2018 ISACA DIGITAL TRANSFORMATION BAROMETER

MANAGE RISK TO ENABLE TODAY'S TRANSFORMATIVE TECHNOLOGIES

AN ISACA RESEARCH REPORT

ISACA®

Mitigating Risk to Drive Digital Transformation

Nineteenth-century naturalist Charles Darwin was famous for using the phrase "survival of the fittest" in his seminal work, *On The Origin of Species*. But what if Darwin had worked in the 21st century—PC on his desk, mobile device in his pocket? Perhaps he would be talking instead about "survival of the most digital."

In recent years, many organizations have approached survival—as well as growth, efficiency and effective customer engagement—through a digital lens. This desire to succeed has led organizations to communicate, collaborate and do business digitally.

Yet, too many organizations are ill-equiped to do so. They began life with a paper-based, brick-and-mortar set of business processes. There are, of course, other organizations that were formed in the digital era. But taken together, both types of organizations largely now embrace digital transformation aimed at improving the customer experience, creating new revenue streams and gaining an advantage in increasingly competitive marketplaces.

Attributes of the Digital Transformation Journey

It's not easy to transform organizations or business processes. The journey requires brave leadership, an adaptable culture and financial investment. Indeed, globally, according to International Data Corporation, an IT researcher based in the US, the total size of the digital transformation market will reach US $1.3 trillion in 2018.

These days, many leaders, eager to survive and thrive, want to embrace change, alter their culture and make the requisite investments to become "the fittest." But what is the profile of these leaders, how do they behave, and when do they actually succeed?

The 2018 ISACA Digital Transformation Barometer, a survey with responses from 5,847 ISACA members, demonstrates that those ***organizations that are ahead of the digital transformation curve tend to be those that are less risk-averse when it comes to considering, testing and adopting emerging, transformative technologies.***

"Not every new technology is the right fit for every organization, but enterprise leaders owe it to their stakeholders to ensure they are actively exploring promising technologies and determining how technology can be securely leveraged to drive the innovation needed to compete in today's digital economy," says Rob Clyde, CISM, NACD Board Leadership Fellow and ISACA Board Chair.

This ISACA research, now in its second year, examines the complicated dynamics of:

- **Digital transformation management**
- **Executive digital literacy and its effect on emerging technology adoption**
- **Organizations' embrace or avoidance of digital risk and security**

ISACA's 2018 Digital Transformation Barometer shows that among many markers, there are three key technologies that may demonstrate how—and with what degree of risk and success—an organization embraces digital transformation. These technologies are: 1) the utilization of big data, 2) artificial intelligence (AI), and 3) public cloud adoption.

For many organizations, testing and implementing new technologies can be painful. Yet those organizations that embrace transformative technologies often are more equipped to tackle the challenges of ever-changing customer requirements, rapid business innovation and fluid market demands.

SECTION 1: **THE CURRENT STATE OF DIGITAL TRANSFORMATION**

The good news is that more than nine in 10 respondents in the ISACA research said they are involved in some kind of transformation effort. Where a particular organization finds itself on the spectrum between just getting started and completion of the journey is, of course, a matter of self-interpretation. The average respondent, on a scale of 1 percent to 100 percent complete, described his or her organization as 42 percent transformation achieved.

The study reveals fairly dramatic differences in how digital transformation progress is measured. Much depended upon whether the respondent believed that his or her organization experienced challenges integrating or deploying emerging technologies.

Ironically, those who have experienced significant challenges indicated that they were a solid 64 percent of the way along their digital transformation journey. Those who said they had experienced no challenges were only 36 percent of the way there. It's the epitome of the expression: no pain, no gain.

HALFWAY TO DIGITAL TRANSFORMATION

Percentage of plan completed

Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

Executive Buy-in Helps Organizations Remain Committed

Having senior executive buy-in undoubtedly helps these early adopters remain committed to pursuing business transformation, even when integration strains resources or patience. Adoption issues aside, emerging, transformative technologies also are viewed as the nexus of digital transformation investment activity.

