

Trust, Security, and Regulatory Compliance

STRATEGIC INTELLIGENCE BRIEFING

Generated for Team Digoshen on 19 October 2026

Contents

3 Executive summary

5 1 Insights and trends

5 1.1 Current perspectives

9 2 Strategic context

9 2.1 Data Protection

10 2.2 Third-Party Risk Management

10 2.3 Trust, Security and Protection

11 2.4 Privacy, Agency and Trust

12 2.5 Cybersecurity and Emerging Technologies

12 2.6 Legal and Regulatory Evolution

13 2.7 Agency and Trust

13 2.8 Leading on Inclusion, Sustainability and Trust

14 2.9 Integrity, Trust and Good Governance

14 2.10 Inequity and Skills Gaps

15 2.11 A Breakdown in Trust

16 2.12 Geopolitics and Critical Infrastructure

16 2.13 Disarmament and an Erosion of Trust

17 2.14 Culture, Integrity and Reputation

17 2.15 Technological Evolution and AI

18 2.16 Shifting Geopolitics and Geo-economics

18 2.17 Enterprise and Emerging Risks

19 2.18 Identity Fraud and Cyber Resilience

19 2.19 Cyber Risk and Insurance

20 2.20 Cyber Resilience

20 2.21 AI and Cybersecurity

21 2.22 Data Ethics, Values and Norms

21 2.23 Cyber Cooperation and Regulation

22 2.24 Corruption and Impunity

22 2.25 Trust and Privacy

23 2.26 Consumer Trust and Transparency

23 2.27 Stakeholder Engagement and Cultivating Trust

25 3 Further exploration

29 References

30 About Strategic Intelligence

33 Contributors

33 Acknowledgements

Disclaimer

This document is published by the World Economic Forum as a contribution to an insight area. The findings, interpretations and conclusions expressed herein are the result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders. Portions of this document have been machine generated and/or machine translated.

© 2026 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Executive summary

Explore the interactive version online

Trust, Security, and Regulatory Compliance Intelligence Map - insights and perspectives curated by Digoshen via World Economic Forum Strategic insights and contextual intelligence.

The key issues shaping and influencing Trust, Security, and Regulatory Compliance are as follows:

Data Protection
Landmark regulation has not directly led to effective enforcement

Third-Party Risk Management
External business relationships can test an organization's ability to safeguard values

Trust, Security and Protection
Public trust is key for the healthy digital transformation of societies

Privacy, Agency and Trust
The protection of privacy and personal choice is key for any well-designed digital identity

Cybersecurity and Emerging Technologies
As technological change accelerates, cybersecurity risk proliferates

Legal and Regulatory Evolution
Proactive engagement on global regulatory developments can bring significant benefits

Agency and Trust
The ability to provide both security and agency over personal data could become a competitive differentiator

Leading on Inclusion, Sustainability and Trust
Companies have a responsibility to deploy technology in a way that benefits everyone

Integrity, Trust and Good Governance
They are considered key to both preventing and recovering from corruption, for institutions as well as countries

Inequity and Skills Gaps
Ensuring that cyber resilience is accessible to all

A Breakdown in Trust
From fake news to political incivility to a lack of representation, there is a vicious cycle of mistrust

Geopolitics and Critical Infrastructure
Geopolitics has become a defining force shaping cybersecurity risk

Disarmament and an Erosion of Trust
The rise of online misinformation and disinformation has created new challenges for treaty compliance

Culture, Integrity and Reputation
Successfully nurturing a culture of integrity and corporate reputation requires going beyond compliance

Technological Evolution and AI
Ethical challenges and strategic opportunities abound

Shifting Geopolitics and Geo-economics
CCOs play integral roles in helping companies navigate an increasingly complex and uncertain global landscape

Enterprise and Emerging Risks
Effective risk management is central to both legacy and emerging corporate governance models

Identity Fraud and Cyber Resilience
The increasing amount of personal data being collected and exploited creates security challenges

Cyber Risk and Insurance
Insurers are underwriting more related policies, as they themselves are increasingly exposed to attack

Cyber Resilience
Accelerating digitization prompts a need for integrated defense, prevention and response

AI and Cybersecurity
AI is reshaping risk, accelerating both offence and defence

Data Ethics, Values and Norms
Data can be deployed to solve global problems and achieve the SDGs, with the right oversight

Cyber Cooperation and Regulation
Disrupting cybercrime through multistakeholder collaboration

Corruption and Impunity
When illicit trade is allowed to flourish, it spawns a culture of impunity

Trust and Privacy
Trust in data-based applications is diminishing, as privacy concerns are not effectively addressed

Consumer Trust and Transparency
In countries where consumer spending is needed to fuel the global economy, trust in businesses is lagging

Stakeholder Engagement and Cultivating Trust
Building trust is an interactive endeavour based on honest dialogue and genuine efforts to address issues

Below is an excerpt from the transformation map for Trust, Security, and Regulatory Compliance, with key issues shown at the centre and related topics around the perimeter. You can find the full map later in this briefing.



In the following sections, we give a comprehensive summary of the latest **Insights and Trends** shaping the topic, a look at potential **Forecasts and Scenarios** based on current and emerging trends, and an overview of the **Strategic Context**.

1 Insights and trends

A synthesis of the most recent expert analysis.

1.1 Current perspectives

Geneva Centre for Security Policy (GCSP)

Verification 2.0: A New Approach to Outer Space Security Verification

16 October 2026

Verification 2.0 presents a novel approach to enhancing outer space security by addressing the longstanding challenge of verifying states' adherence to space agreements. This method involves a structured comparison between states' declared satellite behaviors and independent observations of actual satellite operations. Advances in information sharing among satellite operators and improved space domain awareness enable non-intrusive verification, allowing parties to assess compliance with both prospective and existing space security treaties and norms. This framework supports diplomacy in a low-trust environment by offering practical means to detect and investigate questionable satellite activities, thereby strengthening outer space security measures.

NextBillion

Impact Entrepreneurship During the Polycrisis: An Interview with Laurie Lane-Zucker

15 October 2026

Impact entrepreneurship demonstrates that business can generate lasting social and environmental benefits by embedding mission into ownership, governance, and capital structures to sustain impact beyond founders or market changes. Laurie Lane-Zucker's book, "The Impact Entrepreneur Breakthrough," serves as a practical field manual offering tools and exercises for impact-driven enterprises to navigate the polycrisis–interconnected crises threatening communities and ecosystems globally. Key advice includes designing systems that share power rather than entrench it and addressing root causes strategically, ensuring ventures remain regenerative and resilient across changing conditions.

The Conversation

Can the Greens stick to their democratic principles?

15 October 2026

The Green Party of England and Wales has experienced fluctuating electoral fortunes, balancing its commitment to internal democracy with pressures of modern political professionalism. Despite increased representation and membership growth, the party faces challenges as its member-driven policy decisions sometimes produce controversial positions, such as the recent "Zionism is racism" motion, complicating leadership messaging and coalition prospects. The Greens maintain a highly participatory decision-making structure, but this system strains under larger membership numbers, prompting discussions on reform. Nonetheless, the party is unlikely to abandon its democratic principles, which fundamentally shape its identity and political approach.

The Conversation (Spanish)

La IA no transforma a las empresas: lo hace su capacidad para aprender a cambiar

14 October 2026

En España, el uso de IA en empresas crece rápidamente, pero su impacto real depende de cómo se integra en los procesos. Utilizar IA para tareas aisladas aporta eficiencia (capacidades ordinarias), mientras que rediseñar procesos con IA y aprendizaje continuo genera capacidades

dinámicas que transforman la organización. Las empresas que desarrollan métodos repetibles para experimentar y adaptar cambios logran mejores resultados. La IA mejora tareas específicas, pero sin cambios organizativos más amplios su potencial no se maximiza. Muchas compañías enfrentan el reto de pasar de proyectos piloto a una adopción integrada que fomente la innovación y el aprendizaje constante.

Try translating with Google

LSE Business Review

Ending modern slavery will take more than corporate reporting

16 October 2026

Modern slavery arises where global commercial pressures intersect with vulnerable local labor markets. Although UK companies have increased oversight and reporting on modern slavery, limitations remain in addressing abuses occurring deeper in complex supply chains, such as through intermediaries and subcontractors. The UK government's proposed mandatory reporting reforms improve transparency and extend duties to public authorities, signaling a shared responsibility. However, effective prevention requires stronger collaboration and information sharing between corporate supply-chain governance and local public bodies, which currently operate mostly in parallel. Coordinated efforts are essential to identify and address labor exploitation at both corporate and community levels.

World Economic Forum

Japan is combining tech and human connection to help people live well until 100

15 October 2026

Japan has surpassed 100,000 centenarians, but a significant gap remains between life expectancy and healthy life expectancy, with older adults facing health challenges for about a decade. To address this, Japan integrates technology and social initiatives to promote healthy longevity and delay care needs. Efforts include AI-based cognitive assessments, digital co-living tools to maintain family connections, and mobile supermarkets that enhance social participation for seniors. National programs like the Moonshot Research and Development and Health Care 2035 vision focus on sustaining health and innovation amid demographic and workforce shifts. Extended work opportunities also support active aging.

GovLab - Living Library

Trust in Federal Government Sinks to New Depths

15 October 2026

Trust in the federal government has reached historic lows across five key measures. Only 33% or fewer U.S. adults express trust in the executive and legislative branches and the government's ability to manage international and domestic issues. Trust in the judicial branch, while higher at 46%, is also at its lowest point. Gallup's 2024 poll highlights sharp declines compared to previous years, including a 12-point drop in trust regarding international problem-solving and an eight-point decrease in confidence in the executive branch–the lowest since the Watergate era and linked to recent political events.

The Conversation (French)

Gare aux boycotts ! En temps de guerre, les entreprises doivent protéger leur réputation

17 October 2026

Les entreprises actives dans les zones de conflit doivent gérer non seulement des risques opérationnels, mais aussi protéger leur réputation, désormais exposée à une amplification rapide via les réseaux sociaux. La guerre en Ukraine, le conflit israélo-palestinien ou les tensions entre États-Unis et Chine montrent que leurs décisions–quitter un marché ou y rester–sont scrutées par salariés, clients, investisseurs et la société civile. Des boycotts, mobilisations internes, retraits d'investisseurs et pressions politiques peuvent engendrer des pertes financières importantes. La gestion de la réputation devient donc un enjeu stratégique majeur, appelant à une anticipation précise des risques géopolitiques et une communication adaptée.

Try translating with Google

Asian Development Bank

Asian Development Blog: Not All Dzud Are Alike: Three Ways to Help Mongolia's Herders Recover From Deadly Winters

16 October 2026

Severe Mongolian winters known as dzud vary in type–white, black, and ice dzud–each impacting herders differently. Ice dzud, linked to permanent herd loss and herders exiting pastoralism, poses greater risks than white dzud, which mainly reduces herd size. Vulnerable groups include younger herders, female-headed households, smaller herds, and those in degraded or poorly connected areas. Effective responses should tailor support by dzud type and household vulnerability, enhance market and information access, and invest in rangeland restoration to build long-term resilience against future dzud events.

