Digital Trust and the Audit Function

亦有中文简体译本
www.isaca.org/currentissue

Organizations at the forefront of digital security, reliability, data privacy and data ethics will be the leaders of tomorrow. Industry experts predict that the number of Internet of Things (IoT) devices will exceed 50 billion by the end of 2050,[1] with the global buildout of 5G networks acting as a catalyst. This trend indicates that more consumers and enterprises are going digital, which makes digital trust more important than ever.

With this ever-increasing use of and reliance on the Internet, big data and disruptive technologies, digital trust has become a necessity due to its ability to foster customer, partner and employee confidence in an organization's ability to protect, store and secure data and personal information.

With increasing volumes of personal data being transported across the Internet and between devices, concerns over trust have grown. Aside from issues of data ownership and transportation, there are challenges regarding the determination of those responsible for ensuring that data are accessed, delivered and stored securely.

Digital trust requires the confidence of users. Confidence in the brick-and-mortar world is usually built over time, but time functions differently in the digital world, where interactions are instantaneous and relationships can be fickle. Organizations often have one chance to gain the user's trust. One wrong digital interaction can cost them not only the dissatisfied user, but also the user's friends and the friends of those friends. Users have high expectations, as they should when entrusting organizations with their personal data.

While the old adage counsels that with great power comes great responsibility, its modern-day counterpart could be "With great amounts of data come great responsibility."

Audit can play a crucial role wherever digital trust is a value-adding differentiator. However, current auditing approaches using established auditing tools and methodologies may not be sufficient for building better digital trust.

Building trust requires an organization to demonstrate good privacy and security practices, good data integrity for high reliability, and ethical behavior in all online interactions. The audit function acts as assurance for the implementation of these practices.

Understanding the Digital Trust Ecosystem

The digital ecosystem has evolved from merely connectivity and collaboration and limited supply

GOPIKRISHNA BUTAKA | CISA, CDPSE, CEH, ISO 27001 LA

Is a manager of information systems audit at the State Bank of India (SBI), a Fortune 500 company with more than 22,000 branches worldwide. Apart from conducting various audits, which include IS audits, IT migration audits, and regulatory framework implementation audits, Butaka's work includes preparing and editing various policies for IT, cybersecurity and framework design. Butaka coordinates the technical price negotiation committee, IT strategy committee and audit committee board meetings and ensures their implementation. Butaka is also an author focused primarily on technology evolution and its impact on business and has contributed dozens of articles for SBI's in-house magazines on technology and management issues.

chain integration to a complex structure with a diverse range of business stakeholders, competitors and IT partners in a dynamic environment built on trust (**figure 1**).

The new ecosystem leads to increased opportunity, but it also comes with higher risk.

Perception of Digital Trust

Business models, technological enablers and consumer expectations have all undergone radical shifts because of the increasingly digital character of modern organizations. There is one constant that has not changed despite these quick shifts: the need for trust. As shown in **figure 2**, digital trust is a fundamental component for business growth, as it helps to meet expectations of the various stakeholders in the digital ecosystem. However, the perception of trust as a constant in the real world has not carried over to the digital world, where trust is malleable and subject to change. This is because in the digital world, trust is dynamic and depends on various dynamic factors such as type of transaction, time and regulatory rules.

The idea of digital trust must be comprehensive and multidirectional. It must also be multidimensional, applying to the digital experience, user behaviors, the digital environment and end-user attitudes.

Users have high expectations, as they should when entrusting organizations with their personal data.

To achieve high levels of digital trust, organizations must first earn the confidence of customers, investors, business associates, suppliers and regulators. Organizations should build their digital trust strategy on the concepts of transparency, privacy, control, reliability, security and accessibility to gain the confidence of all stakeholders.

Technology can only be relied on if it is safe, properly implemented and usable. Two main reasons people are wary of digitalization are lack of knowledge and security concerns. Growing skepticism over digital technologies can be attributed to the perception that they lack security, transparency and ethical foundations.

FIGURE 1

Business Ecosystem From a Trust Perspective

Digital trust is not just technology management; its focus is on maintaining confidentiality and integrity in all transactions and becoming more transparent.

