Deloitte.

Future of risk in the digital era

Transformative change.
Disruptive risk.

Contents

Overview

Digital technologies are ushering in a new era and driving transformative changes in every industry, as organizations adopt these technologies to redefine how they create, deliver, and capture value. Identifying, understanding, and addressing new risks associated with digital transformation will help businesses derive more value from their efforts in the future.

What's more, understanding how digital transformation can be applied to risk management will enable organizations to take a more balanced view of digital technologies as both a source of risk and a way to manage risk.

As your organization embarks on its digital journey, we invite you to learn more about the evolving risk landscape and new opportunities to better manage risk.

Key trends:
Emergence of new risks and the evolution of existing risks

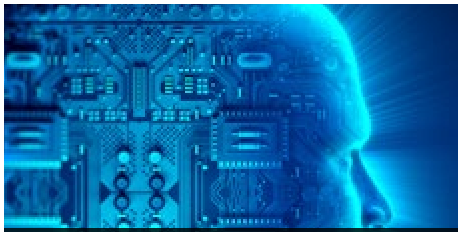
We're witnessing massive investment in digital transformation across industries. An IDC study of worldwide spending on digital transformation estimated more than $1 trillion will be spent in 2018.[1] This spending is driven by a proliferation of new digital technologies and a fear of disruption by tech-enabled competitors. Many organizations have been quick to not only update their technology infrastructures but also transform their operating models, customer engagement models, and even fundamental business models.

Organizations understand that digital transformation can capture new growth opportunities while heading off the threat of disruption. These same organizations soon learn that emerging technologies create new risks that they haven't encountered before and also add complexity to existing risks. The interconnected nature of these risks creates a need to tackle them concurrently, rather than in isolation. Those who hope to capture the full value of their digital investments need new approaches to how they view risk, manage risk, and harness risk for growth.

We see nine key trends shaping risk in the digital era.

[1] IDC, "Worldwide Spending on Digital Transformation Will Soar Past $1 Trillion in 2018," Press release, June 12, 2018, https://www.idc.com/getdoc.jsp?containerId=prUS43979618.

Managing the black box of artificial intelligence



The use of artificial intelligence (AI) techniques and solutions for a wide range of novel use cases leaves organizations open to new AI risks.

Evolving governance and controls for automation

Operating environment changes driven by the adoption of automation technologies call for redefined governance mechanisms and operational controls.

Protecting against the changing cybersecurity risk landscape

In order for digital technologies to deliver on their immense promise, evolving cyber vulnerabilities and threats need to be addressed.

Combating weaponized misinformation

Large-scale spread of misinformation, enabled by advanced information manipulation tools and online platforms, is driving new types of information warfare.

Managing data risks for value creation

Data carries tremendous value for organizations while creating new challenges around transparency, accuracy, security, privacy, social expectations, and legal requirements.

Bolstering organizational resilience in the age of hyperconnectivity

Increased reliance on interconnected systems by organizations amplifies the impact of failure and threatens resilience.

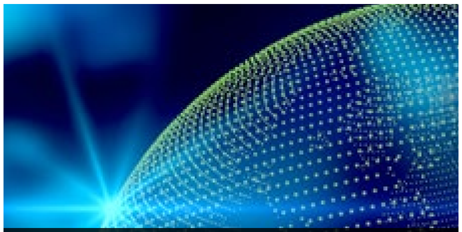
Navigating regulatory change for emerging technologies

Regulatory changes focused on emerging technologies begin to affect business models and increase complexity of compliance.

Enabling digital transformation by managing culture risk

Misalignment between an organization's goals for digital transformation and employee values and behavior creates new culture risks.

Owning digital responsibility and ethics



As part of their digital transformation efforts, organizations need to act responsibly and promote ethical use of technology.

Managing the black box of artificial intelligence

The use of artificial intelligence (AI) techniques and solutions for a wide range of novel applications leaves organizations open to new AI risks.

Why is this trend important today?

Organizations have begun using AI techniques and solutions to affect outcomes across a broad range of purposes, such as approving loans, identifying fraudulent transactions, and performing surveillance. These applications often operate like "black boxes" for decision making. If they produce results without explanation, they make detection of inappropriate decisions difficult. This exposes the organization to vulnerabilities, such as biased data, unsuitable modeling techniques, and incorrect decision making, in the algorithm life cycle.