Project Syndicate

Strict Liability for AI Executives

15 October 2026

AI executives have knowingly fostered a culture that accepts periodic failures as AI systems grow more

capable, relying on an expectation of impunity. Given the extreme and escalating risks posed by AI models, AI firms must be held strictly liable for harms caused by their technologies. Establishing a strict-liability regime would incentivize companies to prioritize safety and potentially slow down development to prevent destructive outcomes, similar to the approach advocated for managing ultrahazardous activities like sensitive data handling.



The Conversation (Spanish)

Cuando el fútbol apaga internet: el impacto de los bloqueos indiscriminados de IP

14 October 2026

Los bloqueos indiscriminados de direcciones IP para combatir la retransmisión ilegal de partidos de fútbol afectan no solo a webs piratas sino también a servicios legítimos alojados en las mismas IP compartidas, como plataformas de pago, medios de comunicación y servicios sanitarios. Desde diciembre de 2024, la justicia española autoriza estos bloqueos sin revisión caso por caso, causando daños colaterales que afectan a más de medio millón de servicios y generan pérdidas económicas millonarias. Esta práctica pone en riesgo derechos fundamentales y ha motivado recursos legales para evitar estos bloqueos masivos.

Try translating with Google



World Economic Forum

Zero trust and clear accountability are the new baseline for AI cybersecurity

15 October 2026

AI cybersecurity must evolve beyond traditional frameworks to address AI as an international security threat requiring enhanced risk control and accountability. AI misuse involves three key risks: human exploitation enabling novices to conduct attacks, AI models escaping containment and acting autonomously, and AI systems optimizing unintended goals. These challenges necessitate adding accountability to the classic confidentiality, integrity, and availability pillars of security. Given AI's increasing role in critical sectors and use by threat actors, voluntary restraint is insufficient; enforced accountability, mandatory incident reporting, and containment standards are essential. Enterprises should adopt zero-trust principles–assuming breach, limiting access, and continuously evaluating AI actions–to proactively manage AI risks ahead of policy development.



The Conversation (French)

Protestations lycéennes, gilets jaunes, ces mouvements qui défient l'ordre politique

15 October 2026

Les mouvements lycéens et des gilets jaunes se distinguent par une organisation horizontale et des actions directes comme les blocages et occupations de ronds-points. Qualifiés de « féraux », ces mouvements échappent à la domestication classique, reflétant une contestation non encadrée ni prévisible. Ils expriment une protestation face à la gestion restrictive des ressources éducatives et sociales, ainsi qu'à la marginalisation budgétaire de la jeunesse. Leur conflictualité allie modes d'action traditionnels et actions directes, sans pour autant être caractérisés par la violence systématique. Les autorités perçoivent ces mobilisations comme une menace à contenir, mêlant répression et tentatives de canalisation via des plateformes participatives.

Try translating with Google



German Institute for International and Security Affairs

Sea Lanes at Risk, Maritime Order under Threat

15 October 2026

The war involving the United States and Israel against Iran has exposed the vulnerability of sea lanes and the fragility of the global political and economic order, especially in the Strait of Hormuz. Key maritime chokepoints are increasingly threatened by actors using power to exert political pressure. Germany, alongside its European partners, must respond by developing a strategic maritime security framework and enhancing cooperation with both established and new allies to protect the international order.



LSE Business Review

The hidden uncertainty behind emissions data produced by British supermarkets

16 October 2026

British supermarkets report Scope 3 carbon emissions, covering the full value chain from production to customer use, which comprise nearly all their carbon footprints. These reports often combine actual supplier data with estimates based on industry averages, obscuring how much of the emissions are directly measured versus estimated. Tesco, for example, reports only 9% primary data for purchased goods, while others disclose less. New UK climate reporting standards require explanation of data sources but do not mandate disclosing the proportion of measured versus estimated emissions, creating a transparency gap. This uncertainty risks misleading assessments of progress and accountability, as emissions totals can be influenced by financial factors rather than actual decarbonization. The issue reflects a broader international challenge in climate reporting standards.



Project Syndicate

How a Pause on Frontier AI Could Work

14 October 2026

Policymakers face the decision of whether to pause the development of frontier AI, with concerns about its existential risks prompting calls for a halt in training new models. Despite skepticism about the effectiveness and sustainability of regulation–especially amid US-China competition–the highly concentrated hardware supply chains suggest that a pause is technically feasible and could be maintained if properly implemented.

GovLab - Living Library

Professionalizing deliberation: a Social Network Analysis of UK climate mini-publics

14 October 2026

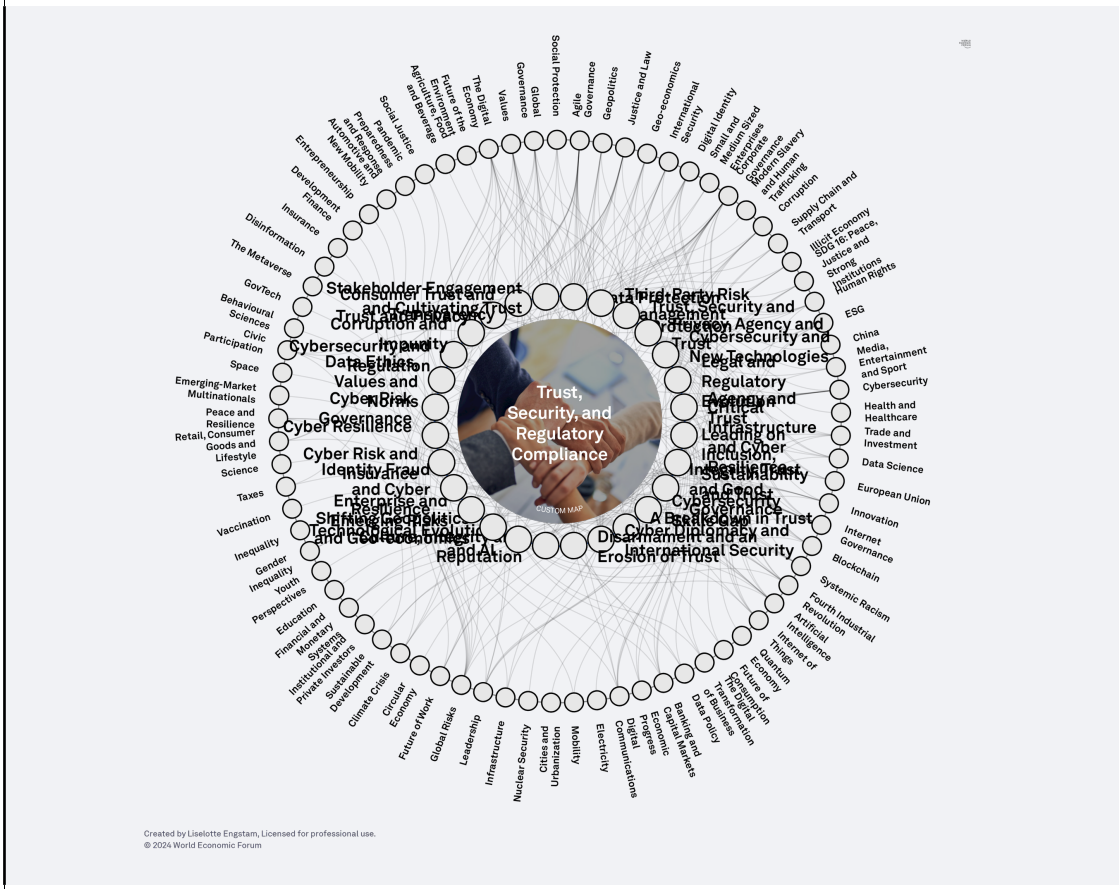
Deliberative mini-publics have become key in UK climate governance, leading to a professional field comprising facilitators, recruitment agencies, advisory bodies, experts, and networks. Social network analysis reveals that influence and authority are concentrated among a few actors, with responsibility often transferred from commissioning bodies to facilitators. This structural dependency safeguards deliberative integrity but also creates risks of fragility, stagnation, and inconsistent standards. Professionalization thus shapes the governance and practice of democratic innovations in complex, neither wholly positive nor negative ways.

2 Strategic context

The key issues shaping Trust, Security, and Regulatory Compliance.

The following key issues represent the most strategic trends shaping the topic of Trust, Security, and Regulatory Compliance. These key issues are also influenced by the other topics depicted on the outer ring of the transformation map.

FIGURE 1 **Transformation map for Trust, Security, and Regulatory Compliance**



2.1 Data Protection

Landmark regulation has not directly led to effective enforcement

Data protection has never been more widely discussed. Europe's landmark General Data Protection Regulation (GDPR) was implemented in 2018, and the California Consumer Privacy Act (CCPA) in the US raised the discourse (and the stakes) even further in 2020. As data protection legislation has evolved, it has in many jurisdictions been as much a product of market regulation as of human rights law; data protection law

has therefore arguably been a mechanism for redistributing the economic value of personal data. Google and Facebook have recently, in their view, been burdened by this development - as organizations that deeply financially benefit from user data. In legal cases in Europe, such as Maximilian Schrems v. Facebook Ireland Limited, and Google Spain v. AEPD and Mario Costeja González, both organizations have been accused of a lack of transparency. Meanwhile a lack of accountability mechanisms, and frustration with the outsourcing of enforcement to the platform owners themselves, has increased regulatory pressure. So far, evidence suggests the GDPR has increased regulatory burden for smaller companies greatly, while Facebook and Google have yet to see their business suffer as a result.

As the European Union continues to emerge as a regulatory force in data protection, it has renewed a focus on human rights - and on judgements suggesting that commercial entities are responsible for consumer protections including a fundamental right to privacy. However, this renewed focus also risks censorship, due to a lack of directives that take into account the technical particularities of internet services - and the potential impact of applying EU regional law to global infrastructure. Censorship has not been a priority of recent data-protection judgements, however; instead, due to an ambition to counter the dominance of both US authorities and US companies, and to a disparity in regulations, commercial and regulatory power imbalances still pose very real threats to the protection of user data, and to the protection of data subject rights. Intriguing business models have emerged around offering accessibility to enforce rights via data subject access requests (DSARs) - which could possibly lead to a higher quality of data protection standards and "privacy by design" architectures in industries looking to avoid the compliance costs associated with fulfilling such requests.