Layers of Digital Trust

To understand digital trust, it is helpful to view it as a layered matrix encompassing five attributes (**figure 3**):

1. **Risk management (RM)**—Detecting, eliminating, mitigating and even controlling the impact of identified and unidentified risk
2. **Identity management (IM)**—Managing the identity of various stakeholders, including digital access management
3. **Privacy management (PM)**—Providing and ensuring safe control of the data of various stakeholders while providing digital services
4. **Security management (SM)**—Securing the IT infrastructure and data of various stakeholders from malicious attacks
5. **Business intelligence (BI)**—Using various types of data to extract meaningful insights and to make scientific predictions and impactful decisions

Combined, these attributes enable trust in people, processes and systems.

FIGURE 2

Significance of Digital Trust

Source: Adapted from ISACA®, "Understanding the Full Digital Trust Ecosystem," ISACA Now, 13 May 2022, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/understanding-the-full-digital-trust-ecosystem.* Reprinted with permission.

Role of Internal Audit in Digital Trust

For audit professionals in the enterprise world, the digital revolution has significant ramifications. The way audits are conducted is influenced by changing business models, the digitization of enterprise activities, and increased reliance on the capacity of auditors to collect, compile and evaluate vast amounts of detailed digital information.

Organizations are evolving as they go digital to resemble more fluid ecosystems with updated value chains and critical components supplied in real time from outside service providers. Across business-to-business (B2B), business-to-consumer (B2C) and business-to-business-to-consumer (B2B2C) enterprises, distribution channels are expanding and diversifying. The ability to integrate trust into these ecosystems is crucial (**figure 2**).

The future boundaries of the audit's scope are likely the largest unknown. With the digital trust transformation, the audit is no longer limited to checks and controls, but can also function as a mechanism for assurance. In the future, it may become a normal practice to use the audit to validate business logic.

Audit will play a vital role in achieving digital trust. As the growth of organizations demands more sophisticated technology and robust systems, the audit system and auditors should be a step ahead to effectively monitor and provide valuable insights. Audit reports act as enablers for digital trust by assuring that appropriate digital processes are in place.

For example, AI and automation increase risk to trust, as stakeholders often may not have faith in emerging technologies. The trust gap can be filled by an audit mechanism, which provides assurance that all the checks and controls are in place for the processes.

> Digital trust is not just technology management; its focus is on maintaining confidentiality and integrity in all transactions and becoming more transparent.

Widening the scope of the internal audit mechanism can position audit as an enabler of digital trust. Certain businesses may require audits for business requirement document (BRD) logic implementation and logic validation to gain the trust of various stakeholders. More audits and more auditors are

required to ensure digital trust in several organizational processes outside the cybersecurity area.

Achieving Digital Trust Through Audit and Assurance

Data-driven procedures have the potential to improve trust and boost confidence in the auditing process by, for instance, guaranteeing the confidentiality and privacy of data collected and used by an inspected organization. By conducting audits that are more data-driven, auditors will be able to explain how they arrived at their judgments, giving stakeholders much more transparency.

The way an audit is conducted must be clear. Auditors must explicitly record what data they assess, the checks they perform, the procedures they follow and the technology they use. Further, auditors must demonstrate—through their knowledge of standard tools, their professional attitudes and the quality of their audit reports—that their assessment makes the system more trustworthy. Only then will there be an increase in trust.

Relying too heavily on technology to conduct an audit is risky. Technology may unquestionably increase an audit's efficiency and accuracy, but it cannot be expected to take the place of an experienced auditor's professional judgment. The procedures established by the audit teams must be strong enough to counteract the possibility of technological failure.

To assist organizations in addressing the new difficulties associated with internal auditing, such as Agile environments, use of new technologies and changing regulatory scenarios, audit functions must be geared toward a digital-first strategy that adapts to the requirements of a hybrid work organization with a distributed workforce. Many organizations have adopted hybrid work due to the COVID-19 pandemic.

Managing digital risk and achieving compliance have become even more crucial in today's evolving regulatory landscape, because just a few failures with regulatory compliance can lead to significant losses from reputational damage, customer defection, declining market valuation and regulator-imposed fines. Therefore, it is critical for enterprises to improve controls over their digital ecosystems to appropriately mitigate risk and function reliably. These goals can be achieved by putting in place a robust audit system that emphasizes digital trust.