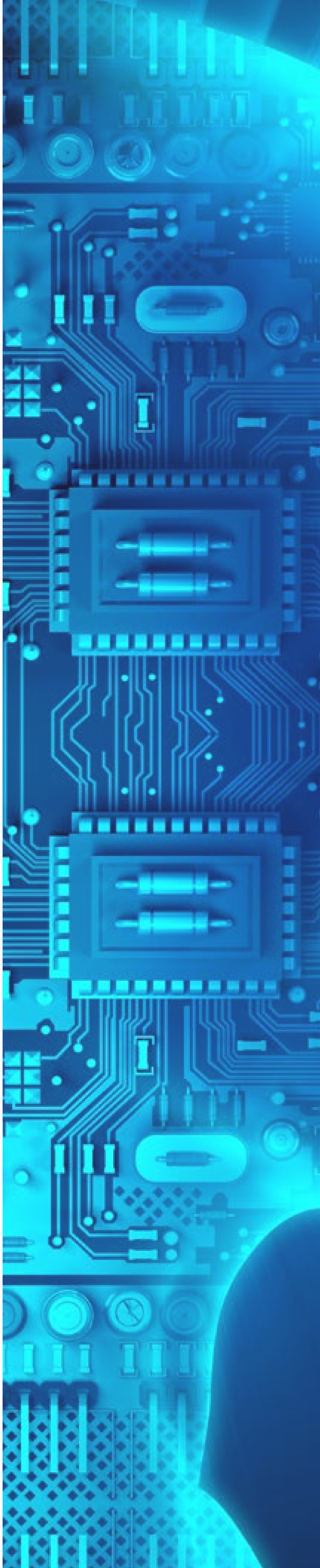
As algorithms become more powerful, pervasive, and sophisticated, the methods for monitoring and troubleshooting them lag behind adoption. Organizations should consider seeking transparency and accountability in how decisions are made by algorithms; consider ethics, fairness, and safety in how algorithms are used; and adopt new approaches to effectively manage the novel risks introduced by complex AI algorithms.

Where has this trend had an impact?

A health care program witnessed backlash from patients when it replaced a manual process with an algorithm that started reducing patients' medical benefits leaving some patients unclear about the rationale behind the decisions.

A crime-predicting algorithm that judges consulted when making sentencing determinations of convicted criminals came under scrutiny when it was found to be no better at predicting an individual's risk of recidivism than random volunteers recruited from the Internet.

Many organizations pulled their advertisements from a website after its programmatic advertising algorithm placed ads next to inappropriate content.



What does this mean for organizations?

- Erroneous decisions made by algorithms trained on biased data leading to poor product performance and even negative impacts on the health and safety of consumers.
- Overlooked vulnerabilities if traditional risk management processes, such as IT general controls and internal audits, fail to consider algorithmic risks.
- Increased scrutiny and higher expectations from consumers for algorithm-driven products to perform without errors.
- Reputational, legal, and regulatory consequences as a result of algorithms making decisions that don't align with social, ethical, cultural, or legal norms.
- Delays in proper redress of business issues in the absence of clear accountability guidelines for managing malfunctioning algorithm-dependent systems.
- Third-party induced risks due to limited visibility into algorithm design and underlying training data when using commercial algorithm-based solutions from external vendors.

How can organizations respond?

- Assess the AI applications inventory and develop AI risk management strategy and governance structure, covering areas such as policies, training, roles, and responsibilities.
- Review black box algorithms (internal and external) and establish controls across the algorithm life cycle, including data gathering, preparation, model selection, training, evaluation, validation, and deployment.
- Institute standardized disclosure practices to inform relevant stakeholders when decisions affecting them are being made using algorithms.
- Develop and maintain surveillance processes to help monitor outcomes from algorithms.
- Conduct periodic independent auditing or validation of algorithms based on established baseline parameters to test the validity of the training data, assess security against manipulation, and optimize model performance.
- Engage with researchers, think tanks, and innovators to adopt leading practices and cutting-edge tools to address algorithmic risks.

What should organizations be asking themselves?

Is algorithmic risk management on the agenda for board conversations?

Do we have a clearly established governance structure for overseeing the risks emanating from complex algorithms?

Have we evaluated the potential impact of an improperly functioning algorithm?

Explore all nine trends ▷

Evolving governance and controls for automation

Operating environment changes driven by the adoption of automation technologies call for redefined governance mechanisms and operational controls.

Why is this trend important today?

Automation is becoming the new norm for organizations to support their growth and cost optimization strategies. And it's driving them to adopt automation technologies, such as robotic process automation (RPA), intelligent automation, and AI-based decision-making tools (refer to our "Managing the black box of artificial intelligence" trend). Unintended consequences, including the obsolescence of existing controls, complexity in operations, and the possibility of cascading errors, become top areas of concern. Legacy infrastructure and fragmented operating environments can limit the benefits that organizations may be seeking.

To realize the complete advantages of automation, organizations need to adopt a holistic change management approach, including business-IT alignment, employee culture (refer to our "Enabling digital transformation by managing culture risk" trend), and new controls designed to the specific risks emerging from automation technologies.

Where has this trend had an impact?

An automation tool used by a media organization automatically published a breaking news story in 2017 about an earthquake that happened in 1925, causing mass panic and huge ripples over social media websites.

A company's automated pricing algorithm kicked in during a national emergency, without consulting with the organization's management about how to handle the sensitive situation. As a result, customers were charged inflated prices during the incident.

A manufacturing organization completely automated a process in their assembly line without changing the quality controls designed for manual human assessment, leading to reduced product quality and increased costs.

What does this mean for organizations?

- Increased complexity because different types of automation require different types of controls while outdated controls need to be replaced. In background checks, for example, controls for humans conducting them may be replaced with software robot (bot) specific controls for exception handling and outliers.
- Increased fragility as minor changes to source systems require cascading change management across automation tools to maintain consistent operations.
- Amplified damage from cyber incidents as hackers may gain access to an automated system or acquire large quantities of confidential data through bots with excessive access and privileges.
- Implementation challenges due to operational setbacks, such as employee apprehension over working with automated systems, and incompatibility with legacy infrastructure.
- Complexity in testing automation systems driven by difficulty in replicating complex production environments.
- Difficulty in realizing the full potential of automation driven by an excessive focus on reducing costs, often overlooking other benefits such as consistency, quality, and accuracy.