The Digital Transformation Barometer study asked which leading emerging technology stood the greatest chance of delivering the most transformative value to their organizations. The leaders? Big data at 28 percent, followed by AI/machine learning/cognitive tech at 25 percent, public cloud at 18 percent, IoT at 12 percent and blockchain at 8 percent.

Indeed, the research also demonstrates that those organizations that are furthest along in terms of testing and adoption regard themselves as well-advanced on their digital transformation journey. Yet, importantly, many organizations remain concerned about the security of adopting and integrating new technologies.

SECTION 2: **UNDERSTANDING TRANSFORMATIVE TECHNOLOGIES**

Before assessing risk and security implications, organizations need to understand why a particular emerging technology may fuel its digital transformation. It's no surprise that big data, AI (including machine learning), and public cloud adoption lead the pack.

Each of these three transformative technologies can help organizations innovate, better engage with customers and operate more efficiently.

BENEFITS OF BIG 3 TRANSFORMATIVE TECHNOLOGIES

BIG DATA describes large data sets that may be analyzed to reveal patterns, trends and associations. Applications include managing road traffic patterns, understanding consumer behavior, drug discovery and loan processing.

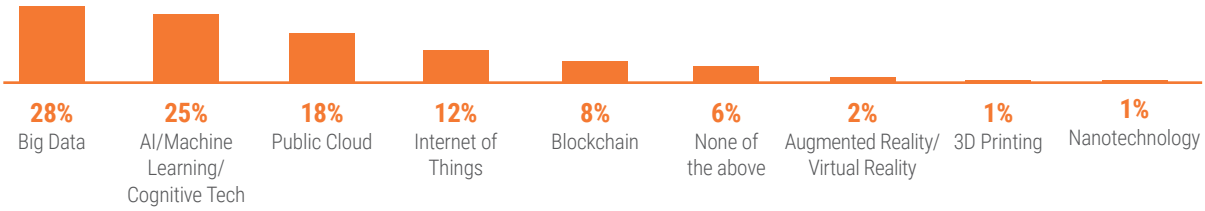
ARTIFICIAL INTELLIGENCE—bolstered by machine learning—allows organizations to learn and interact much faster than workers or customers can themselves. AI is used in sectors as varied as marketing, manufacturing, financial services, medicine, healthcare, energy exploration, government, entertainment (particularly sports) and retail.

PUBLIC CLOUD is an approach where computing is made available as a service to organizations (or individuals). Organizations tend to use the public cloud for non-strategic applications, such as sales (customer relationship management), human resources or the fast "spinning up" of resources for application development.

We see how AI, big data and public cloud have become the "Big Three" when it comes to the *perception* of which technologies will transform organizations. But it's critical to understand how each is perceived when it comes to delivering *value* to the organization.

TECHNOLOGIES THAT HELP DRIVE TRANSFORMATION

Which emerging technology stands the greatest chance of delivering transformational value to your organization?



Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

At the same time, it's important to consider which of these (and other) technologies organizations are testing and which they intend to deploy. For instance, close to half of all survey respondents say they intend to test the public cloud (46 percent) and big data (45 percent).

AI and IoT were mentioned by three in 10. And when it comes to intent to deploy, the big three also stand out among other emerging technologies: big data (36 percent), public cloud (33 percent) and AI (27 percent).

AI is a unique case because of the extent to which testing and intent to deploy skyrocketed between ISACA's 2017 and 2018 Digital Transformation Barometer surveys. In just one year, the proportion of AI testers grew by a half; the proportion of organizations intending to deploy AI grew by 35 percent.[1]

"Organizations should consider how they would alter their business design by putting AI at its core," says Richard Jhang, founder/CEO of StratMinds. "This will help them frame how to approach AI strategically, going beyond short-sighted, opportunistic ideas."