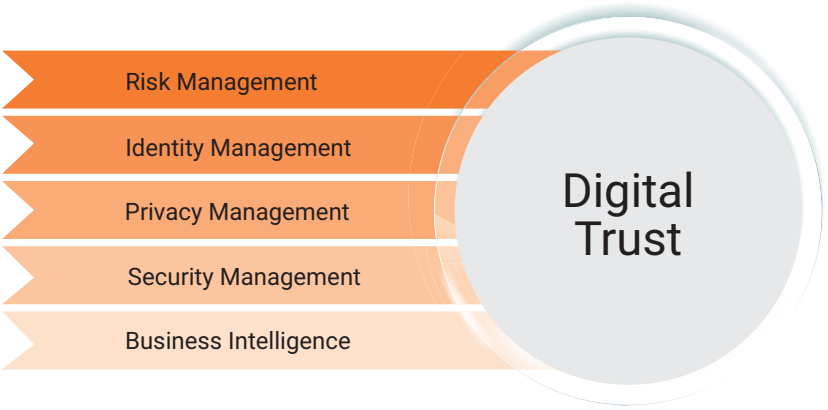
By conducting audits that are more data-driven, auditors will be able to explain how they arrived at their judgments, giving stakeholders much more transparency.

Some of the qualities and skill sets that go a long way toward helping auditors strengthen digital trust in an organization are:

- Passionate interest in the digital trust topic, curiosity about consumer-to-government (C2G), consumer-to-business (C2B) and B2B digital trust service and operating models
- Ability to play a consultative role when new processes are being rolled out or existing processes are being modified so that a business can have confidence in the actions it is taking
- Ability to help build a proactive compliance culture by staying up to date on compliance requirements for relevant global privacy and data protection rules and regulations
- Familiarity with behavioral analytics, biometric security and other tools for managing distributed trust
- Expertise in auditing cloud computing environments and automated data infrastructures as cloud storage has become the norm for storing vital information
- Ability to provide market confidence through transparency of the control ecosystem

FIGURE 3

Layers of Digital Trust



ENJOYING THIS ARTICLE?

- Explore the Digital Trust Ecosystem Framework. *www.isaca.org/digital-trust*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- Ability to provide cross-skill training on various technology processes
- Ability to provide valid enablers for digital processes and controls
- Ability to play an active role in imparting digital trust training to all staff
- Ability to assist in new areas such as control of emerging technology risk
- Ability to analyze various categories of digital risk and assess their impact
- Ability to act as digital confidence enabler by creating value through the improvement of trust in digital capabilities and thereby closing the skills gap
- Knowledge of qualitative and quantitative culture assessment techniques apart from the traditional audit methods
- Advocacy of a co-creation approach for designing critical cybersecurity and data governance strategies
- Ability to coordinate with first- and second-line roles (Though an independent audit is important, it should not be isolated from the other two lines. Coordination among the three lines improves the effectiveness of cybersecurity risk audits, contributing to digital trust.)
- Ability to provide valuable inputs during the creation of data and compliance-related frameworks
- Ability to collaborate well with other digital trust professionals in pursuit of constant learning and updating
- Ability to engage with stakeholders and provide assurances of complicated processes and promote best practices regarding governance of emerging technologies
- Efficiency in carrying out audit and compliance tasks
- Ability to periodically evaluate digital projects and report potential threats
- Coordination of various audit teams to mitigate the risk presented by emerging technologies
- Knowledge of emerging technologies' governance and audit advancements
- Ability to act as digital assurance specialists by delivering technology assurance services including cybersecurity assessments and other emerging technologies
- Ability to perform data audits with a focus on data completeness and data loss prevention
- Ability to perform data quality assessments
- Knowledge of the various automated tools that help analyze anomalies in data and offer remedies
- A thorough understanding of data collection, storage and use processes

