs of the customer would result in new, non-standard technologies being introduced into the environment. During this time, enterprise architecture's role in IoT adoption includes tracking emergent architecture and trends in the market, assessing the technologies introduced by the innovation teams and setting enterprise standards to enable scaling of the select technologies while discouraging the use of others.

The boundaries and evolution of IoT use cases are decided based on buy-in from the business and are dependent on inputs from the EA function. It is beneficial to target business areas that are fit for reinventing their processes and capabilities at the business architecture level. The enterprise architecture function and IoT innovation team should be incentivized and empowered to collaborate when charting requirements for the design of the information and application layers of IoT-related technologies. This approach reduces friction during the initial stages and has a higher potential for adoption in the long term. Additionally, the approach minimizes the cost of transition.

Another important area for IoT is the management of IoT assets. Given that IoT solutions use physical sensors and devices, managing the inventory and lifecycle of these assets is key. All physical assets have a usable life, and the device manufacturers may not be able to estimate life-span accurately due to physical and environmental factors that affect the devices in unpredictable ways. Managing inventory involves sourcing from high-quality OEMs, collecting performance data in real time, monitoring the network in aggregate for performance drift, and proactively scheduling maintenance and replacements.

As the IoT use cases mature and become part of the product and portfolio roadmaps, the EA function can help upgrade standards at an enterprise level. This applies not just to IoT but to innovation in general. The challenge with managing standards within an organization lies in the wide variety of standards that different sensor and device manufacturers follow. Building a multi-vendor environment can mean that devices would not be interoperable and may need additional interfaces and calibrations as part of the solution design.

At present, IoT offerings and solution providers compose an immature but rapidly evolving market. The same is true for standards and leading practices for IoT within EA. An evolving market can be hard to predict, so it is important for the EA function to stay engaged, informed and nimble. However, standards can only change after successful experimentation. Hence, the focus of EA standards at the early stages of IoT adoption should be to enable scale and industrialization.

Similarly, tools and providers are also evolving. Established technology giants and new entrants are all working on a range of offerings and, in the early stages of going to market, both large enterprise software vendors and small providers have similar capabilities. In the **Initiation** phase, many teams select tools that are easy to use, affordable and dedicated to IoT. In the **Formalization** and **Industrialization** phases, it is important to choose tools that are interoperable with the organization's existing suite of tools and have a proven track record of supporting complex and large implementations.

IoT tools bridge the crossover from physical sensors to digital applications. Given the dependencies with other third-party providers and OEMs, the right mix of tools becomes a key factor of success. There is a range of tools in the market with varying features and capabilities: software development tools, tools that support microprocessor programming, tools for real-time monitoring and support, tools for interoperability, and tools for analytics and data synthesis.

Most IoT devices are designed to be low-cost and conform to proprietary standards for measurement, precision and reliability. Differences in implementation and tolerances that are perfectly acceptable for package handling or warehouse monitoring can cause a problem when used for advanced sensing or real-time applications with profound implications for safety-critical systems such as traffic control, autonomous driving, health care or public utilities.

# 4 Emergent capabilities and positive disruptions

Nanosensors

Private 5G Networks

Wifi-6

Digital Twin

As IoT adoption accelerates, organizations will increasingly face scalability challenges around sensor and communication capabilities: congested networks, heterogeneity of data and flood of input, to name a few. IoT is part of an ecosystem of intricately woven solutions that harness the combinatorial effect of technology. Accurate sensors, dedicated networks and strong wireless connectivity all need to work together harmoniously to deliver value effectively. Beyond the short-term IoT strategy and tactical implementation processes, organizations need to consider adopting emerging technologies that enable IT organizations to innovate more rapidly.

A| **Nanosensors**: In industries that rely on specialized devices, such as manufacturing plants or health care providers, IT and operational technology (OT) teams collaborate to apply IoT technologies to specialized use cases such as manufacturing controls and equipment monitoring. For IoT use cases requiring ultra-sensitive monitoring, such as medical diagnostics, precision equipment monitoring and food safety, nanosensors are being increasingly employed.

As defined by Nature Portfolio, **nanosensors** are "chemical or mechanical sensors that can be used to detect the presence of chemical species and nanoparticles, or monitor physical parameters such as temperature, on the nanoscale." Other methods to detect similar particles usually require expensive equipment and need highly skilled labor to collect species and operate. Nanosensors perform sample preparation, recognition and signal transduction by themselves and send out computable signals. As a result, they are cheaper and easier to implement for real-time delivery of results. [7]

B| **Private 5G Networks**: According to the EY 5G enterprise study (2020), "Private and secure network capability at specific locations" was ranked as the number one perceived benefit of 5G technology. Private 5G networks are often localized and operated within the confines of factories and warehouses. A **private 5G** network allows the organization to entirely localize data and put up an additional layer against security threats. For organizations demanding great configurability or data isolation in their IoT strategy, a private 5G network could be an important connectivity option. [8]