SECTION 3: **ORGANIZATIONAL RESISTANCE**

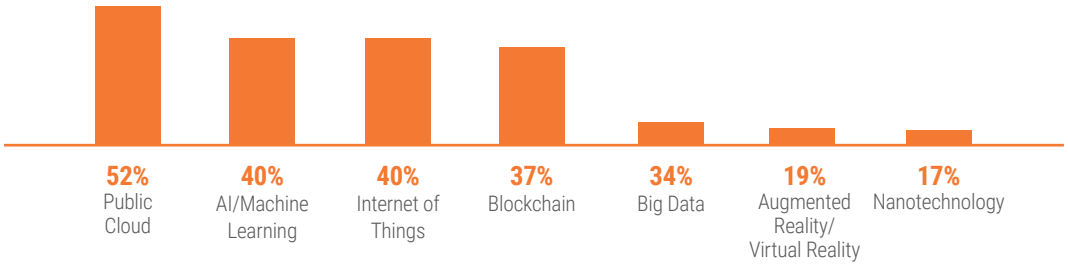
Testing is no guarantee that an organization will embrace the utility of emerging technologies. Although AI, big data and public cloud are good barometers of progress when it comes to digital transformation, their testing and deployment often are met with organizational resistance and internal pushback.

More than half of the surveyed organizations said that the public cloud faces organizational resistance; about four in 10 said the same about AI and IoT; and more than a third report experiencing resistance to blockchain and big data.

Those organizations that work through cultural or integration concerns and proceed with testing a particular emerging technology tend to be further along on the digital transformation journey than those that don't make that leap of faith or the investment in beta testing.

NEW TECH PUSHBACK

Which emerging technologies face the greatest organizational resistance?



Note: Multiple responses allowed
Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

As a case in point, let's examine the profile of organizations that say they are testing AI. Within this group, nearly three in four also are big data testers, and more than six in 10 are public cloud testers.

Interestingly, just because one organization fails to embrace one technology doesn't mean it eschews the others. For example, among non-AI testers, the appetite to explore other transformative technologies remains surprisingly strong: 64 percent for public cloud and 63 percent for big data.

That means we have to dig deeper to understand the relationship between key emerging technologies and where a particular company may be on its digital transformation path. It turns out that factors such as perceived executive digital literacy and organizational views about the risk of deploying a technology provide an even clearer indication of the extent to which an organization has advanced its digital transformation agenda.

SECTION 4: **THE CONTINUING IMPACT OF DIGITAL LITERACY**

When analyzing the results of the 2017 ISACA Digital Transformation Barometer Survey, we noted that organizations that perceive their leadership to be digitally literate—meaning they have a solid understanding of the technologies, their benefits and their risks—are more receptive than other organizations to evaluating and adopting emerging technologies in their pursuit of digital transformation.

Between 2017 and 2018, there was little change in the proportion of respondents who described their leadership as being digitally literate: 53 percent in 2017 vs. 54 percent this year. ***Receptivity to adopting all emerging technologies is far greater among organizations with digitally literate leaders*** (96 percent for very or moderately receptive in 2018) compared with other executives (55 percent for very or moderately receptive.)

DIGITALLY LITERATE-LED ORGANIZATIONS EMBRACE TRANSFORMATIONAL TECH

Which technologies do organizations plan to deploy within the next year?

Note: Multiple responses allowed. "Digitally literate" refers to organizations where leaders are perceived to possess that expertise.
Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

Across the board, those organizations that believe they have digitally literate leaders anticipate less resistance within their organizations to emerging technologies, compared with organizations led by less digitally inclined executives. Those organizations that do not believe they are led by digitally literate managers are significantly more likely to resist deployment.

When analyzing individual technologies, respondents with digitally literate leaders were more likely to say they would deploy new technologies in the coming year. Organizations with well-versed digital leaders are nearly twice as likely to deploy AI within the next year and slightly more likely to deploy big data than other organizations.

SECTION 5: **HOW ORGANIZATIONS PERCEIVE AND MITIGATE RISK**

While digital literacy helps us to understand whether an organization may deploy an emerging technology, it's also important to note how organizations perceive and manage risk. The way in which an organization deals with risk, it turns out, correlates with the extent to which that organization adopts emerging, transformative technologies.