How can organizations respond?

- Establish a centralized governance initiative to manage the risk of automation by establishing parameters for where automation can and can't be applied and setting policies concerning process design, development, testing, and maintenance.
- Digitize existing controls through analytics and other technologies, and design new controls specific to each technology, such as built-in error handling capabilities, alert mechanisms for process breakdowns, and manual exception handling for unexpected circumstances.
- Build digital proficiency and educate employees on the benefits of automation to alleviate their fears, accelerate adoption, and encourage identification of potential use cases for development.
- Redesign the control framework across businesses, risk management, and internal audit teams, and use technology-enhanced tools to test or audit automated processes.
- Extend existing change management models to account for bots and enhance existing IT incident and crisis management strategies to support and triage potential incidents associated with use of bots.

What should organizations be asking themselves?

Who in the organization is responsible for governing and managing risks emerging from automated processes?

How are we adapting our controls to account for the complexity of automation?

Are we prepared to respond quickly to automation-induced errors?

Explore all nine trends ▷

Protecting against the changing cybersecurity risk landscape

In order for digital technologies to deliver on their immense promise, evolving cyber vulnerabilities and threats need to be addressed.

Why is this trend important today?

The rapid adoption of emerging technologies is greatly increasing efficiency while adding dynamic cybersecurity challenges for organizations. Cyberattacks have moved beyond identity theft and online account hacks. They threaten our code-enabled physical world—our homes, our cities, our infrastructure, and even the medical devices in our bodies. A host of digital technologies such as AI, automated botnets, Internet of Things (IoT), and cloud computing both facilitate attacks and defend against them at a scale, speed, and level of sophistication never seen before. New types of malware such as automated phishing tools and crypto mining software combined with emerging technologies are expanding the cyber risk landscape. Organizations must continuously revisit their cybersecurity measures to defend against the onslaught.

Where has this trend had an impact?

A software company lost millions in revenue after it fell prey to a malware attack that scrambled computer hard drives, which affected its order receiving and processing systems.

Security researchers unveiled vulnerabilities in connected medical devices that can be exploited by hackers remotely to alter vital signs of patients in real time and potentially cause medical staff to make inappropriate critical care decisions.

A financial services firm experienced financial losses due to a software glitch in its high-frequency trading algorithm that forced the company to automatically sell overvalued shares back to the market at a lower price.

What does this mean for organizations?

- Invisibility of cyber risks for digital transformation leaders and other senior executives because cyber risk management is distributed among lower-level IT professionals and technology service providers.
- Increased complexity in addressing new cyber risk challenges as adoption of digital technologies such as IoT and cloud have increased the attack surface.
- Greater difficulty in identifying intelligent malware as it learns to mimic normal user behavior to avoid being detected.
- More instances of impact to physical safety, especially as automated attacks compromise or subvert physical systems, such as home automation systems and even industrial infrastructure.
- Increased frequency of intelligent attacks on a large scale using AI and automation technologies delivered via the cloud.

How can organizations respond?

- Create a culture of risk intelligence and security awareness by clearly defining security-related roles and accountability for business units and technology groups undergoing digital transformation.
- Restructure processes to support DevSecOps by integrating security as an integral part of the development life cycle and incorporating automation where possible.
- Augment existing cyber risk programs to account for the risks to newly deployed technologies, as well as the increasingly sophisticated nature of cyberattacks enabled by emerging technologies.
- Speed the adoption of digital technologies as a means to reduce technology complexity, make cyber protection simpler, and reduce the number of potential attack targets.
- Improve automation of security operations, secure code reviews, and digital identity management to reduce human errors, rein in escalating costs, and speed detection and response.
- Run crisis war-gaming exercises to train everyone who would be involved in a real crisis to improve their confidence in being able to address a variety of cyber incidents and crisis events.

What should organizations be asking themselves?

Can our existing security measures deal with emerging cyber risks?

How are we raising the digital savviness of our workforce and limiting exploitation of human vulnerabilities?

Have we considered risks to emerging platforms and solutions such as smart devices and software bots?

Combating weaponized misinformation

Large-scale spread of misinformation, enabled by advanced information manipulation tools and online platforms, is driving new types of information warfare.

Why is this trend important today?

Access to sophisticated tools that employ machine learning, automated software bots, and natural language generation makes it easier for people with limited technical skills to create and spread manipulated information at scale. This manifests in a variety of ways, such as social media bots influencing public opinion, false trends through paid online reviews, fake photos and videos that look eerily genuine, and financial trading based on false perception. This problem is further intensified when algorithms innocuously glean inaccurate insights from manipulated information (refer to our "Managing the black box of artificial intelligence" trend), leading to serious errors in decision making.

Nation-states, organized crime groups, companies, and even disgruntled customers have begun using such tools to promote a malicious agenda, gain a competitive advantage, or simply create mischief. What's alarming is not only how easy it is to start and spread misinformation at scale but also the difficulty in determining its authenticity and stopping it from spreading. In such an environment, organizations need to protect their brand safety and reputation by closely monitoring publicly created content.