C| **Wifi-6**: Wi-Fi will also continue to play a large role in fulfilling the connectivity demands of IoT. Given the high accessibility of Wi-Fi among households and the improved capability of supporting multiple devices, Wi-Fi 6 could be a good fit for smart home devices. **Wi-Fi 6** is a new generation of Wi-Fi standard that can work in 6-GHz frequency bands. Wi-Fi 6 lets routers communicate with more devices at once. Enterprise users can assess the optional functionalities of Wi-Fi 6 when they construct IoT systems with significant improvements in security protocols. In an environment with obstacles, it offers reliable connection as it penetrates those obstacles effectively. [9]

D| **Digital Twin:** Digital twin is a virtual tool that can create exact digital replicas of functioning operations. This allows for proactive planning and scenario building, enabling greater flexibility and modification of the physical environment. Artificial intelligence (AI)/machine learning (ML) runs predictive analysis and maps out various scenarios using real-time input from IoT sensors. Additionally, the digital twin provides a safety mechanism: If operations unexpectedly lose function, the exact digital copy allows for little to no downtime in the face of serious operational issues. [10]

Deep understanding of the physical use case is a crucial step to harnessing emerging technologies in a scalable and sustainable fashion. In addition to the technical considerations, social and regulatory factors remain key topics in decision-making. As previously discussed, the ubiquitous nature of IoT infrastructure is a persistent source of personal privacy concerns - a strategy for data protection and public communication must be developed early. Finally, the IT team needs to overcome the organizational segregation and collaborate with OT and the business teams to define and iterate a capability roadmap and monitor emerging technological options.

# 5 What's next?

The very first IoT device was birthed in the early 1980s on Carnegie Mellon University's campus. A graduate student in the Computer Science department had a craving for a cold soda, but the machine was often empty and rather far away. Wanting to avoid the disappointment of a long walk met with no caffeine jolt, a group of students applied the use of IoT to create a revolutionary device. From anywhere on campus, students that were logged into one of the school's 300 ARPANET-connected computers could look up if there were any sodas in stock and, if so, which ones were cold. [11]

But what a difference 40 years can make! Today, there are billions of devices connected to the internet, and IoT is considered one of the most important technological catalysts of the fourth industrial revolution. Since the 1980s, we have seen a large acceleration of businesses needing to undergo major technology transformations to remain competitive. Some contributing factors to the wider adoption rates include consumer demand for omnichannel experiences, declining hardware and software costs, and increased hiring of technical roles.

When the soda machine monitor was first created, scaling IoT was a huge financial undertaking, which slowed the rate of adoption. A few decades later, hardware and software costs have dropped significantly. Technology careers are expanding and organizations that wouldn't typically be considered tech are starting to employ an increasing number of in-house technical roles.

## So, what's next for your organization?

The businesses that will gain the most potential value from IoT are those that operate in standardized production environments such as manufacturing, health, retail and hospitality. However, a properly implemented and strategic IoT transformation can benefit organizations within any industry sector. To embark on an IoT transformation, the organization must first focus on how it will manage its IoT ecosystem: establish governance and security policies, design the organizational model and empower enterprise architecture.

Organizations with strong foundational capabilities stand to realize the full potential of emerging technologies that both enhance the existing offerings and also create new revenue-generating opportunities.

# 6 References and sources:

1. "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030," *Statista website*, accessed 17 October 2022, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide.
2. "Placing IoT technology at the heart of your digital transformation | EY – US I Suez Case," *EY website*, https://www.ey.com/en_us/consulting/placing-iot-technology-at-the-heart-of-your-digital-transform, accessed 17 October 2022.
3. "Securing Your 'Internet of Things' Devices," *U.S. Department of Justice website*, https://www.justice.gov/criminal-ccips/page/file/984001/download, July 2017.
4. "Cyber Security for Consumer Internet of Things," *ETSI website*, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf, accessed 17 October 2022.
5. "Foundational Cybersecurity Activities for IoT Device Manufacturers," *NIST website*, https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers, accessed 17 October 2022.
6. "The Personal Information Protection Law: China's Version of the GDPR?," *Columbia Journal of Transnational Law website*, https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr, 14 February 2022.
7. "Nanosensors," *Nature.com website*, https://www.nature.com/subjects/nanosensors, accessed 17 October 2022.
8. "5G IoT Private & Dedicated Networks for Industry 4.0," *GSMA website*, https://www.gsma.com/iot/wp-content/uploads/2020/10/2020-10-GSMA-5G-IoT-Private-and-Dedicated-Networks-for-Industry-4.0.pdf, October 2020.
9. "Wi-Fi 6 and Wi-Fi 6E: The key to IoT," *The Beacon website*, https://www.wi-fi.org/beacon/kevin-robinson/wi-fi-6-and-wi-fi-6e-the-key-to-iot, 21 March 2022.
10. "Can a supply chain digital twin make you twice as agile?," *EY website*, https://www.ey.com/en_us/advanced-manufacturing/can-a-supply-chain-digital-twin-make-you-twice-as-agile, accessed 17 October 2022.
11. "The Little-known story of the first IoT device," *IBM website*, https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/, 7 February 2018.