Of course, to leverage any new technology, organizations must embrace some amount of risk. For instance: Nearly half of all organizations perceive the public cloud as presenting only medium to low risk. For IoT, that proportion grows to nearly six in 10. And nearly three out of four organizations say that AI adoption presents only medium or low risk. Still, for most enterprises, failure is not an option.

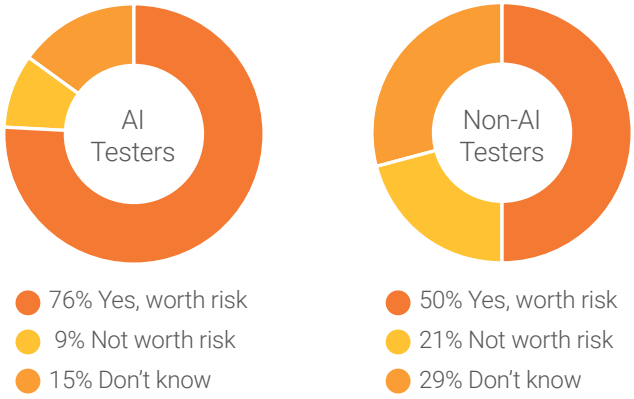
Organizations' reactions to the risk of embracing emerging technologies are influenced by their cultural history and experience. Organizations that have had significant challenges integrating or deploying a particular technology, in order to fuel the digital transformation journey, are far more likely to perceive that technology as risky. Once bitten, twice shy.

The perception that a technology may be considered high risk drops substantially in organizations with digitally literate leaders. For instance, about a quarter of organizations with digitally literate leaders consider AI to be high risk while, for other organizations, the perception of high risk is greater, at one-third.

For their part, AI testers—those with experience when it comes to working with the technology—are far more likely to say that implementing AI technology is worth the risk.

TECH FAMILIARITY BREEDS WARMER EMBRACE

Is AI/Machine Learning Worth the Business Risk?



Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

SECTION 6: **BALANCING SECURITY AND DIGITAL TRANSFORMATION**

We've seen that there is a significant difference between those that have experienced challenges integrating new technologies and those that have not. It is instructive, once again, to examine AI to illustrate the point.

We saw previously that those organizations that said they experienced significant challenges considered AI to be "high risk." Still, there are two possibilities: either the perception of high risk means that organizations are less likely to implement AI. Or the opposite may be true.

Familiarity can create better understanding of a technology. And the intelligent use of security policies, practices and technologies make it *more* likely that an organization will use a technology such as AI.

SECURING TRANSFORMATIVE TECHNOLOGIES CHECKLIST

When testing or implementing transformative technologies, consider the following security and management checkpoints:

For Any Emerging Technology

- ❑ Remember to **train IT and business staff**—and in some cases customers and contractors—with regard to responsibilities and how to mitigate threats. In many cases organizations will need to budget more for training than they have previously.
- ❑ Create an **internal communications plan.**
- ❑ Create contingencies for any **external communications**, especially in light of a breach.
- ❑ "Automate everything"—Try to **automate** as much of the staging, testing, security and audit validation, configuration checking, deployment, and other elements of the systems using the technology. This will reduce human error, allow for more rapid updates to meet customer needs, and improve security. Strongly consider implementing **DevOps** to do this.

For Public Cloud Implementations

- ❑ Define **roles and responsibilities** for yourself and from the service provider, especially with regard to downtime and breaches.
- ❑ Remember to **outline formal Service Level Agreements (SLAs)** for vulnerability scanning, patches, backup, breach notification, data backup.
- ❑ Ensure that all configurations, including at the **virtual machine and container** level, are properly scanned and hardened.
- ❑ Outline **compliance and audit** governance and procedures.
- ❑ Pay attention to the **virtual network**: switches, routers, firewalls.
- ❑ Implement a system for **information management** when it comes to migration, storage and deletion.
- ❑ Ensure that **admin accounts** are properly secured with more than just user name and password (i.e., use two factor authentication). Those accounts will be the prime target for attackers.
- ❑ Some admin actions should require secondary approvals to ensure that production systems are not accidentally or deliberately disrupted. For example, a single admin should not be able to delete all off the production workloads in VMs and containers without secondary approval.
- ❑ Consider using **DevOps** as a method to deliver applications to the software environment. Include appropriate security and audit tools and automation in the continuous improvement (CI) and continuous delivery (CD) pipelines.
- ❑ In the event of issues after a software update, provide the ability to quickly roll back to an earlier known good application with the push of a button.
- ❑ Have a **dashboard** that shows the **KPIs** for the current state of the public cloud applications, including sufficient log information to ensure that problems can be quickly and easily detected and addressed.