Where has this trend had an impact?

Over the past year, a retail chain has experienced multiple instances of negative false news spreading virally, such as fabricated reports of discrimination, leading to increased public scrutiny and damage to its brand and reputation.

A company experienced significant drop in stock price and reduced sales as fake news, which used misquoted interview statements by an executive, began spreading across social media, leading to consumer backlash.

A new AI-based image synthesis technique, "deepfake," was employed to create a video of a former US president saying derogatory things about the current US president. The altered video footage was almost indistinguishable from a genuine video.

What does this mean for organizations?

- Brand and reputational damage as false information, created using digital editing and imitation technologies, spreads rapidly to a large audience—inciting unwarranted reactions and delegitimizing leaders and influencers.
- Loss of public trust in organizations due to amplification of manipulated information to create fake trends through false online reviews, biased search engine results, spam emails, and activism.
- Financial losses, such as drops in market capitalization and product sales associated with loss of stakeholder or public trust due to rapid spread of misinformation.
- Difficulty identifying the individual or groups responsible for the origin of false news and curbing that disinformation as it spreads quickly across private social media networks.

How can organizations respond?

- Formulate a brand safety and resiliency strategy by identifying potential vulnerabilities and developing an action plan to mitigate risks of large-scale spread of fake information.
- Augment existing social media strategies to include collaborating with social media platforms to build a strong voice online and flag inaccurate content.
- Proactively develop guidelines to vet public relations firms' social media strategies to avoid association with vendors that may be using unethical practices to generate positive endorsements.
- Leverage sophisticated social media risk sensing tools that can monitor digital media platforms and data sources, such as proprietary databases and content in different languages, in real time to predict and detect issues before they spiral out of control.
- Develop a crisis response plan that helps stakeholders effectively communicate the difference between perceived and actual reality and reduce the risk of alienating existing and new customers.

What should organizations be asking themselves?

What tools and technologies are we currently using to monitor social media content and proactively detect inaccurate information?

Do we have systems in place to contain crises before they escalate out of control?

How are we monitoring the execution of our social media strategy?

Managing data risks for value creation

Data carries tremendous value for organizations while creating new challenges around transparency, accuracy, security, privacy, social expectations, and legal requirements.

Why is this trend important today?

It's no secret that the digital economy is fueled by data. To remain competitive, organizations are collecting, storing, analyzing, using, monetizing, and sharing data more than ever before. On one hand, this results in better and more personalized products and services, more efficient business processes, and new revenue streams. On the other hand, it raises concerns on data usage, transparency, control, accuracy (refer to our "Combating weaponized misinformation" trend), ethics, security, reliability, and privacy. Regulators agree, leading to new regulations across the world, such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act (AB 375). To gain the trust of customers, business partners, regulators, and other stakeholders, organizations are reevaluating traditional approaches to manage emerging data risks.

Where has this trend had an impact?

Auto manufacturers are monetizing driver data such as location and driving behavior from onboard sensors to create personalized services for drivers, potentially display targeted in-car advertisements, and share the data with auto insurers, which raises consumer privacy concerns.

A top-selling, low-cost smartphone sold across top e-commerce platforms has been suspected of sharing customer data with servers in Asia through pre-installed software, raising questions around the extent of accountability these platforms should share.

A partnership between a health care body and a technology company came under scrutiny when it was found that the foundation shared patient data with the latter without the consent of patients, resulting in legal, regulatory, and reputational consequences for both parties.

What does this mean for organizations?

- Increased public scrutiny around data usage as users now expect transparency and control over their data, including the right to access it, limit its use, and delete it.
- Tough strategic decisions, such as potentially backing away from data monetization opportunities that affect the trust of customers and other stakeholders.
- Obligatory requirements driven by regulations to build a risk-aware corporate culture, infrastructure, and policies to respect privacy and protect customer data.
- Increased reputational and legal risk as a result of sharing data, including third-party data breaches and use of questionable data purchased from brokers.
- Increased focus on standardization to manage the high costs of handling data due to inefficiencies, such as duplication of systems, multiple data standards, inability to monetize data, and different protection strategies for different types of data.

How can organizations respond?

- Acknowledge and treat data as a valuable asset and identify associated risks and opportunities.
- Determine accountability and ownership of data assets so data is collected, stored, and used for the appropriate reasons.
- Use technology that speeds up data collection and classification and allows for ongoing maintenance of data definitions.
- Conduct data risk assessments to align proposed data usage with organizational values, stakeholder expectations, and regulatory restrictions.
- Safeguard critical data by applying AI-enabled controls and advanced surveillance methods to identify and mitigate data risks.
- Manage brand and credibility in the market through focused efforts to preserve the value of critical data.
- Invest to achieve compliance with data regulations by building data risk-focused business strategies, policies, and processes.

What should organizations be asking themselves?

Do we have business processes that may be collecting or using sensitive customer data without their knowledge or consent?

Do we know what data is being shared with our third parties and whether they're protecting the data as we would expect?

Are we complying with the various data-related regulations in all the geographies where we operate?

Bolstering organizational resilience in the age of hyperconnectivity

Increased reliance on interconnected systems by organizations amplifies the impact of failure and threatens resilience.