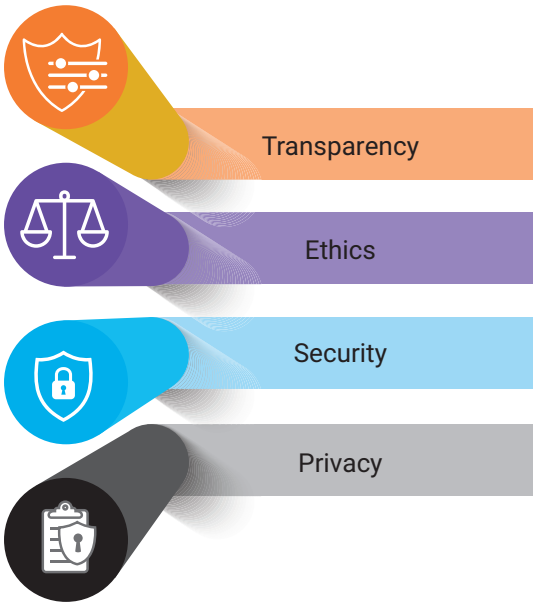
Designing a Digital Trust Framework

Organizations may lose customers because they do not have a strong digital trust program in place. Therefore, the use of a digital trust framework is essential. The framework should be based on four suggested pillars of digital trust: transparency, ethics, privacy and security (**figure 4**):[2]

1. **Transparency**—As enterprises push more transactions onto a digital platform, customers and other stakeholders expect transparency because they want to understand how their transaction and personal data are processed and stored.
2. **Ethics**—In this digital world, the trust of a customer and other stakeholders can be earned by an organization demonstrating ethics and morals. Organizations should align their digital transactions and operations with their ethical standards.
3. **Privacy**—Privacy has become a mandatory design component of every digital product and process. There is a disparity between what customers think they are providing their data for during transactions and for what purposes an organization actually

FIGURE 4

Four Suggested Pillars of Digital Trust



uses that data. The terms of agreement of the organization should be implemented more strictly to ensure that there is no unauthorized use of customer or stakeholder data. Privacy protection and assurance to customers that their data are kept confidential go a long way toward building digital trust.

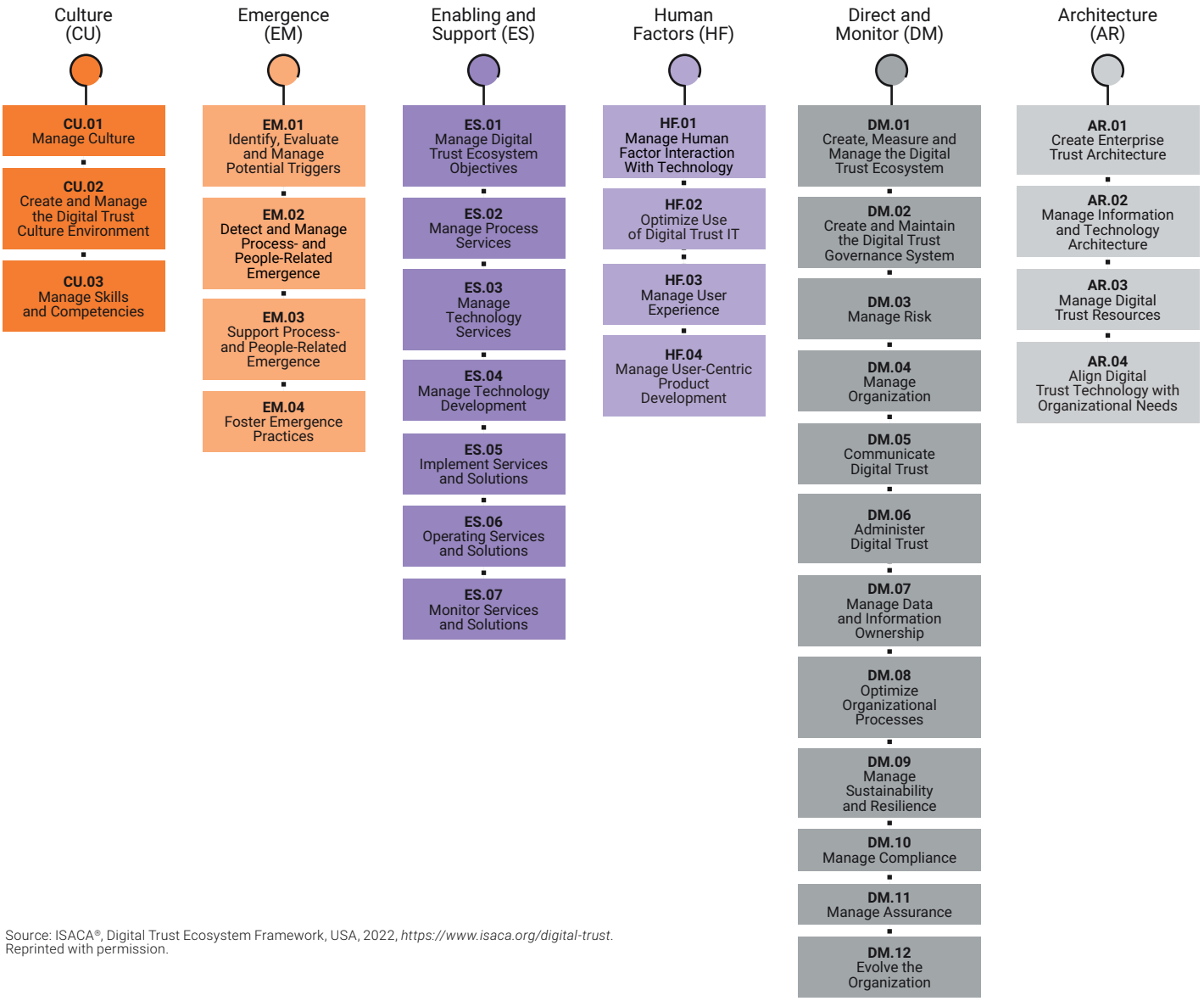
4. **Security**—Security has become the most vital pillar for all digital transactions, forcing organizations to build a robust and reliable digital security ecosystem. Organizations cannot afford any security breaches and lapses, as a security incident can no longer be hidden from customers and stakeholders, and will impact business negatively. Organizations need to demonstrate strong security by applying relevant standards and good practices.