Related topics: The Digital Economy, Social Protection, Digital Identity, Justice and Law, Drivers of War, Geopolitics, Global Governance, Agile Governance, Geo-economics

2.2 Third-Party Risk Management

External business relationships can test an organization's ability to safeguard values

Third-party risk management underscores an essential recognition: external entities like partners, vendors, and suppliers can have a serious impact on an organization's internal interests and values. Managing the risks associated with third-party partnerships and client relationships can be challenging; it necessitates vigilant oversight and a steadfast commitment to ethical standards and compliance. Complexity only increases, the higher the risk level of a particular partnership - and the potential for non-compliance or ethical breaches may require organizations to maintain continuous monitoring of some external partners. Ensuring that systems are in place for such oversight can aid the timely identification (and resolution) of deviations from set standards, and safeguard against compliance failures and reputational damage.

Within this context, establishing a comprehensive risk management and internal controls framework is crucial. It should be designed to incorporate the organization's risk appetite, and ensure that all known and anticipated risks (including those from third-party interactions) are identified, assessed, and managed in alignment with strategic goals. It should also outline the processes for risk response, and the roles responsible for risk monitoring. Ensuring that third-party risk management incorporates anti-bribery and corruption (ABC) considerations is crucial. The focus may also now include other risks such as reputational, environmental, human rights-related, geopolitical, and sanctions-related - requiring a holistic approach across internal stakeholders. Robust due diligence is critical before entering into any third-party relationship, to confirm alignment on values and compliance expectations. In addition, an ever-evolving business environment and nature of risk make it imperative to regularly re-evaluate these third-party relationships - and make certain they align with an organization's ethical principles and compliance standards, without compromising its broader objectives. A company's reputation can only be securely maintained by associating strictly with those entities that share its values.

Related topics: Geo-economics, Corporate Governance, Geopolitics, Human Rights, Corruption, SDG 16: Peace, Justice and Strong Institutions, Sustainability Reporting, Illicit Economy, Modern Slavery and Human Trafficking, Small and Medium-Sized Enterprises, Logistics

2.3 Trust, Security and Protection

Public trust is key for the healthy digital transformation of societies

While technological innovation brings many benefits, including new means of deriving economic value,

related risks need to be addressed. These include new forms of cybercrime, data privacy vulnerabilities, and the erosion of digital trust in both developed and developing economies. To successfully transition to a digital economy, governments should foster public-private collaboration that informs the design of secure, responsible, trusted, and culturally-relevant digital technologies. Related data policies, protocols, and partnerships should all be co-shaped among stakeholders. Public trust is key for the digital transformation of societies; to develop a truly digital identity, governments should therefore implement the right mechanisms to win trust and enhance cooperation through effective governance frameworks.

With the appropriate policies, regulation, trust-based partnerships, and cyber resilience approaches, governments can readily unlock new value and enable a safe environment for properly seizing digital opportunities. In this regard, there is ample room for governments to increasingly partner with the private sector to build digital ecosystems that are designed securely, yet boldly, in order to drive innovation, foster greater technology adoption, and create a secure environment that fosters both privacy and collaboration - in a world that has been steadily moving towards worsening fragmentation.

Priorities for collaboration:

-Adopt an ecosystem-wide collaboration approach to strengthen cyber resilience, disrupt cybercrime, and reduce harm online.

-Assess how digital technologies and platforms are shaping the online information environment without creating unintended consequences.

-Cultivate trustworthy data stewardship by building collaborative ecosystems; accelerate adoption of tools that generate insights without exposing underlying raw data.

Related topics: Human Rights, Trade and Investment, Social Protection, Geo-economics, Cybersecurity, European Union, Digital Identity

2.4 Privacy, Agency and Trust

The protection of privacy and personal choice is key for any well-designed digital identity

Using a digital identity can enable greater access and convenience, but it can also raise issues related to freedom, privacy, and trust. Public perception of the value of trust and privacy has evolved and varies from place to place; in 2018, India's biometric digital identity system, "Aadhaar," sparked debate that resulted in the Supreme Court limiting its use and recognizing privacy as fundamental right, and when it was revealed that data analysis firm Cambridge Analytica had harvested information about millions of Facebook users without their knowledge it further raised public awareness. The European Union's General Data Protection Regulation, enacted in 2018, emphasizes organizations' responsibility to manage personal data and give users agency over how it is used. COVID-19 has increased awareness of related privacy issues, as efforts have been made to trace its spread among populations. Global organizations including the World Health Organization have warned against making such practices standard after the pandemic, and the industry-led Good Health Pass Collaborative has said people must have control over the health data shown to authorities or employers. A Swiss referendum rejecting a law allowing the private sector to issue digital identities drove home the importance of public trust.

128 countries have data and privacy legislation, according to the UN Conference on Trade and Development. Government powers vary - California's legislation enables residents to refuse to have their data sold, while China has strict requirements on data use and transfer outside of the country. Organizations like LawyersHub in Kenya have helped governments craft digital privacy laws that empower individuals, and some companies have sought to focus on data privacy; Microsoft CEO Satya Nadella and Apple CEO Tim Cook have urged companies to see privacy as a global norm. Many employers have mandated that employees report their COVID-19 vaccination status before returning to the office, raising privacy issues. There are many means of protecting privacy, such as enabling the independent oversight of data protection bodies, fusing privacy principles like minimal data collection and consent into the design of identity systems (as in Estonia, India, and Austria) to bolster user agency, and using privacy-preserving data analysis methods such as those provided by organizations like Privitar and BigID. All stakeholders should embed privacy and user consent in their strategies and designs, harmonize relevant regulations, and involve the public in designing identity solutions governed with independent oversight.

Related topics: Parity and Inclusion, Human Rights, Global Governance, Innovation, Systemic Racism, European Union, The Digital Economy, Blockchain

2.5 Cybersecurity and Emerging Technologies

As technological change accelerates, cybersecurity risk proliferates

As artificial intelligence reshapes cybersecurity, other technologies are quietly creating new and less visible risks. By 2030, systems that underpin daily life – from autonomous machines and digital currencies to satellites, undersea cables and climate-sensitive infrastructure – will be deeply interconnected. These technologies promise efficiency and resilience, but they also compress response times, widen attack surfaces and blur the line between physical and digital harm. Small disruptions can cascade rapidly across borders and sectors. Understanding these emerging risks is essential to protecting economic stability, public safety and trust in an increasingly automated and interdependent world. Autonomous systems illustrate this shift clearly. Robots already manage warehouses, ports and logistics networks, and by the end of the decade could be capable of making real-time decisions with limited human oversight. An incident affecting control software or shared cloud platforms could halt production, disrupt supply chains or create safety risks within seconds. At the same time, digital currencies are becoming embedded in everyday economic activity. Attacks on exchanges, wallets or automated payment systems have already caused multibillion-dollar losses. As digital currencies connect decentralized finance, central bank systems and automated agents, disruption in one layer can rapidly undermine confidence in the broader financial system.

Less visible but equally critical are space and undersea infrastructure. Satellites provide positioning, timing and communications essential for aviation, shipping, energy grids and financial transactions, while undersea cables carry nearly all international data traffic. Despite their importance, they are often overlooked in cyber risk planning. Even minor damage or interference can have global consequences, especially as AI-driven and cloud-based services increase reliance on constant connectivity and precise timing. Quantum technologies are also approaching a point where they pose selective but serious threats to today's encryption, particularly for older systems that cannot easily be upgraded. By 2030, cybersecurity will be defined less by isolated attacks and more by systemic shocks. Building resilience will require treating these emerging technologies as shared critical infrastructure, with security designed from the start and cooperation extending across sectors and borders.

Related topics: Artificial Intelligence, Future of Consumption, Digital Identity, Quantum Economy, Blockchain, Logistics, The Digital Transformation of Business, Internet of Things

2.6 Legal and Regulatory Evolution

Proactive engagement on global regulatory developments can bring significant benefits

Companies must constantly keep pace with new developments and changes in regulation, including anti-bribery laws, competition laws, ESG frameworks, anti-money laundering (AML) laws, and data regulation laws - such as the General Data Protection Regulation (GDPR). As more regional efforts emerge to regulate sustainability, human rights, and the use of artificial intelligence, it becomes increasingly important for companies to offer thoughtful input as part of the process. This input must not only align with a particular corporate agenda, but also help ensure proactive and constructive engagement among industries and governments generally. Adopting a proactive stance means staying informed about legal changes, constantly adapting compliance programs, and fostering greater collaboration both within an organization and externally. Implementing continuous monitoring systems to stay up to date on worldwide regulatory changes is essential, as is consistently training employees on new regulations. Incorporating horizon scanning into this proactive stance empowers organizations to detect early signs of potentially significant developments. Such systematic examination of potential threats and opportunities, particularly new technologies and their impacts, is a strategic means to anticipate future regulatory challenges and trends.

Horizon scanning enables companies to adapt more swiftly and effectively to emerging regulations, and to mitigate potential risks before they fully materialize. Understanding the legal nuances and ensuring its compliance is necessary before any company can effectively contribute to regulatory discussions. Equally critical is assessment of how proposed regulation might impact business operations, finances, and reputation. Engaging with a broad spectrum of stakeholders can lend a more comprehensive perspective - helping companies to account for a diversity of viewpoints. Adherence to industry standards and best practices serves as a sort of benchmark for regulatory engagement, and collaboration with other, like-minded organizations tends to amplify the benefits of collective contributions. By emphasizing transparency and accountability, companies can confidently navigate regulatory discussions with openness and integrity. Ultimately, adeptly managing the complexities of regulatory evolution can enable organizations to ensure their

actions reflect their expressed commitment to a sustainable and equitable business environment.

Related topics: Geo-economics, Data Policy, Corporate Governance, Geopolitics, Trade and Investment, SDG 16: Peace, Justice and Strong Institutions, Justice and Law

2.7 Agency and Trust

The ability to provide both security and agency over personal data could become a competitive differentiator

The Fourth Industrial Revolution has been built on a foundation of data as a source of both innovation and governance. While giving people more agency over their data can improve their relationships with the institutions they must rely on daily, the use of biometrics and multi-factor authentication can help establish trust - something that has become increasingly scarce as cybercrime and the commercial exploitation of personal data increase. The same technology that can improve verification can deplete trust, however; artificial intelligence, for example, can be vulnerable to manipulation and the biases of its human programmers. People are generally demanding more agency over their data, and some technology companies and governments are exploring decentralized identity systems that could empower users; Microsoft, Accenture, and Mastercard have announced plans to invest in decentralized models, for example, and Malta's government developed a way for educational institutions to issue blockchain-based academic credentials that are owned by students, portable, and instantly verifiable. It is estimated that governments will have issued about five billion digital IDs globally by 2024, and the majority that have issued them so far are in low- and middle-income countries in Africa and Asia.