For Artificial Intelligence Implementations

- ❑ **Connect your AI goals** with corporate and IT governance and cybersecurity.
- ❑ **Understand data inputs** for decisions that may be made with AI systems.

- ❑ Be sure that in regulated markets (healthcare, financial services, any PII consumer information) you account for national and international **regulations and privacy rules**.
- ❑ Implement the ability to **trace an answer** back to an original dataset or document.
- ❑ Consider the use of **natural language processing** algorithms, which help decipher meanings and extract data based on context.
- ❑ Understand and audit the way that AIs train and self-learn.
- ❑ Determine how to test the integrity and security of AIs you use. Consider the use of one AI to test another.

For Big Data Implementations

- ❑ **Inform stakeholders** about projects.
- ❑ **Define governance and policies** around data, processes and systems.
- ❑ Ensure **alignment between security and operations** for those building and managing data lakes.
- ❑ Include internal and external **privacy rules** and ensure that constraints are part of your big data project.
- ❑ Be sure that in regulated markets (healthcare, financial services, any PII consumer information) you account for national and international **regulations and privacy rules**. This not only includes data you store, but the results that come from **big data analysis**.
- ❑ Build a **risk mitigation plan** in case there's a breach.
- ❑ Include security in your **dashboards and KPIs**.

AI testers, for instance, may feel that AI is high risk, but better than three in four of them say that it is "worth the risk." And the proportion among non-AI testers? Only one-half say that AI is worth the risk.

So what is that risk, according to the ISACA survey respondents? Both AI testers and non-AI testers say that manipulating media content, social engineering, data poisoning and political propaganda pose the greatest threats from maliciously trained AI.

So does that make these organizations gun-shy about adopting a transformative technology such as AI? Hardly. What's important is the degree of confidence an organization has that it can assess the security of systems based on AI. On that front, there is much work to do, as only 40 percent of respondents expressed confidence that their organization can accurately assess the security of systems based on AI and machine learning.

"Enterprises must make the needed investments in well-trained staffs capable of putting AI safeguards in place," says ISACA's Clyde. "As AI evolves—consider the likely proliferation of self-driving vehicles, or AI systems designed to reduce urban traffic—it will become imperative that enterprises can provide assurance that the AI will not take action that puts people in harm's way."

UNDERSTANDING HOW AI AFFECTS SECURITY

Can your organization confidently assess the security of systems based on AI/Machine Learning?

Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

We can only conclude that the more exposure an organization has to a transformative technology such as AI, the greater the likelihood that the organization has implemented the kind of security systems and protocols required to safely adopt the technology.

Still, it's clear that some organizations fail to view digital transformation as a team effort. "Today, many of the digital transformation efforts are driven by the business owners with security and IT teams involved as an afterthought," says Mike Wons, chief client officer at PayIt. "That unfortunately puts cybersecurity and risk on the backburner and often exacerbates the risk introduced by some of these new technologies."

Organizations that can elevate security to a business enabler rather than view it as a hindrance may hold the key to unlocking digital transformation success.

SECTION 7: **SIZE, INDUSTRY AND REGIONAL VIEWS**

Of course, nothing is standard when it comes to emerging technology adoption or identifying where companies find themselves on the digital transformation path. Different industries and regions of the world vary in how these technologies are being explored and implemented.

For instance, there are more plans to adopt AI and machine learning in Europe and Asia than in the rest of the world. Big data is slightly more popular in Europe and Latin America. And the public cloud will become slightly more popular in Oceania, North America and Europe than it will be elsewhere over the next year.