Why is this trend important today?

Organizations have begun moving critical infrastructure and processes to the cloud, enhancing operational awareness through sensors, and increasing touchpoints with the external ecosystem. Such changes to the operating environment increase complexity and fragility and expose organizations to a wide variety of unforeseen risks. These include increased dependence on third parties, and cascading failures as a single error may rapidly spread across a multitude of seemingly unrelated systems. In addition, rapid expansion of the attack surface through introduction of new systems, such as mobile devices and Internet of Things, is prompting organizations to rethink what resilience means in the digital age.

Where has this trend had an impact?

Multiple websites experienced disruption due to an unforeseen outage at their service provider, causing millions in collective losses in market capitalization and decreased website performance.

Researchers remotely hacked cars connected to a cellular network that provided their onboard wireless services. The hackers were allegedly able to gain control over dashboard functions. This led to product recalls by the manufacturer.

A virus infected smart consumer devices such as connected cameras and televisions and enslaved them into botnets, bombarding servers with traffic until they collapsed. This impeded access to many popular websites across the United States for the better part of a day.

What does this mean for organizations?

- Reduced insight into resilience by organization leaders due to limited availability of monitoring tools and real-time dashboards that provide insight into operational continuity.
- Increased fragility of systems created by stitching together services from a multitude of providers, often retrofitting legacy technology, incorporating open source components, or adopting agile development and operations (DevOps) models with frequent changes.
- Difficulty identifying potential points of failure and subsequent containment due to network complexity that makes risk modeling challenging.
- Difficulty in technology recovery planning and response orchestration as a result of continually changing interdependencies due to rapidly evolving technologies and technology providers.
- Increased dependence on third parties for testing resiliency protocols and restarting operations in cases of failures as critical processes begin to reside with a wide range of third parties.
- Incidents escalating into crises and brand and reputation issues in the absence of coordinated response plans across organization boundaries.

How can organizations respond?

- Devise a set of metrics that enables executives to monitor the effectiveness of the resilience program and build confidence in response and recovery.
- Continuously monitor risks from interconnected systems using digital assessment tools capable of detecting issues before they escalate.
- Design for organizational resilience by determining critical business services, support systems, applications, and third parties to plan for business continuity.
- Design for redundancy and real-time automatic recovery rather than piecemeal, manual backup plans.
- Conduct random, unannounced “unplug” tests to simulate failures to determine the resiliency of connected systems.
- Practice incident response and recovery planning with service providers to train leaders, employees, and vendors to handle disruptive events appropriately.

What should organizations be asking themselves?

Do we know which business services are critical and can we identify the systems that support them?

How do we design strategies and fail-safe alternatives to limit cascading failures across a network?

How effective are we at triaging, responding to, and recovering from the various risks that we’re exposed to?

Explore all nine trends ▷

Navigating regulatory change for emerging technologies

Regulatory changes focused on emerging technologies begin to affect business models and increase complexity of compliance.

Why is this trend important today?

Emerging business and service models suggest that innovation continues to outpace regulation. In such an environment, regulators ask themselves: How do we protect consumers and ensure transparent markets while allowing innovation and business to flourish?

Regulatory and supervisory bodies are adopting more flexible approaches to develop policy (such as regulatory sandboxes, outcome-based regulation, risk-weighted regulation, and adaptive regulation), considering supervisory technologies to provide oversight, and publishing guidelines in emerging technology topics, such as data privacy, algorithmic decision making, autonomous vehicles, and initial coin offerings. A fluid regulatory environment gives organizations an opportunity to influence regulations and modernize their approaches to compliance for enhanced effectiveness and cost efficiencies.

Where has this trend had an impact?

Ten organizations have partnered with the US government to collaboratively test the use of unmanned aerial vehicles in an environment that allows them to experiment with uses currently forbidden by federal law.

Businesses based on sharing platforms are facing tough regulatory oversight globally, which is likely to affect their revenue. The fear that regulatory actions may limit benefits of emerging technologies is causing organizations to adopt a wait-and-watch approach to innovation.

California's Consumer Privacy Act requires organizations to let customers opt out of having their data sold while prohibiting companies from charging a customer or treating them differently for having done so, causing Internet service giants to reconsider their business models.

What does this mean for organizations?

- Reduced speed of adoption of emerging technologies and their use, such as blockchain and autonomous cars, due to lack of regulatory clarity.
- Loss of investments and future revenue as new regulations potentially render existing business models ineffective or infeasible.
- Frequent changes to business models or operations due to regulatory changes during a product or service life cycle.
- Increased cost of compliance driven by complex, varying, and sometimes conflicting regulations.
- Increased competitive pressures as new unregulated entrants have the freedom to operate in ways that existing regulated organizations can't.

How can organizations respond?

- Educate regulators and explore emerging technology impacts together to contribute to the development of regulations that protect public interest without impeding innovation.
- Create policies and standards on the use of emerging technology through industry-driven collaborative standard setting and self-regulating bodies.
- Clarify the organization's risk appetite when evaluating projects that lie outside current regulations.
- Use AI technologies for continuous horizon scanning to identify new regulations, track amendments to existing regulations, and understand the associated effects to the organization.
- Train product and technology professionals on risk concepts to be better prepared to comply with emerging regulations while innovating with emerging technologies.