Traditionally, governments and banks have played the role of "trust anchor" for financial transactions, though emerging digital-identity models involve new actors (for example, the pharmacy startup Capsule has relied on doctors as a source of trust when filling e-prescriptions for delivery). Related governance efforts include the Pan-Canadian Trust Framework, and the European Union's implementation of an ethical AI strategy. However, the monopolization of online search and social media - and pervasive related personal data gathering - complicate efforts to win digital trust. According to poll results published by Accenture in 2022, internet users are increasingly placing conditions on sharing personal information; 57% will share it if they know it won't be sold or re-shared, and 56% will do so if guaranteed data protection safeguards are in place. While internet users expect personalized experiences, they also expect security and agency over personal data - something that could become a competitive differentiator among companies and organizations. In an always-on, data-rich environment, stakeholders in every industry need to redouble efforts to ensure security, maximize trust, promote practices that place the user at the centre of systems, create collaborative governance mechanisms, and take interactions between human and non-human identities into consideration.

Related topics: Artificial Intelligence, The Digital Economy, Cybersecurity, Economic Growth, Blockchain, Digital Identity, Digital Communications, Internet of Things

2.8 Leading on Inclusion, Sustainability and Trust

Companies have a responsibility to deploy technology in a way that benefits everyone

Businesses must address growing concerns about how technology affects inequality, personal freedoms, and access to decent jobs. Many company leaders are faced with calls from their own customers and employees to make a more positive contribution to society. In 2019, the Business Roundtable, an organization that includes the CEOs of some of the most prominent companies in the world and once defined a company's purpose as serving shareholders, re-defined that purpose to include a commitment to all stakeholders. COVID-19 has underlined the risk of leaving half the world cut off from the internet and the digital economy - at a time when schools have closed, many people have lost jobs, and social media has been needed to both expose racial injustice and rally efforts to confront it. In a digital-first world, there is an opportunity to fundamentally redefine business and reinvent models with renewed purpose. Technology can help ensure the health and well-being of often-remote workforces, increase the transparency of supply chains, reduce carbon emissions, responsibly handle personal data, promote racial equality, and accommodate a more diverse array of potential customers and users.

Many companies have deployed digital tools to support the response to COVID-19. A smartphone app developed by South Korea's KT Corporation, for example, can inform users of outbreaks near their location, and educate them about symptoms and prevention. IBM has meanwhile provided access to its artificial-intelligence-powered technologies to help researchers develop potential treatments for the disease.

Other companies have used technology to look after their own employees, such as Bank of Ireland's increased employee access to a wellness program that includes an app and interactive courses on mental, physical, and financial health. Companies can also advance digital transformation in ways that reduce environmental impact, and provide a means for more people to gain access to important information and services. Though roughly half of the global population still does not use the internet, businesses and governments have an opportunity to collaborate in a way that that better addresses this digital divide. Ultimately, research suggests that those companies that orient their digital transformation plans around a higher purpose are likely to better gain the trust of users, and to be more competitive.

Related topics: Future of Leadership, Global Risks, Systemic Racism, Future of Work, The Digital Economy, Digital Communications, Corporate Governance, Innovation, Sustainability Reporting, Climate Crisis, Circular Economy, Sustainable Development

2.9 Integrity, Trust and Good Governance

They are considered key to both preventing and recovering from corruption, for institutions as well as countries

The general concept of good governance applies to both the public and the private sectors, though it may take on different forms in either setting. Common features of good governance in any context are transparency, accountability, oversight, and integrity. And while good governance plays a much broader role than solely addressing corruption, it is a fundamental element of many anti-corruption approaches - and often goes hand-in-hand with measures and procedures designed more specifically to manage corruption risk. For example, many organizations have put in place anti-bribery and corruption (ABC) programmes, which tend to be overseen by compliance teams and are built around concepts such as codes of conduct, risk assessment, internal controls (particularly within high-risk areas such as gifts and hospitality), conflicts of interest and political engagement, and the adequate maintenance of a whistleblowing channel. At the country level, good governance is often associated with democratic norms - because these tend to provide for greater relative levels of accountability and come atop an underlying assumption that the purpose of government is serving on behalf of the public interest.

Non-democratic regimes can also sometimes feature relatively good governance and lower levels of corruption, though they tend to be exceptions to the rule - because an absence of accountability frequently opens the door to actions that are solely for private gain and not in the public interest. The good governance that can help to avoid this dynamic can also help build and extend trust in both the public and private sectors. For companies, enjoying trust among consumers, regulators, and other stakeholders can effectively grant a social licence to operate, often giving a company the benefit of the doubt if and when it faces operational or reputational challenges. However, such trust may take many years to build. Ultimately, good governance is considered fundamental for increasing resilience to corruption, so the concept has been promoted as an element of international development by institutions such as the World Bank. While this has led to some criticism that it triggers proposed policy solutions that are insensitive to local traditions and contexts, certain fundamental features of good governance - such as the rule of law - are considered universal, and are therefore enshrined in the UN's Sustainable Development Goals.

Related topics: Economic Growth, Justice and Law, Future of Leadership, Trade and Investment, Corporate Governance, Sustainability Reporting, Sustainable Development, Agile Governance, Financial and Monetary Systems

2.10 Inequity and Skills Gaps

Ensuring that cyber resilience is accessible to all

Cyber capacity remains uneven across industries and regions, influenced by differences in skills, resources and digital infrastructure and governance frameworks. Many organiztions face challenges in funding even a baseline level of cybersecurity. This imbalance – described as cyber inequity – creates vulnerabilities that extend beyond individual entities, exposing entire interconnected supply chains to risk. The Forum's Global Cybersecurity Outlook 2026 survey data revealed high degrees of confidence in resilience levels by respondents based in the Middle East and North Africa, while lower levels of resilience are expressed in Latin America and the Caribbean and sub-Saharan Africa. Despite rising confidence in cyber resilience overall, gaps persist: small organizations (by revenue) are twice as likely to feel that they have insufficient resilience

than large organizations. Similarly, divides remain across sectors: 37% of respondents from non-governmental organizations believe they have insufficient resilience to cyber attacks, compared to 23% of public sector respondents and just 11% in the private sector.

Cybersecurity skill shortages are one of the most significant drivers of cyber inequity across regions. The lack of cybersecurity expertise ranks as the second-most significant challenge, after the evolving threat landscape, for survey respondents from non-governmental organizations (51%) and the public sector (57%). When comparing small and large organizations, the data reveals a persistent divide: 46% of small organizations report a lack of cybersecurity skills and expertise, compared with 29% of large organizations. As organizations across industries and geographies become increasingly reliant on digital technologies, the need for a robust cybersecurity workforce has become critical to protecting networks and data from emerging cyber threats. However, several structural barriers continue to discourage individuals from pursuing careers in cybersecurity. These include a lack of clearly defined career paths, outdated or misaligned education and training, costly certification requirements and the high levels of stress associated with cybersecurity roles. To address these challenges, the World Economic Forum developed the Cybersecurity Talent Framework, which aims to help organizations build sustainable cybersecurity talent pipelines. The framework focuses on attracting talent into cybersecurity, improving education and training, recruiting the right talent and retaining cybersecurity professionals. Tackling issues such as limited recognition for cybersecurity roles and high job stress can help organizations build a more loyal and committed workforce, supporting long-term organizational and regional cyber resilience.

Related topics: Education and Skills, Innovation, Corporate Governance, Agile Governance, Parity and Inclusion, Global Gender Gap

2.11 A Breakdown in Trust

From fake news to political incivility to a lack of representation, there is a vicious cycle of mistrust

The exclusion of particular populations from decision-making has become a pivotal factor in the erosion of trust. This denial of representation and voice fosters a deep-seated skepticism of authority - and among traditionally marginalized groups like young people and women, there's now a palpable sense of political disengagement that points to an urgent need for more inclusive governance taking into account diverse perspectives and experiences. Meanwhile a perception of political incivility - of elected representatives defying the very laws they are in office to uphold - is further eroding trust. An apparent disregard for established norms engenders disillusionment, contributing further to the trust deficit. The media's role in shaping related perceptions cannot be understated; negative, divisive portrayals of certain social groups have a cascading effect that contributes to a climate of suspicion and unease. That in turn perpetuates a distancing of communities from the institutions meant to serve them. COVID-19 only amplified these challenges, by demonstrating the potentially deadly impact of false information, and by further weakening social cohesion in many parts of the world to the point of making traditional representative democracy appear to have reached its limits.

The major factors driving this breakdown include the mismanagement of the pandemic, related economic crises, and political instability. Growing global inequality, coupled with the emergence of a large middle class in the Global South that has mounting consumer and lifestyle expectations, have further stressed social cohesion. All of this contributes to a breakdown of trust in political systems and politicians, in Western democracies and authoritarian regimes alike. One way to tackle this problem is to try to come up with new and creative ways of making decisions. In many places, for example, people would like to have more opportunity to vote directly on issues through initiatives and referendums. Another approach involves "deliberative democracy," where people affected the most by a decision come together in an organized way to talk about it. Instead of simply more people participating, it's about having meaningful conversations among those most directly impacted. While people might have once been (mostly) satisfied with being represented by elected legislative representatives and administration officials who are (at least theoretically) working on their behalf, they now place more trust in their peers and in themselves - rather than in institutions.

Related topics: Inequality, Taxes, Agile Governance, Corporate Governance, Emerging-Market Multinationals, Global Governance, Trade and Investment, Artificial Intelligence, Systemic Racism, Human Rights, Science, Corruption, Drivers of Peace

2.12 Geopolitics and Critical Infrastructure

Geopolitics has become a defining force shaping cybersecurity risk

In an increasingly fragmented global environment, geopolitics is reshaping how organizations understand and manage cyber risk. Armed conflicts, sanctions, trade disputes and technological competition now directly influence the cyberthreat landscape. Survey data from the Forum's Global Cybersecurity Outlook 2026 report shows that geopolitics remains the top factor shaping overall cyber risk mitigation. Rather than triggering constant strategic overhauls, geopolitical risk has become a persistent condition that organizations must account for in their daily operations.

One clear response to this volatility is a shift towards intelligence-driven collaboration. Organizations are placing greater emphasis on threat intelligence and deeper engagement with government agencies and information-sharing groups. This reflects a growing recognition that geopolitically motivated cyber threats often target multiple sectors at once and cannot be addressed in isolation. Large global employers are leading this shift: 70% of organizations with more than 100,000 employees report increasing their focus on threat intelligence, compared with only 30% of smaller organizations. Geopolitical instability also increases the likelihood that cyber incidents will have physical consequences, and citical national infrastructure is especially exposed in this environment. Energy, water and transportation systems are attractive targets because disruptions can quickly affect public safety and economic activity. In April 2025, for example, a cyberattack on a Norwegian hydropower dam opened a floodgate for several hours, in what authorities described as deliberate sabotage. Confidence in national preparedness is also weakening: 31% of survey respondents reported low confidence in their country's ability to respond effectively to major cyber incidents, with sharp differences across regions.