TRANSFORMATIONAL TECHNOLOGY ADOPTION

Do you plan to deploy AI, Big Data or Public Cloud in the next 12 months?

Regional Snapshot

	AI/Machine Learning	Big Data	Public Cloud
Africa	15%	36%	26%
Asia	32%	37%	32%
Europe	33%	41%	34%
Latin America	22%	45%	31%
Middle East	19%	32%	31%
North America	23%	33%	35%
Oceania	28%	36%	41%

Industry Snapshot

	AI/Machine Learning	Big Data	Public Cloud
Financial/ Banking	30%	39%	29%
Tech Services/ Cons.	32%	33%	37%
Government/ Military	12%	32%	38%

Note: Multiple responses allowed
Source: ISACA's 2018 Digital Transformation Barometer Study of 5,847 members

It's likely that these regional differences occur because of organizations' differing experiences working with the technologies in different geographies. Examining tech adoption in different industries illustrates a similar point.

Public cloud adoption is lower in financial services than in the technology services and government sectors. Conversely, the data shows that financial services and technology services/consulting companies both convey more confidence about the security and utility of AI and machine learning.

Kris Seeburn, an independent technology consultant and the ISACA International Organization of Supreme Audit Institutions (INTOSAI), Working Group on IT Audit (WGITA) Liaison, explains the appeal of digital transformation to enterprises in the financial services sector. "Machine learning and advanced analytics are enhancing risk monitoring, controls and risk mitigation across the banking industry," says Seeburn. "Banks are able to leverage expanded internal and market data to better understand key customer and financial transaction-related risk factors."

The 2018 ISACA Digital Transformation Barometer Survey also demonstrates the effect of organization size on intent to adopt in the next year. Larger organizations generally have more resources to test, secure and monitor emerging technologies. Taking AI as an example, smaller organizations, which for purposes of this study have 1,499 or fewer employees, rank AI and machine learning fourth in terms of intent-to-adopt in the next year, after public cloud, big data and IoT. But at least one-third of larger companies say that they intend to deploy big data, public cloud and AI in the next year (in that order). That's most likely true because they have resources available to both test and integrate the technologies.

SECTION 8: **HOW TO FUEL DIGITAL TRANSFORMATION**

Nothing remains static in the realm of digital transformation, especially as more leaders within organizations gain digital literacy. Although this growth is incremental, we expect to see more organizations begin testing and assessing technologies that they may perceive as being risky. Information gleaned from testing is the currency they use to make informed adoption decisions.

A regional look at this year's data compared with last year's demonstrates this point. Among Europeans, the appetite to deploy AI more than doubled over the past year, from 14 percent of survey respondents in 2017 to 33 percent in 2018. For North Americans, the increase was even more dramatic; 8 percent of respondents last year intended to deploy AI. Today, the proportion is 23 percent—a nearly three-fold increase.

The increases for other technologies were equally dramatic. One of the biggest jumps was for big data in Latin America (25 percent to 45 percent). And in Europe, public cloud adoption nearly doubled from 2017 to 2018 (18 percent to 34 percent). Increasingly, organizations in these areas of the world see smart, measured, tested adoption as critical to digital transformation and business success.

The organizations around the world that focus on risk mitigation—through digital awareness, sound governance practices and testing—will accelerate their digital transformation efforts.

Secure, measured testing and adoption is critical for organizations to reap the rewards of emerging technologies and digital transformation. No organization can stand still. It is truly survival of the digitally fittest.

About ISACA's 2018 Digital Transformation Barometer Research

The ISACA Digital Transformation Barometer research, conducted in the first quarter of 2018, includes survey responses from 5,847 information technology, security and business executives, managers and professionals from a wide range of industries, company sizes and global locations, including Africa, Asia, Europe, Latin America, Middle East, North America and Oceania. Results can be found at www.isaca.org/digital-transformation-barometer.

[1]Proportion of organizations testing AI in 2017 was 20 percent; in 2018 it is 30 percent. Proportion of organizations intending to deploy AI in 2017 was 20 percent; in 2018 it is 27 percent.