What should organizations be asking themselves?

How are we managing our investments in areas that lack regulatory certainty?

How should we collaborate with regulators to set appropriate regulations on emerging technologies?

How can we use technology to make our compliance program more effective?

Enabling digital transformation by managing culture risk

Misalignment between an organization's goals for digital transformation and employee values and behavior creates new culture risks.

Why is this trend important today?

As organizations transform to thrive in a digital environment, their success is affected by how well they integrate their workforce into the transformation journey. Organizations need to construct a digital culture thoughtfully, incorporating principles of experimentation, smart risk-taking, continuous learning, and collaboration. They must understand how to transmit this culture beyond their employees to their contractors, vendors, and other workforce participants, even software bots acting on behalf of the organization.

Building a digitally savvy leadership and skilled workforce to enable intelligent and ethical use of technology will make the difference between a successful transition and one that's beset by risks and glitches. Digital transformation requires the overhaul of culture beyond technology updates or process redesign in order to reap the anticipated benefits.

Where has this trend had an impact?

The failure of a digital transformation project undertaken by a federal government to centralize and automate a financial system was blamed on a lack of digital culture attributes, such as transparency, accountability, and willingness to experiment.

A large insurance company started experimenting with robotic process automation. One year later, it was still unable to deploy a robot to carry out processes, largely due to an old-fashioned organizational culture averse to new technologies.

Employee concerns around the use of emerging technologies for potentially harmful purposes led several organizations to succumb to employee pressure and curtail work in areas that include controversial uses of technology.

What does this mean for organizations?

- Missed anticipated returns from digital transformation initiatives due to cultural resistance or slow adoption of digital technologies.
- Increased likelihood of irresponsible behavior across the organization, if managing risks continues to be seen as someone else's responsibility or a check-the-box compliance effort.
- Increased need for improving workforce skills to create a culture where technology and humans complement each other, including knowing how to work around machine limitations and biases.
- Reputational consequences of unprecedented levels of transparency into corporate decision making and prevalent culture through social media websites and public forums.
- Loss of market competitiveness due to organizational challenges in balancing an experimentation mind-set and a risk-averse culture.
- Challenges due to misalignment of services provided by temporary or gig workers who have limited understanding of the organization's strategy and culture.

How can organizations respond?

- Establish an organization-wide culture risk-management program to understand the prevalent culture, identify signs that highlight culture challenges (e.g., through employee behavior monitoring and social media sensing), and institute behavioral changes needed for successful digital transformation.
- Refresh organizational core values to embed desirable behaviors, such as smart risk-taking, collaboration, continuous learning conducive to digital transformation, and performance metrics and incentive structures aligned with digital culture goals.
- Conduct periodic pulse checks through talent surveys, town halls, and online platforms to evaluate employee engagement as well as connect with digital culture transformation initiatives.
- Cultivate a digitally proficient risk function to drive early collaboration with business and technology teams leading digital transformations.
- Embed risk-based decision making and risk management concepts in digital proficiency programs to enable a digital culture and frontline employees to take smart risks effectively.
- Use behavioral science techniques and training to nudge employees toward desired behaviors, and reinforce these through monitoring high-risk activities.

What should organizations be asking themselves?

How do we build a digitally savvy leadership and skilled workforce?

How do we take our employees, contractors, and vendors along on the digital transformation journey?

How do we identify and monitor signs that can indicate culture-related risks?

Explore all nine trends ▷

Owning digital responsibility and ethics

As part of their digital transformation efforts, organizations need to act responsibly and promote ethical use of technology.

Why is this trend important today?

The power of digital technologies to enable new sources of revenue can be significant. Due to a proliferation of digital technologies and the particular ethical challenges they present, organizations are increasingly expected to consider ethical obligations, social responsibilities, and organizational values as guides to which digital opportunities to pursue and how to pursue them.

As discussed in the "Managing data risks for value creation" trend, responsible and unbiased collection, handling, use, and privacy are top areas for concern when it comes to data. Also, there are increasing calls for digital services that are fair and equitably accessible, promote physically and mentally healthful uses, encourage inclusion, and are geared toward socially beneficial uses. Digital adopters want technologies that aren't harmful or abusive and are safe and error-free. There's an opportunity to do well by doing good—pursuing digitally responsible growth strategies that build stakeholder trust.

Where has this trend had an impact?

As a response to societal concerns around increasing cellphone use, as well as to create long-term value through ethical leadership, a technology company has added new tools to its operating system that help users monitor and curb time spent on mobile devices.

A series of accidents involving robotics shined a spotlight on questions of responsibility and decision making by autonomous systems in situations where human judgment isn't involved.

A facial recognition software company has established an "AI ethics board" with the goal to develop public trust and guide its use of artificial intelligence to limit social biases in its future products.

What does this mean for organizations?

- Changes in strategic choices as organizations think about digital trust as a brand value and market differentiator.
- Difficulty in making decisions that involve balancing revenue opportunities against brand trust, especially when other market participants may not be behaving in responsible ways.
- Reputational impact due to unanticipated consequences of innovations, such as when digital assistants "listen in" on conversations or computer-generated voices sound uncannily human.
- Legal and regulatory consequences of inappropriate decision making by machines that may amplify social and economic biases or function in ethically gray areas.
- Pressure to go beyond meeting regulatory requirements and demonstrate good citizenship by promoting thoughtful and socially beneficial use of technology.