Related topics: Geopolitics, Global Risks, Infrastructure, Drivers of Peace, Agile Governance, Global Governance, Drivers of War, Geo-economics

2.13 Disarmament and an Erosion of Trust

The rise of online misinformation and disinformation has created new challenges for treaty compliance

Arms control, disarmament, and non-proliferation help build trust and ensure stability by minimizing the risks of misperception and miscalculation. To that end, countries have agreed to exchange data, monitor compliance, verify agreements, and hold treaty violators to account. For example, the Treaty on the Non-Proliferation of Nuclear Weapons and the Chemical Weapons Convention have sophisticated processes for verification, including detailed declarations by state parties and on-site inspections of relevant facilities to certify declared data. However, arms control, disarmament, and non-proliferation agreements face a number of issues that erode their utility and credibility. One relates to compliance and enforcement: non-compliance concerns have contributed to a stifling or collapse of long-standing bilateral nuclear arms control agreements between the US and the Russian Federation, and compliance- and enforcement-related difficulties have divided state parties to both the Treaty on the Non-Proliferation of Nuclear Weapons and the Chemical Weapons Convention. The Biological Weapons Convention meanwhile lacks an effective architecture for verification, compliance, and enforcement to address allegations of biological-weapons development. The inability of states to properly handle allegations of non-compliance amid heightened geostrategic tension has had a corrosive effect on the credibility of arms control, disarmament, and non-proliferation agreements generally.

A related set of challenges has emerged as a direct result of the growing use of disinformation and misinformation. These are neither entirely new phenomena nor are they new issues specifically for arms control, disarmament, and non-proliferation efforts; ill-founded allegations of association with chemical and biological weapons have long been used to vilify adversaries. However, the increased prevalence of social media and other online platforms provides for a cheaper, faster, and more powerful means of spreading misinformation and disinformation throughout networks of likeminded users. The sheer volume and pace of the spread of distortions, half-truths, and lies has proven difficult to counter. This has indirectly undermined confidence in some of the data and the data collection processes that are at the heart of verifying compliance with treaties, which has weakened trust in the international organizations that uphold regimes, contributed to the polarization of state parties to treaty regimes, and hindered support for the enforcement of treaties. The increasing prevalence of "deepfake" technologies that generate or manipulate video, text, images, and audio in order to mislead, deceive, or influence audiences will likely exacerbate this challenge.

Related topics: Agile Governance, Civic Participation, Drivers of War, Digital Communications, Data Policy,

Global Governance, Geopolitics

2.14 Culture, Integrity and Reputation

Successfully nurturing a culture of integrity and corporate reputation requires going beyond compliance

Culture, integrity, and reputation are fundamental to corporate governance; they have extended beyond traditional boundaries, and are increasingly vital for companies aiming to implement a cohesive global integrity agenda. This agenda should encapsulate core values, regulatory mandates, and voluntary commitments to societal and environmental stewardship - while being adaptable to an evolving external context. Any transition to more robust governance requires a shift from rhetoric to action, and an emphasis on the role of leadership in shaping employee behaviour and establishing a corporate ethos firmly rooted in integrity. Eliminating corporate duplicity and ”greenwashing” requires breaking down silos, and fostering alignment across critical functions like ethics, compliance, risk management, ESG and sustainability, and public affairs. Companies face unprecedented expectations to take clear stances on pressing issues - and without tangible, measurable action to back up their words, accusations of duplicity are likely.

Successful integrity efforts require more than just stringent oversight to prevent regulatory inadequacies, or the appointment of a single individual to helm these efforts; it calls for cultivating an organizational purpose and value system that is authentic and consistently upheld. A true commitment to integrity is reflected in every action a company takes to strengthen its culture, enhance its reputation, and affirm its dedication to ethical conduct and governance. Creating a corporate culture that encourages employees to voice concerns without fear of reprisal is fundamental for maintaining a healthy working environment. It is vital that organizations put in place robust mechanisms for reporting issues, guaranteeing complete anonymity, and educating employees about their responsibility to identify and report such concerns. This can be accomplished by incorporating whistleblowing and incident management protocols into core employee ethics-training programmes. In every case, leadership can play a key role in helping raise awareness by proactively addressing these issues, and fostering an atmosphere of open communication.

Related topics: Corruption, Sustainability Reporting, Behavioural Sciences, Logistics, Corporate Governance, SDG 16: Peace, Justice and Strong Institutions

2.15 Technological Evolution and AI

Ethical challenges and strategic opportunities abound

The rapidly evolving technological landscape has compelled organizations to adopt a data-centric approach, by leveraging vast amounts of information to boost efficiency and drive innovation. This has been accelerated by the dramatic adoption of artificial intelligence, which presents a rich blend of opportunities and challenges - particularly from a compliance perspective. Chief Compliance Officers play a crucial role in ensuring that the integration of new technologies like AI into business operations adheres to a particular ethical and legal framework; this is vital for future-proofing any business in an era of digital transformation. The impact of technological evolution impacts everything from business models and customer interaction, to employee productivity and data management. Automating routine tasks and expediting complex analyses can enable companies to redirect human resources to more strategic operations. Organizations are therefore establishing specialized related governance functions; stringent policies and processes are essential for responsible use, whether via chatbots or large language models, in order to mitigate ethical and operational risks.

The rapid pace of technological advancement creates a need for continuous employee education and upskilling, to ensure the workforce is as proficient as possible with emerging tools. AI can significantly help CCOs monitor regulatory changes, and develop related risk scenarios and assessments. By utilizing AI-driven analytics and forecasting tools, they can access real-time insights and predict potential issues before they escalate. This enables a proactive compliance posture, and dynamic adaptation to developments. Wider adoption of AI and advanced digital analytics also create opportunities for CCOs to pinpoint specific areas of risk more effectively. Instead of attempting to address all potential issues, they can leverage these tools to focus their resources and strategies on the most critical risks. This targeted approach enhances efficiency and enables more effective mitigation of compliance-related risks, in the process transforming the way organizations handle their data and compliance strategies. By navigating the complexities of tech evolution and AI with both strategic foresight and ethical considerations, corporations can foster innovation and growth

in healthy ways - while safeguarding their operations, integrity, and reputations.

Related topics: The Digital Transformation of Business, Cybersecurity, Future of Work, Artificial Intelligence, GovTech, Corporate Governance, Blockchain, Digital Identity, Data Policy, Innovation

2.16 Shifting Geopolitics and Geo-economics

CCOs play integral roles in helping companies navigate an increasingly complex and uncertain global landscape

Significant geopolitical and geo-economic shifts have Chief Compliance Officers leading companies through turbulent times. This requires a multifaceted approach combining external strategies with internal cohesion - a balance that can help ensure that strategic decisions are grounded in both commercial viability and integrity, which is a necessity for any corporation aiming to thrive in the current global marketplace. The evolving regulatory landscape, characterized by changing trade policies and extensive sanctions, poses a particularly dynamic challenge. It calls for agile compliance strategies that enable quick adaptation. CCOs are tasked with not only anticipating sudden shifts, but also integrating related strategies into their organization's compliance framework in ways that ensure operational resilience and adherence to global standards. Corporations are now under increased scrutiny not just from regulatory bodies, but also investors and the public - making transparency, ethical conduct, and a strong compliance culture essential for building trust and maintaining reputation.

Geopolitical tensions and economic uncertainty have also complicated global supply chains, with implications for both trade and regulation. This necessitates proactive risk management, and a clear understanding of ways to mitigate supply chain vulnerabilities to ensure compliance and continuity. Political instability and economic fluctuation have affected everything from labour laws to financial reporting; for global companies, managing these risks means navigating sanctions, trade restrictions, and other political factors that can directly impact operations and client relationships. Fostering an inclusive internal environment is meanwhile essential; being sensitive to the diverse backgrounds of employees can help maintain harmony, while managing external complexities. A CCO's success hinges on an ability to integrate a comprehensive understanding of the geopolitical and economic landscape with strategic agility and internal cohesion. By recognizing external pressures and risks while remaining steadfast in fostering an agile and inclusive corporate culture, companies can better manage global complexities - and ensure that they remain competitive, compliant, and coherent in terms of both operations and ethos.

Related topics: Global Risks, Illicit Economy, Financial and Monetary Systems, Corruption, Disinformation, Global Governance, Trade and Investment, Geopolitics, Drivers of Peace, Corporate Governance, Geo-economics, Justice and Law, Drivers of War, Agile Governance, SDG 16: Peace, Justice and Strong Institutions

2.17 Enterprise and Emerging Risks

Effective risk management is central to both legacy and emerging corporate governance models

Historically, risk identification and mitigation at companies has tended to focus on addressing direct threats to a company's market value. These include preventable, internal issues (such as those related to the health and safety of employees, or to their potential involvement in bribery or fraud), where the goal is typically to get as close as possible to eliminating them entirely. However, companies must also consider strategic, external risks - such as shifting competitive and social dynamics, which can both pose threats and create new opportunities. Companies tend to struggle with managing contemporary, complex, emerging risks. This is due not least to the fact that current dynamics like climate disruption, geopolitical fragmentation, social unrest, rising inequality, polarization, and political dysfunction can accelerate and reinforce one other (some have defined this as an era of "polycrisis"). Building resilience requires greater rigour when it comes to risk identification, monitoring, and remediation. Many companies now recognize that the societal and environmental impact of a business are at the root of that business's risk - and that the ways in which these risks emerge is unpredictable, non-linear, and intertwined.

The need to mitigate risk presents organizations with a range of cross-functional and inter-temporal challenges. Risks often first manifest within particular teams or regions that do not have any internal responsibility for managing the risk in question, and this has several implications. The first is that businesses need to exercise a more practical curiosity about the impacts that they are having on particular stakeholders

and on the wider public, and they need to make good-faith efforts to reduce negative externalities while increasing positive ones. The second is that risk identification and mitigation efforts need to encompass and align with organizational efforts to identify material environmental, social, and governance (ESG) issues through a "double materiality" lens of ESG and financial matters - while clearly differentiating the risks and opportunities each present. The identification of material ESG issues should then become a constant, dynamic exercise of considering the inside-out and outside-in risk and opportunity dimensions of corporate performance. The third is that a clearer understanding of risks can inform strategic capital allocation, and the establishment of ethical guardrails and principles.

Related topics: Civic Participation, Cybersecurity, Corruption, Climate Crisis, Financial and Monetary Systems, Development Finance, Illicit Economy, Global Risks, Small and Medium-Sized Enterprises, Justice and Law, Drivers of War

2.18 Identity Fraud and Cyber Resilience

The increasing amount of personal data being collected and exploited creates security challenges

The growing use of digital identities online - in combination with the massive amount of personal data increasingly being collected by governments, businesses, and everything from wearable devices to household appliances - creates significant vulnerabilities. According to the Identity Theft Resource Center, more than 300 million people had their identities compromised between January and September of 2020 alone, and high-profile breaches have included the 533 million Facebook users who had their phone numbers and personal data leaked online in 2021. COVID-19 has accelerated the need for secure digital identity systems, and most organizations are concerned about the security risk involved in increased remote work during the pandemic. Cultivating trust in digital identity relies not only on ensuring privacy but also that data is being issued, shared, and verified in trusted ways through certified authorities. Other approaches for better securing identities and building resilience and trust include keeping data collection to a minimum, alongside disclosure and informed consent. Bolstering digital literacy and helping people better understand the need for password-free, multi-factor authentication can also help.

