Each year, the world grows more heavily digitized, and in a hyperconnected digital era, society will be critically dependent on technology to function. For companies to succeed in this world, security is clearly imperative — yet it’s only the foundation upon which trust, the ultimate enabler, is built. Do you trust the quality of data that you use for forecasting? Do you trust artificial intelligence and other technologies to help you make key decisions? Do your customers trust that your company will protect their data and deliver services without interruption?

59% of organizations have experienced a significant or material breach in the last 12 months, according to the EY Global Information Security Survey 2020.

### Hurdles in achieving trust

Companies today are confronting three factors that make technology trust a more rare commodity:

1. **High expectations.** CIOs must deal with a group of stakeholders — customers, employees, executives, suppliers and business partners — that want the right technology, right now, and they want it to be simple, fast and a perfect match for their needs. Matching business needs to the available tech options is increasingly challenging, and satisfying all the demands could require trade-offs.

2. **Pace of change.** Technology-enabled business transformations are no longer an event; most companies are undergoing one transformation after another or multiple transformations all at once. It also becomes difficult to maintain or source the skills necessary to achieve the desired business objectives.

3. **Complexity.** As companies implement newer technologies, complexity increases. Point solutions address a specific business need, but existing applications remain. Over time, more applications, supporting technologies and tools — and outsourced service organizations and vendors — may simplify the user experience, but a complex patchwork of interdependencies lurks behind the scenes.

At many companies, the challenges of high expectations, pace of change and complexity have resulted in rigid, outmoded technology architecture that is challenging to operate, maintain and change.
Trust brings confidence

In this highly dynamic environment, organizations will need to shift their focus from simply mitigating risk to embracing new opportunities. But the lack of trust creates friction, which slows down decisions – subverting the promise and potential of the Transformative Age. Too often, companies are responding to change with process requirements and controls after the fact, rather than considering them up front.

As you seek the confidence to make strategic moves and seize the upside of disruption, trust in systems, design and data positions your organization to take on more risk, intelligently. You may consider internal controls as a tool to prevent the worst, but they also allow you the strive for the best. Appropriately tuned internal controls, designed with trust in mind, serve as the net underneath your organization as its ambitions take off, and the brakes as your growth plans accelerate: the backstops you can rely on as you move forward.

The journey to trusted technology

Consider the following questions as you shape your technology trust framework:

**Are you taking just an inward, enterprise-focused view to build trust?**

Consider trust in the context of your business priorities and how cyber domain knowledge is uniquely applied within them. For instance, sometimes people are myopically focused on whatever tech is in their minds for the internal organization, when it can have implications for vendors across the supply chain. In an outward-looking approach to trust, you focus on influencing the dynamics of the whole, with accretive individual contributions of value and ideas, and greater standardization and integration through the security and the right transactional behaviors.

**Are you thinking about trust too late?**

Risk and control considerations need to happen at the onset of developing new products, evolving the customer experience and implementing new technologies. Transition from a “process, risk, control” framework to one with a focus on the product life cycle along with a connection to the customer journey. For example, when the experience of engaging with a customer changes, your security and how you engage with your business applications need to be considered differently as well. When you embed risk discussions in product and service design and operations, you position yourself to accelerate speed to market while sustaining trust.

---

**Are you balancing compliance and operations with disruptive innovation?**

Risk should be at the forefront of business strategy, beyond the context of just downside risks. Upside risk (the penalty of not seizing an opportunity) and outside risk (beyond your control, such as from your competitors or a natural disaster) pose crucial implications as well. Technology risk is often thought of purely in downside terms: you have architecture that needs to be secure. But the ability of the cyber organization to enable business innovation, and to operate capabilities based on how both threats and the industry evolve, will become the new measure of success.

Have you digitized risk intelligence, monitoring and reporting? Efficient risk operations keep pace with the business landscape while maintaining strong risk oversight and real-time risk intelligence to enable dynamic decision-making aligned with strategic priorities. This is key to driving trust – and preventing decisions made with unwarranted confidence because of data problems, with more risk than intended unknowingly accepted.

To learn more about technology trust and how to build it, begin your trust journey [here](#).