How can organizations respond?

- Integrate ethics in the organization's strategy by instituting an ethics board or appointing a chief ethics officer that works closely with business units and oversees transformation efforts to guide use of technologies in beneficial ways.
- Build a culture of responsibility by training employees on industry-leading practices, such as integrating principles of fairness, ethics, and safety though the product or service life cycle, and encouraging desirable behaviors through strong support from the top and supporting performance management systems.
- Evaluate proposed applications of emerging technologies in products and services to consider possible ethical, social, and cultural implications.
- Collaborate with industry stakeholders to build ethical frameworks for the use of emerging technologies, in the absence of established standards and norms, to be viewed as the leader in the space.

What should organizations be asking themselves?

What are the ethical implications of our products and decisions, and are our actions aligned with our strategy and brand?

How are we promoting the ethical and responsible use of digital technology in our products and services as well as within our organization?

Where are we making risky decisions, and do we have a plan to deal with potential backlash from unintended consequences?

Explore all nine trends ▷

Digital opportunities:
Leveraging technology can help organizations better manage risk

While digital technologies introduce new risks, they can also enhance risk management, enabling new capabilities and unlocking possibilities considered infeasible in the past. Investments in digital technologies to manage risk can increase effectiveness and efficiency and even transform approaches that render certain risks irrelevant.

Organizations can use digital as a lever to rationalize and optimize their risk management practices to derive efficiencies and reinvest in modernizing risk. While knowing what to focus on can be daunting at first, the following framework can help organizations identify potential uses of emerging technology to better address risks.

EFFICIENT

Reduce cost and increase speed in identifying and addressing risk issues

INTELLIGENT

Improve quality, increase accuracy, and derive richer insights to identify and address risk issues

TRANSFORMATIVE

Adopt a completely new approach to identifying and addressing risk issues

ILLUSTRATIVE EXAMPLES

Accelerated identity and access management enabled by robotic process automation
Automate processes, such as managing access requests and role provisioning, to reduce response time by decreasing the need for manual interventions.

Automated regulatory reporting enabled by natural language generation
Automate generation of suspicious activity reports after reviewing account transaction history to identify anomalies.

Easier access to compliance information through conversational interfaces
Communicate with a chatbot to easily identify relevant policies and regulations required to stay compliant.

Accelerated financial close processes enabled by cloud-based workflow tools
Use cloud-based accounting and reporting tools to accelerate financial close processes that were once manual and scattered.

Augmented detection capabilities through computer vision
Automate inspection of products and environments to spot anomalies invisible to the human eye, such as small cracks and leaks.

Simulated crisis management situations in digital reality
Simulate real-world crisis events in an immersive environment to better prepare people to respond optimally.

Reduced risk of insider trading through machine learning
Use past communications from traders to build a model that determines anomalous behaviors associated with trading violations to avoid regulatory infractions.

Enhanced due diligence for third parties
Perform ongoing due diligence for third parties by automatically searching open and deep web sources, watch lists, sanction lists, and regulatory sites.

Reduced supply chain risk using blockchain-enabled proof-of-provenance
Provide a trusted and accelerated process of verifying origin, safety, and authenticity of products across the supply chain.

Transform third-party risk oversight through a shared utility model
Employ a cloud-based platform that enables sharing of third-party risk assessment data and insights, analogous to the way ratings websites offer data and insights on consumer businesses.

Proactive management of reputation and culture risk
Continuous monitoring of insider threat and reputation risk through predictive analysis of online behaviors, and proactively intervening before bad conduct occurs.

Enhanced product safety and quality enabled by digital twins (virtual replicas of physical objects)
Analyze sensor data on a large scale in real time to predict faults before they occur and schedule maintenance.

What should organizations be asking themselves?

Have we assessed our digital readiness to better manage risk in using technology?

What technology investments are we exploring to reduce the cost of compliance?

How can we use technology to transform the risk function?

Conclusion:
Organizations can harness risk to power performance in a digital world

Organizations are conscious that digital transformation involves more than technology adoption. It requires concerted efforts to define how enterprises organize, operate, and behave by aligning strategy, structures, processes, people, and technology to build a unique digital DNA. Organizations can sidestep unnecessary risks and harness risk to power performance by adopting a risk lens and a holistic approach as part of their efforts. Below are a few guiding principles.

Make smart(er) risk management a part of digital transformation

As digital transformation initiatives gain steam, stakeholder expectations around value creation rise. It's vital that smart risk taking and risk mitigation, along with ethics and transparency, are integral parts of the digital transformation journey.

Organizations need to move away from siloed risk management efforts to facilitate digital transformation. Establishing an agile, hybrid model (centralized and distributed) and enabling a digital culture where managing risk is an essential part of everyday business will erase the outdated model of a checklist exercise assigned to only a few in risk functions.

Plan for a digitally proficient workforce

For digital transformations to succeed, organizations need leaders who are digitally savvy and risk aware. In addition, employees must be trained to understand and work with emerging technologies and manage associated risks. Developing this risk mind-set throughout the organization and especially in people who are leading, developing, and managing digital transformation efforts is crucial.