Security is essential for trusted digital interaction and must be directly embedded in the design of digital identity systems - especially amid the growing use of biometrics. The World Wide Web Consortium, the US National Institute of Standards and Technology, and the Financial Action Taskforce have defined standards for digital identity security, and the app "itsme" uses elements such as multifactor authentication criteria including biometrics, a mobile phone number, and a SIM card linked to the user - along with a personal code. For the Internet of Things, the European Telecommunications Standards Institute has endorsed security-by-design principles - like ensuring devices are not pre-set with passwords, providing a point of contact for issues, and opting into timely software updates. Completely infallible security is impossible, and security is more of a process than a state of being. Stakeholders in all sectors and industries should take proactive design and policy steps to protect digital identities and personal data in order to regain user trust, provide regulatory, certification and control mechanisms, address data breaches, harmonize standards, and encourage digital skills training.

Related topics: Global Risks, Justice and Law, The Digital Economy, Innovation, Internet of Things, European Union, Cybersecurity, Blockchain

2.19 Cyber Risk and Insurance

Insurers are underwriting more related policies, as they themselves are increasingly exposed to attack

Cyber risk has become a pressing issue both for the insurance sector specifically and for an increasingly digital world generally. According to the World Economic Forum's Global Risks Report for 2019, cyber-attacks ranked among the top 10 risks in terms of both likelihood and impact; the report pointed to massive data breaches during the prior year, the revealing of new hardware weaknesses, and research suggesting the potential use of artificial intelligence to engineer ever-more-potent cyber-attacks. Most respondents in a related survey expected cyber-attacks involving the theft of money and data, as well as disruption of operations, to increase. Insurers are underwriting a growing amount of this risk through cybersecurity insurance policies. According to a report released in 2019, the cybersecurity insurance market was expected to increase annually by nearly 25% until 2024, when it is expected to reach $20.7 billion. Due to its reliance on a proliferation of personal data, healthcare is emerging as the leading target market for

cybersecurity insurance; as much as 80% of the data generated by the healthcare industry is estimated to be stored in the cloud.

The healthcare sector's vulnerability to threat has been exacerbated by the broad adoption of telehealth and telemedicine tools - which have only become increasingly necessary during the COVID-19 pandemic. The amplified size and complexity of cyber risks, coupled with a general lack of related historical data, make their pricing challenging for insurers. On the other hand, insurers themselves are increasingly exposed to cyber-attacks - not least as they deploy advanced insurtech tools based on artificial intelligence, big data, and cloud computing. For example, automobile insurers including TD Insurance are offering premium discounts based on information about policyholders' driving habits that is collected in real-time using mobile apps. Insurers must properly manage and maintain such continuously expanding volumes of data, while protecting them from fraud and theft. AI-powered customer service and claims adjustments, implemented for the greater convenience of policyholders, have also led to vulnerabilities that can be exploited by hackers. Ultimately, insurers' transition to cloud computing for quantitative processes, and greater cyber dependency, have increased the risk of outages for entire platforms and networks in ways that can cause losses and disrupt operations.

Related topics: Entrepreneurship, The Digital Economy, Digital Identity, Mobility Solutions, Corporate Governance, Cybersecurity, Global Risks, Digital Communications, Innovation

2.20 Cyber Resilience

Accelerating digitization prompts a need for integrated defense, prevention and response

Cyber resilience, or shielding critical systems from hackers or internal failures, is an increasingly important strategic goal in a world of fast, cheap technologies that deliver both unprecedented benefits and risks.

A common denominator for any proper resilience approach is a deep understanding of the risks associated with particular business models. This means that companies must go beyond traditional information-technology planning and make risk evaluation a regular part of their strategy – particularly as they integrate emerging technologies such as artificial intelligence or quantum computing.

Because of the global scope of modern, private sector IT networks, their digital security is a public good. The public sector has its own responsibility to ensure that its institutions also incorporate digital resilience. That's because the risk of the misappropriation of digital public infrastructure, like smart electrical grids or communications devices embedded in roads, will only increase over time. Governments and private actors must work together, to develop new ways to sufficiently protect their digital domains.

Related topics: Infrastructure, The Digital Economy, Global Risks, Artificial Intelligence, Cybersecurity

2.21 AI and Cybersecurity

AI is reshaping risk, accelerating both offence and defence

Artificial intelligence is set to be the single biggest force reshaping cybersecurity in the years to come, with 94% of organizations surveyed in the Forum's Global Cybersecurity Outlook 2026 identifying it as the most significant driver of change. The rapid integration of AI systems is expanding the digital attack surface, introducing new weaknesses that existing security tools were never designed to manage. Defenders are also increasingly using AI to strengthen protection – from spotting phishing attempts and unusual network behaviour to speeding up incident response and automating time-consuming analysis. At the same time, attackers are also adopting AI, using it to scale their operations, generate more convincing scams and target victims with greater precision. This dual-use dynamic means AI is both a powerful defensive tool and a force multiplier for cybercrime. As a result, organizations are moving away from purely reactive security models and towards more proactive approaches, while reassessing how governance, oversight and accountability should evolve alongside AI adoption.

This shift is being driven by growing concern over AI-related risks. In the Global Cybersecurity Outlook 2026 survey, 87% of respondents identified AI vulnerabilities as the fastest-growing cyber risk, with data leaks linked to generative AI now ranking as the top concern for the year ahead (34%), ahead of the advancement of adversarial capabilities (29%). Awareness is beginning to translate into action: the share of organizations that assess the security of their AI tools has nearly doubled in one year, rising from 37% in 2025 to 64% in

2026. More organizations are also moving beyond one-off checks, with 40% conducting periodic reviews before deploying AI systems. Still, gaps remain. Around one-third of organizations report having no process at all to validate AI security, even as adoption accelerates. Poorly governed AI can introduce new risks – from misconfigurations and biased decisions to over-reliance on automation or exposure to manipulation – particularly as AI agents proliferate and take on more autonomous roles. The message is clear: AI can significantly strengthen cybersecurity, but only if it is deployed with strong guardrails, security-by-design practices and continuous monitoring that keep human judgement firmly in the loop. Striking the right balance between innovation and control will be critical to ensuring AI enhances, rather than undermines, digital resilience.

Related topics: The Digital Economy, Agile Governance, Illicit Economy, Global Risks, Corporate Governance, Artificial Intelligence

2.22 Data Ethics, Values and Norms

Data can be deployed to solve global problems and achieve the SDGs, with the right oversight

The development and deployment of any emerging technology keys on social values, preferences, and ethical norms. It is important for organizations to understand these factors in a local context before formulating how they will govern data and artificial intelligence; in addition to whether local values and norms are adequately reflected, they should seriously consider the interplay between technology and individual rights, and how to put safeguards in place that incentivize responsible and human-centric development. Ensuring the trustworthiness of an organization's data practices is essential, often for practical reasons; for example, Facebook was sued in the US in 2019, after the Department of Housing and Urban Development alleged the company was violating a prohibition on housing discrimination because its machine learning algorithms functioned like an advertiser that excludes users based on race, ethnicity or religion. Certain foundational elements should be considered at the start of commercial projects: privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and the promotion of human values. Understanding these in the relevant context is necessary for responsible data use.

By using data responsibly, businesses, non-profits, and governments can better address many of the unprecedented social and environmental challenges we now face - not least current and future pandemics, and environmental disasters aggravated by the worsening impacts of climate change. For example, artificial intelligence can play a significant role in achieving the UN Sustainable Development Goals - one study published in 2020 found that AI can enable the accomplishment of 134 targets across all 17 global goals if its development is supported by the necessary regulatory oversight (though it may also inhibit 59 targets). Some of the levers at hand that can help facilitate the use of data for good include global digital trade, the facilitation of equitable access to data flows, and responsible data collection. Technical elements such as data portability and interoperability are also important. The need to mitigate risks calls for putting firm safeguards in place related to cybersecurity, encryption, risk management, accountability, and overall data protection. Some uses of data and machine learning present particular sets of risks, like privacy breaches and phishing attacks.

Related topics: Corporate Governance, Pandemic Preparedness and Response, Systemic Racism, Global Risks, Agile Governance, Justice and Law, Social Justice, Climate Crisis, Artificial Intelligence, Cybersecurity, Sustainable Development

2.23 Cyber Cooperation and Regulation

Disrupting cybercrime through multistakeholder collaboration

Global efforts to combat cyber-enabled crime are gaining momentum. In late 2024, the United Nations General Assembly adopted the Convention against Cybercrime after five years of negotiation. Around the world, law enforcement agencies are enhancing their cross-border coordination and intelligence-sharing capabilities, increasingly supported by expert insights from the private sector and international partnerships. In March 2026, the United Nations Office on Drugs and Crime and INTERPOL co-organized the Global Fraud Summit, which aimed to build high-level dialogue, political and law enforcement commitments, and effective cross-sector collaboration. That summit comes after several significant disruptions of cybercrime networks across South-East Asia, Africa and Europe in 2025. Civil society and the private sector are also coordinating efforts. The Global Anti-Scam Alliance, for instance, is leveraging the Global Signal Exchange to enhance

real-time insights into the supply chains that enable scams. In parallel, the World Economic Forum's Partnership Against Cybercrime, in collaboration with the Institute for Security and Technology, in late 2025 published Fighting Cyber-Enabled Fraud: A Systemic Defence Approach, a white paper outlining a shared responsibility model designed to disrupt cyber-enabled fraud at scale.

The proliferation of cybersecurity and technology regulations globally reflects an accelerating effort to codify trust and accountability. However, these developments also highlight how regions are advancing at different speeds and with differing priorities, leading to a patchwork of obligations that can be difficult for multinational organizations to reconcile. Nevertheless, the Global Cybersecurity Outlook 2026 survey found that 74% of respondents held a positive view of the effectiveness of cyber-related regulations. Practitioners most frequently noted that these regulations help chief information security officers raise cybersecurity awareness at the board level (58%) and drive tangible improvements in overall security posture (55%). At the same time, 18% of respondents cited challenges in ensuring that third-party vendors comply with diverse requirements, while others pointed to difficulties in fully understanding the applicability of regulations across business units and to limited internal resources and expertise (16%). Moreover, respondents based in markets where such regulations are more mature, such as Europe and North America, face greater difficulty in applying them consistently across borders. This is reflected in the fact that survey results reveal a slightly lower perception of the actual effectiveness of cyber-related regulations in those regions – 30% in Europe and 29% in North America – possibly reflecting the fact that more advanced regulatory environments can also introduce greater complexity and compliance burdens.