Digital Trust Framework and the Auditor

As digital trust is still an emerging concept for many organizations, auditors can proactively help implement a digital trust framework.

FIGURE 5

Digital Trust Framework



Source: ISACA®, Digital Trust Ecosystem Framework, USA, 2022, *https://www.isaca.org/digital-trust*. Reprinted with permission.

The foundation of digital trust is a combination of trustworthy systems, high-quality business performance and efficient design and monitoring procedures.

Figure 5 shows the domains and trust factors included in ISACA's Digital Trust Ecosystem Framework (DTEF), which can be used as a baseline for organizations with the ability to customize it to their needs as required.[3]

The framework is indicative and based on the nature of the business. Organizations can build the framework in various permutations and combinations of parameters, subparameters and classifications.

Conclusion

Future generations are certain to place increasing demands on organizations to gain their trust to do business with them. Organizations must lay foundations for trust building while recognizing the inherent complexities and uncertainties involved in the effort. All stakeholders in digital transformation are currently in extraordinarily powerful positions, with the ability to play roles in changing the conversation on digital trust and contributing to a more digitally trustworthy tomorrow.

In the quest to achieve a future that gauges success by digital trust, there is a constant need to track developments in digital ecosystems (networks of stakeholders that digitally connect and interact to create value). To understand a digital ecosystem, it is necessary to embrace the latest technologies.

A technology audit is key to ensuring digital trust among stakeholders through assured transactions. Building a future in which digital trust is a solid component of an established business model requires dedication to ensuring that customers are confident when entrusting their data to an organization. Working toward digital trust requires the inclusion of a robust audit structure and a sound understanding of the underlying digital trust framework described herein.

Internal audits will be vital to the ethical development and implementation of automated and intelligent technologies. Intelligent systems should be developed with digital trust built in from the very beginning rather than as a response to a later audit. The foundation of digital trust is a combination of trustworthy systems, high-quality business performance and efficient design and monitoring procedures.

Because digital trust is an increasingly important driver of consumer decisions, it is essential to maintaining business resilience in the digital era. It will only become more vital in the future.

Endnotes

1 Ericsson, "Why IoT Changes Everything," *https://www.ericsson.com/en/internet-of-things*

2 Jain, S.; "What Is Digital Trust and Why It's Important," Engati, 6 October, *https://www.engati.com/blog/what-is-digital-trust-and-why-its-important*

3 ISACA® has developed a Digital Trust Ecosystem Framework based on systems theory. It is another way to look at digital trust and how to measure it. ISACA, Digital Trust Ecosystem Framework, USA, 2023, *https://www.isaca.org/digital-trust/digital-trust-ecosystem-framework-interest*