It's equally important for risk functions to cultivate digitally proficient talent that supports the business to make swift risk-based decisions to power performance.

Digitally transform risk activities

Those managing risk functions today should study emerging technologies that transform traditional processes to drive a fundamentally more efficient, intelligent, and transformative way of managing risks. Given the rapid pace of technological change, organizations should continually revisit how technology can add capability and capacity to simplify risk management at lower costs and enhanced value.

Revamp operations to manage risks from emerging technologies

As technologies evolve, new governance processes and operational controls are needed to identify and limit unintended impacts to the business and its stakeholders. These measures will vary based on the technologies involved and the business issues they're deployed to solve. We offer a range of recommendations on the individual trend profiles.

Build ecosystem partnerships to manage risks

Digital transformation exacerbates the interplay of risks that can arise from companies working closely through extended ecosystems of business partners, technology vendors, and services providers. Organizations should proactively form networks with peers, innovators, and regulators to better understand and manage risks through information sharing, adoption of leading-edge solutions, and industry-driven regulation.

What should organizations be asking themselves?

Are there risks highlighted in this report that are especially relevant for my organization?

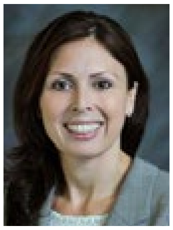
Are our digital transformation initiatives appropriately considering the associated risk implications?

How are we transforming our risk activities with digital technologies?

Contact us

Contact us to discuss how these risk trends impact your organization and how you can better prepare for what's ahead. We can help you identify ways for your organization to manage risk, create value, and effectively power your performance.

Authors



Nancy Albinson
Managing Director
Deloitte & Touche LLP
nalbinson@deloitte.com
+1 973 602 4523

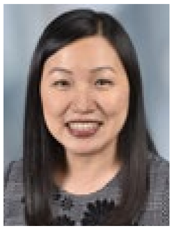
Nancy is a managing director at Deloitte & Touche LLP and leads Global Risk Advisory Innovation. She focuses on innovation strategy, sensing of emerging trends, experimentation, and efforts to invest in and scale new or adjacent solutions. She leads a program focused on making strategic investments in emerging megatrends and technologies and engages in efforts to transform core offerings with digital technologies. She leads talent development for Risk and Financial Advisory to help shape the workforce of the future.

Cherian Thomas
Managing Director
Deloitte Financial Advisory Services
India Private Limited
chethomas@deloitte.com
+1 678 299 7310

Cherian is a managing director at Deloitte Financial Advisory Services India Private Limited and a leader within the Strategy and Transformation organization. He shapes and drives a market-leading innovation and transformation program to drive growth for Deloitte's Risk and Financial Advisory practice. He is a futurist, with experience in identifying opportunities and risk implications of emerging business and technology trends and commercializing promising opportunities. As a co-leader of Deloitte Risk and Financial Advisory's Moonshot Incubator, he leads a team that explores strategic investments in emerging megatrends and technologies for Deloitte. Cherian has led several leadership roles at Deloitte, spanning innovation and strategy, digital transformation, talent acquisition, and talent development.

Michael Rohrig
Partner
Deloitte & Touche LLP
mrohrig@deloitte.com
+1 713 982 2600

Mike is a partner at Deloitte & Touche LLP and leads Deloitte Risk and Financial Advisory's portfolio of offerings, which help organizations effectively navigate business risks and opportunities—from strategic, reputation, and financial risks to operational, cyber, and regulatory risks—to gain competitive advantage.



Yang Chu
Senior Manager
Deloitte & Touche LLP
yangchu@deloitte.com
+1 415 783 4060

Yang is an innovation futurist at Deloitte & Touche LLP, focused on exploring emerging trends, experimenting with cutting-edge technologies, and engaging with the innovation ecosystem for clients and for Deloitte Risk and Financial Advisory. She is a specialist in strategic, financial, operational, technological, and regulatory risks.

Research team

Jeannette Marsh
Senior Manager
Deloitte Financial Advisory Services
India Private Limited
jeamarsh@deloitte.com

Kashvi Bhachawat
Senior Consultant
Deloitte Financial Advisory Services
India Private Limited
kbhachawat@deloitte.com

Sachin Maheshwari
Senior Consultant
Deloitte Financial Advisory Services
India Private Limited
sacmaheshwari@deloitte.com

Arushi Nagpal
Consultant
Deloitte Financial Advisory Services
India Private Limited
arnagpal@deloitte.com

Contributors

A special thanks to:
Scott Barret, Ninad Bhangle, Andrew Blau, Indranil Roy Chowdhury, Edward Hida, Satish Iyengar, Sunil Kapur, Vivek Katyal, Michael Kearney, Ishita Kishore, Michael Koppelmann, Dilip Krishna, Katherine Kuperus, Cory Liepold, Jeff Lui, Joseph Mendel, Pavan Murali, Carey Oven, Meghna Panwar, Vibha Patil, Subramaniam Raman, Martin Rogulja, Rishab Sapra, David Schatsky, Ritika Shetty, and Damian Walch.

Endnotes

This report is based on interviews with Deloitte and external specialists, as well as analysis based on secondary sources.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.