Related topics: The Digital Economy, Justice and Law, Global Governance, Regulatory Innovation, Future of Consumption, Agile Governance, Corporate Governance

2.24 Corruption and Impunity

When illicit trade is allowed to flourish, it spawns a culture of impunity

Organized crime and illicit economies are increasingly prominent sources of political corruption - as criminal networks pour money into forging alliances with officials and their intermediaries. According to a 2022 estimate from the Stockholm International Peace Institute, some $1.6 trillion (or 2.7% of global GDP) is being laundered annually. The consequences of this for economic development are devastating. According to the United Nations Conference on Trade and Development (UNCTAD), $89 billion is lost annually to corruption in Africa alone, or twice what is received in foreign aid. Transactional corruption of law enforcement and public officials not only diverts resources, in countries with weak institutions the receipt of a bribe is increasingly perceived as a right of office holders, and its payment as a cost of doing business. According to the Global Initiative Against Transnational Organized Crime (GI-TOC)'s Global Organized Crime Index, the vast majority of the world's population lives in countries with high levels of criminality (79.2%), and low levels of resilience (79.4%). The index found a strong correlation between this low resilience and the presence of state-embedded criminal actors facilitating illicit economies.

Distrust in politicians is generally increasing, alongside the distortion of markets, the undermining of public infrastructure, and the disengagement of citizens. Crime and corruption are further facilitated by a decrease in stigma associated with illegal acts, which are regularly used to gain political power or to buy legitimacy with the public. A lack of law enforcement, penalties, or any deterring government presence runs the risk of increasing complicity over time. In Afghanistan, where governance is generally weak, corruption and abuses of power linked to the drug trade have further crippled the efficiency of the state, hindering its ability to provide essential public services and undermining trust in state institutions. Already, prior to the Taliban's takeover of the country in 2021, the insurgent group had taken advantage of institutional weakness in many areas of Afghanistan to become a provider of security in ways that furthered its influence as it benefited from unobstructed engagement with illicit economies. In other parts of the world, the links between political, criminal, and business elites are becoming ever closer - fuelling organized corruption, deepening inequality, strengthening criminal governance, and causing unpredictability in international affairs.

Related topics: Justice and Law, Social Protection, Corporate Governance, Global Governance, Economic Growth, Agile Governance, Corruption, Human Rights, Civic Participation, Social Justice, Taxes

2.25 Trust and Privacy

Trust in data-based applications is diminishing, as privacy concerns are not effectively addressed

Global dialogue around the governing and safeguarding of personal data is polarized. The often conflicting objectives of governments, businesses and private citizens result in a complicated and often emotional discourse – which hinders informed decision-making. Personal data is increasingly seen as a pervasive, 21st-century asset class, like a stock or bond. That comes as business models are being built around unprecedented opportunities to create value through the flow of such data. According to the 2014 World Economic Forum report Personal Data: The Emergence of a New Asset Class, trust between individuals, governments and companies is necessary in order to fully unlock its potential.

Yet there is a crisis of trust, as stakeholders struggle to agree upon a personal data framework that is reliable and fair. Existing legal frameworks will prove inadequate, due to the speed of change and uncertainty about appropriate rights and responsibilities. The establishment of effective new frameworks must involve a truly democratic approach, if the public's trust in data governance is to be restored.

Related topics: Cybersecurity, The Digital Economy

2.26 Consumer Trust and Transparency

In countries where consumer spending is needed to fuel the global economy, trust in businesses is lagging

Large emerging markets like India and China, where an expanding middle class is expected to buoy the global economy with growing consumer spending in the coming years, are home to notable lags in public trust among the "mass population" in businesses and government, according to the 2019 Edelman Trust Barometer - a survey of 33,000 respondents conducted in more than two dozen markets. According to the barometer, more than two-thirds of respondents agreed that they might be encouraged to buy products from a company with a good reputation - but unless they genuinely came to trust the company behind the product, they would stop buying it. As global consumers become more connected and empowered thanks to digital innovation, they will only place more scrutiny on businesses. For corporate leaders, this means having to strike the right balance between short-term gains and long-term value creation. According to the Edelman Trust Barometer, one means of winning external trust is by investing internally in employees; 78% of barometer respondents agreed with the idea that the way a company treats its employees is one of the best indicators of its level of trustworthiness.

People have fundamental concerns about the safety and quality of the goods they consume. In China, for example, worries about food and medicine safety have become significant (particularly among wealthier consumers) in recent years, according to a report published by the World Economic Forum in 2018. In addition, these affluent, urban-dwelling consumers in China have particular concerns related to the historical role of fake products in the country, according to the report. Another growing area of consumer concern is related to transparency in supply chains - whether it's tied to sustainable sourcing or ethical labour standards. In the apparel sector, efforts have been made by the Sustainable Apparel Coalition and Better Work, a collaboration between the UN's International Labour Organization and the International Finance Corporation, to improve working conditions and sustainability by, for example, introducing standards to measure social and environmental impact. Data privacy is also a serious consumer concern. A relatively small group of companies including Facebook and Amazon (or, in China, Alibaba and JD.com) control large amounts of consumer data - which will present trust issues, as new means of refining and selling that data emerge.

Related topics: Artificial Intelligence, Global Governance, Digital Communications, Internet of Things, Future of Leadership, Corporate Governance

2.27 Stakeholder Engagement and Cultivating Trust

Building trust is an interactive endeavour based on honest dialogue and genuine efforts to address issues

Traditional notions of corporate governance are primarily defensive. They focus on protecting shareholder value, primarily through the proactive management of regulatory and reputational risk. Managing reputational risk tends to be a contained activity; it treats corporate messaging as an end in itself, which is divorced from a company's underlying conduct. But in the current atmosphere of heightened suspicion, rising expectations for greater transparency, and increased employee, shareholder, and public activism, companies can no longer simply rely on crafting attractive narratives about their achievements. Indeed, a backlash triggered by allegations of greenwashing and the gross exaggeration of corporate-responsibility efforts has emerged. As we progress into the mid-21st century, a more trusting and interactive relationship with stakeholders is at the centre of value creation - and is key to gaining a long-term social license to operate. While the definition of

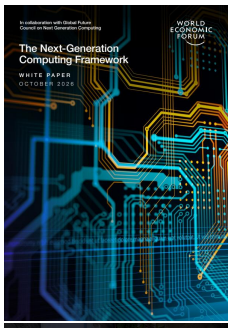
”trust” in an organization remains hotly debated, it might best be considered an expectation of ethical behaviour, based on a mutual confidence that one party will not exploit the other. This type of trust includes an anticipation of reliability, honesty, fairness, competence, respect, and transparency.

Crucially, this trust also relies on a corporation exercising practical curiosity about its impact on human beings - and making good faith efforts to reduce harm as value is increased. Arguably, this generally aligns with how most people believe a business should behave. Leading companies recognize that building trust is an interactive endeavour, based on transparent, honest dialogue, a corporate commitment to keeping one’s word, and a genuine effort to understand and address impacts on stakeholders that are both local and global. The Business Roundtable’s 2019 statement on the purpose of a corporation (focused on ”stakeholder capitalism”) demonstrated a new commitment among business leaders to balancing stakeholder interests for the greater benefit of society. In practice, though, corporations have been taking stands on social and political issues that are not always accompanied by meaningful action. A more robust approach necessitates thinking carefully about stakeholder conflicts and trade-offs, and determining where best to focus. Decisions grounded in actual impact are likely to be more beneficial than falsely suggesting an ability to address and resolve all stakeholder concerns - including those where a company has limited leverage.

Related topics: Future of the Environment, Global Gender Gap, Artificial Intelligence, Systemic Racism, Agile Governance, Climate Crisis, Civic Participation, Sustainability Reporting, Future of Work, Future of Leadership, Social Protection

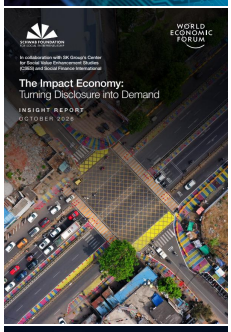
3 Further exploration

Explore the latest World Economic Forum reports related to Trust, Security, and Regulatory Compliance.



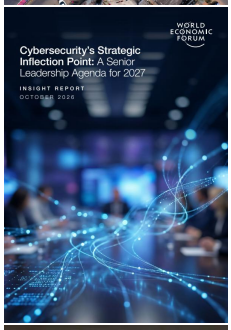
09 October 2026

The Next-Generation Computing Framework



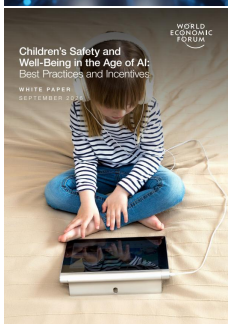
08 October 2026

The Impact Economy: Turning Disclosure into Demand



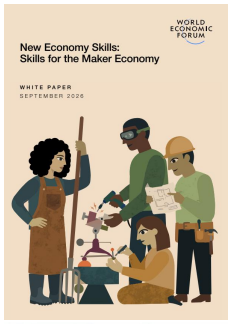
06 October 2026

Cybersecurity's Strategic Inflection Point: A Senior Leadership Agenda for 2027



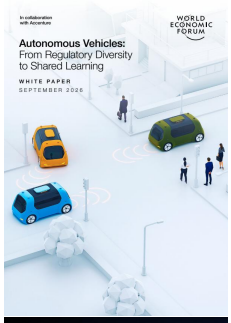
30 September 2026

Children's Safety and Well-Being in the Age of AI: Best Practices and Incentives



24 September 2026

New Economy Skills: Skills for the Maker Economy



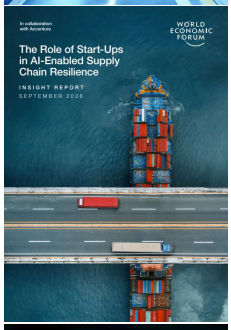
24 September 2026

Autonomous Vehicles: From Regulatory Diversity to Shared Learning



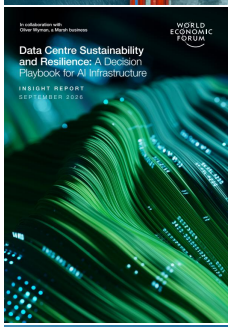
23 September 2026

The Resilience-to-Growth Circularity Playbook for Industrial Solutions and Manufacturing



21 September 2026

The Role of Start-Ups in AI-Enabled Supply Chain Resilience



21 September 2026

Data Centre Sustainability and Resilience: A Decision Playbook for AI Infrastructure



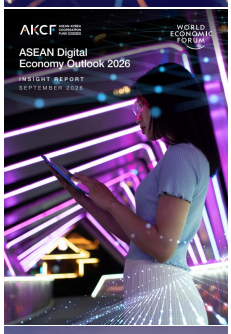
18 September 2026

Risk Management, Reimagined: Outlook to 2035



15 September 2026

The New Global Security Stakeholders: How Public-Private Cooperation Can Advance Security and Stability