# Ernst & Young LLP authors

**Mike Ray**
Executive Director
mike.ray@ey.com

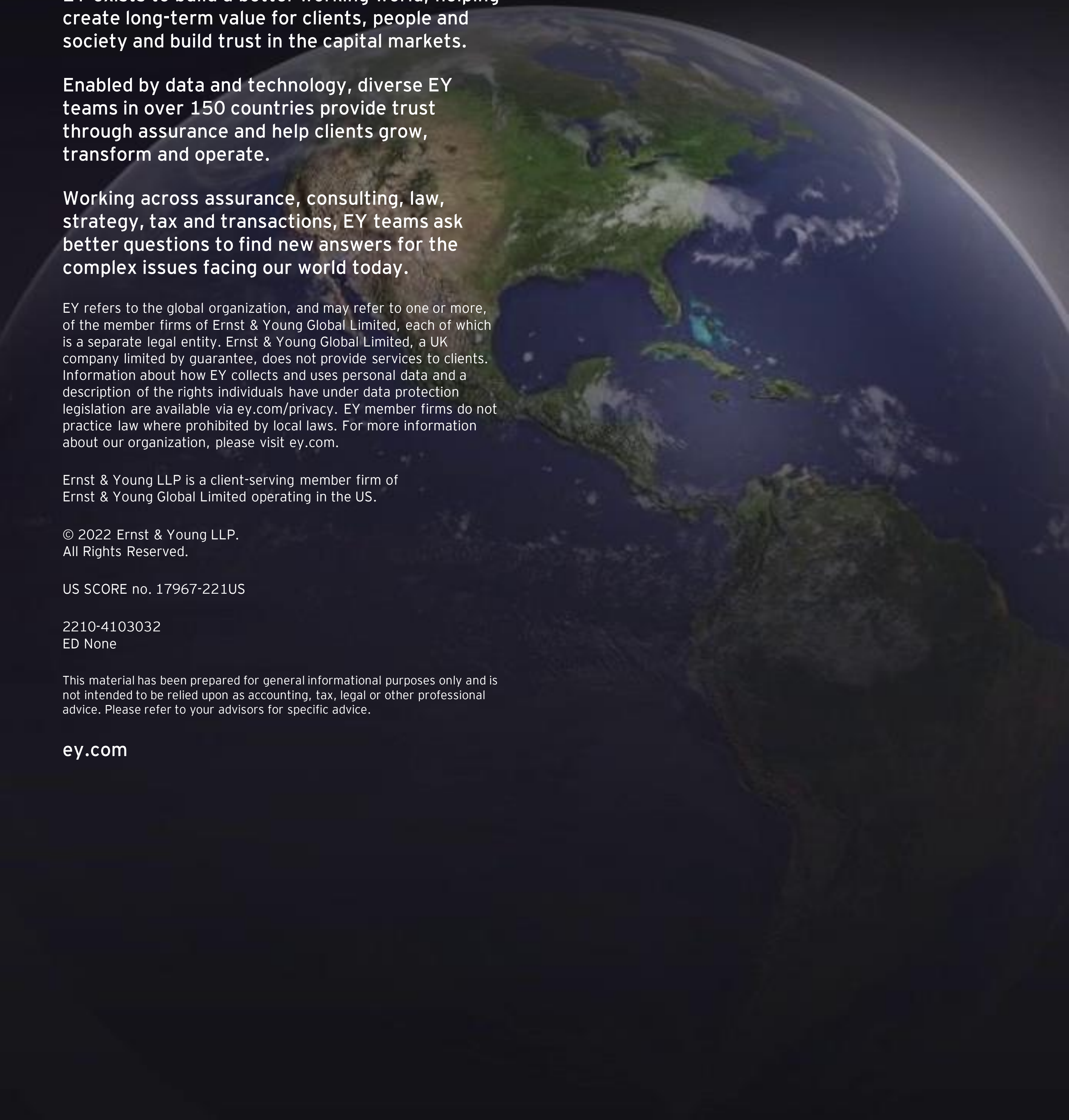
**Stephanie Danis**
Senior
stephanie.danis@ey.com

**Dmitriy Afanasyev**
Senior Manager
dmitriy.afanasyev@ey.com

**Theo Pu**
Senior
theo.pu@ey.com

**Rishikesh Muchhala**
Manager
rishikesh.c.muchhala@ey.com

**Harshad D. Kulkarni**
Senior
harshad.d.kulkarni@ey.com



## EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

US SCORE no. 17967-221US

2210-4103032
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com