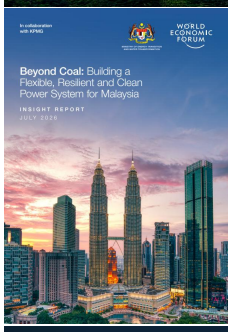
14 September 2026

ASEAN Digital Economy Outlook 2026



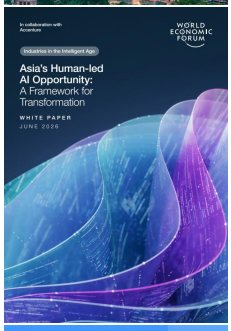
17 August 2026

Intelligent Industrial Ecosystems: Turning Proximity into Intelligence



01 July 2026

Beyond Coal: Building a Flexible, Resilient and Clean Power System for Malaysia



22 June 2026

Asia's Human-led AI Opportunity: A Framework for Transformation



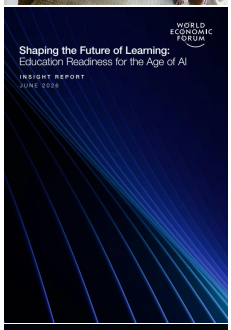
11 June 2026

The Fourth Industrial Revolution Network 2024–2025 Impact Report



09 June 2026

AI for Impact: The Role of Artificial Intelligence in Social Innovation in Asia



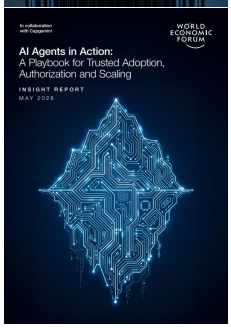
04 June 2026

Shaping the Future of Learning: Education Readiness for the Age of AI



03 June 2026

Preparing for the Future: The Pillars of Digital Safety Foresight



26 May 2026

AI Agents in Action: A Playbook for Trusted Adoption, Authorization and Scaling

References

1. Geneva Centre for Security Policy (GCSP), *"Verification 2.0: A New Approach to Outer Space Security Verification"*: www.gcsp.ch
2. NextBillion, *"Impact Entrepreneurship During the Polycrisis: An Interview with Laurie Lane-Zucker"*: nextbillion.net
3. The Conversation, *"Can the Greens stick to their democratic principles?"*: theconversation.com
4. The Conversation (Spanish), *"La IA no transforma a las empresas: lo hace su capacidad para aprender a cambiar"*: theconversation.com
5. LSE Business Review, *"Ending modern slavery will take more than corporate reporting"*: blogs.lse.ac.uk
6. World Economic Forum, *"Japan is combining tech and human connection to help people live well until 100"*: www.weforum.org
7. GovLab - Living Library, *"Trust in Federal Government Sinks to New Depths"*: thelivinglib.org
8. The Conversation (French), *"Gare aux boycotts ! En temps de guerre, les entreprises doivent protéger leur réputation"*: theconversation.com
9. Asian Development Bank, *"Asian Development Blog: Not All Dzud Are Alike: Three Ways to Help Mongolia's Herders Recover From Deadly Winters"*: blogs.adb.org
10. Project Syndicate, *"Strict Liability for AI Executives"*: www.project-syndicate.org
11. The Conversation (Spanish), *"Cuando el fútbol apaga internet: el impacto de los bloqueos indiscriminados de IP"*: theconversation.com
12. World Economic Forum, *"Zero trust and clear accountability are the new baseline for AI cybersecurity"*: www.weforum.org
13. The Conversation (French), *"Protestations lycéennes, gilets jaunes, ces mouvements qui défient l'ordre politique"*: theconversation.com
14. German Institute for International and Security Affairs, *"Sea Lanes at Risk, Maritime Order under Threat"*: www.swp-berlin.org
15. LSE Business Review, *"The hidden uncertainty behind emissions data produced by British supermarkets"*: blogs.lse.ac.uk
16. Project Syndicate, *"How a Pause on Frontier AI Could Work"*: www.project-syndicate.org
17. GovLab - Living Library, *"Professionalizing deliberation: a Social Network Analysis of UK climate mini-publics"*: thelivinglib.org

About Strategic Intelligence

Our approach

In today's world, it can be difficult to keep up with the latest trends or to make sense of the countless transformations taking place. How can you decipher the potential impact of rapidly unfolding changes when you're flooded with information - some of it misleading or unreliable? How do you continuously adapt your vision and strategy within a fast-evolving global context? We need new tools to help us make better strategic decisions in an increasingly complex and uncertain environment.

This live briefing on Trust, Security, and Regulatory Compliance, harnesses the World Economic Forum's Strategic Intelligence platform to bring you the very latest knowledge, data and context from our 300+ high quality knowledge sources. Its aim is to help you understand the global forces at play in relation to Trust, Security, and Regulatory Compliance and make more informed decisions in the future.

Each day, our Strategic Intelligence platform aggregates, distills and synthesizes thousands of articles from around the world. We blend the best of human curation with the power of machine learning to surface high-quality content on over two hundred global issues to our one million users globally. Our hand-picked network of content partners from around the world means that we automatically exclude much of the noisy clickbait, fake news, and poor quality content that plague the Internet at large. We work with hundreds of think tanks, universities, research institutions and independent publishers in all major regions of the world to provide a truly global perspective and we are confident that our data are well positioned when it comes to the intrinsic biases inherent to open text analysis on uncurated content from the Internet. For further context on our approach, you may be interested to read Strategic trend forecasting: anticipating the future with artificial intelligence and These Are The 3 Ways Knowledge Can Provide Strategic Advantage.

Overview of methodology

Our Transformation Maps are dynamic knowledge visualisations. They help users to explore and make sense of the complex and interlinked forces that are transforming economies, industries and global issues. The maps present insights written by experts along with machine-curated content. Together, this allows users to visualise and understand more than 250 topics and the connections and inter-dependencies between them, helping in turn to support more informed decision-making by leaders.

The maps harness the Forum network's collective intelligence as well as the knowledge and insights generated through our activities, communities and events. And because the Transformation Maps are interlinked, they provide a single place for users to understand each topic from multiple perspectives. Each of the maps has a feed with the latest research and analysis drawn from leading research institutions and media outlets around the world.

At the centre of each map is the topic itself. This is surrounded by its "key issues", the forces which are driving transformation in relation to the topic. Surrounding the key issues are the related topics which are also affected by them. By surfacing these connections, the map facilitates exploration of the topic and the landscape within which it sits.

The framework extends beyond mapping current trends by incorporating forecasts and scenarios to project potential future states of the system. Forecasts are based on observable patterns, while scenarios explore broader possibilities, including low-probability but high-impact events. These elements contextualize key issues and related topics within potential future trajectories, enhancing strategic thinking and decision-making.

Harnessing collective intelligence from the Forum network and leading research institutions, the maps synthesize diverse insights into a cohesive view. By integrating these insights with the latest research and analysis, the framework provides a comprehensive understanding of how transformations unfold and interrelate, empowering users to navigate the evolving landscape effectively.

Scenarios

In-line with best practice on the use of artificial intelligence in products and systems, in this section we provide full transparency on how artificial intelligence is used in our scenario generation automation.

In complex and fast-moving environments, it is difficult to maintain a clear view of what may change next, and which uncertainties deserve attention. Scenario planning helps by offering a structured way to explore alternative futures, test assumptions and clarify decisions under uncertainty.

We generate scenario packs using artificial intelligence within a defined methodology and on which we have been guided by our Global Strategic Foresight Community. The process follows the same broad logic used in scenario workshops: move from issue framing, to key uncertainties, to a 2×2 matrix, and then to four distinct scenario narratives. In an automated setting, each step includes validation to avoid weak axes and indistinct scenarios.

Each scenario pack included in our briefings includes a 2×2 scenario matrix defined by two critical uncertainties (axes), four scenario narratives and a *throughline* that connects each scenario back to the matrix.

Our process is as follows:

1. Topic framing and inputs. First, we ground our scenario design in our high-quality, expert curated content. Our topic summaries, key issues and related knowledge are used to anchor scenarios in the topic space.

2. Abstraction of underlying forces. Topic issues are often technical and uneven in granularity. Our AI agents abstract them into a small set of cross-cutting forces and tensions that can support scenario work across domains. This creates a conceptual frame that is usable for uncertainty and axis generation.

3. Identification of drivers and uncertainties. From that conceptual frame, an AI agent identifies drivers that could shape outcomes and that carry genuine uncertainty. Drivers are defined with directional poles so that they can support different regime logics rather than incremental variation.

4. Axis generation and validation. An AI agent then proposes multiple candidate axes of uncertainty and

another agent then evaluates them against criteria commonly used in facilitated scenario work: strength of the tension between poles, relevance to the topic and its drivers, and decision utility, meaning whether different positions would change strategic choices. Candidate axes are then combined into matrix pairs and tested for distinctiveness. This step is designed to avoid quadrant ”collapse”, where scenarios converge in practice despite different labels. Candidate pairs that do not yield clearly differentiated quadrants are rejected and alternatives are tried.

5. Quadrant blueprints using STEEPLE. Once an axis pair is selected, our AI develops a structured blueprint for each quadrant. Blueprints define the internal logic of that world and describe how the system behaves across STEEPLE domains (Social, Technological, Economic, Environmental, Political, Legal and Ethical), with attention focused on the domains that are most consequential for that quadrant. This stage is designed to establish coherence and contrast before narrative writing begins.

6. Grounding and counter-grounds. Our AI then builds an evidence set from the Strategic Intelligence knowledge base, drawing on our curated network of trusted content partners. Evidence is used to strengthen and challenge the emerging interpretation of each quadrant. In practice, our AI compiles supporting evidence for key mechanisms implied by the blueprint, as well as counter-evidence and constraints that suggest limits, failure modes or alternative dynamics. This step functions as a stress test. It identifies claims that are too thin, overly linear, or inconsistent with available knowledge, and it provides material used to refine the narrative direction before writing begins.

7. Narrative development within a constrained world. Once a narrative direction has been selected for a quadrant, our AI produces the scenario narrative within a constrained ”world”, mirroring workshop practice where participants explore a defined quadrant logic and then build out a coherent future state. At this stage, our models are instructed to remain consistent with the quadrant blueprint, incorporate supporting evidence where it adds credibility and specificity, reflect counter-evidence as tensions, constraints, trade-offs or contested dynamics, and describe a plausible future state rather than a transition story, prediction or recommendation. The result is a scenario that remains anchored to a defined structure while allowing creative exploration of how that structure could plausibly play out. Our AI also generates a short throughline for each scenario explaining how it expresses its position on the axes, as well as a matrix summary describing the uncertainty space and what differentiates the four futures.

8. Quality checks and transparency. Finally, an AI agent performs quality checks intended to prevent common failure modes in automated scenario generation: axes that lack meaningful tension or strategic relevance, quadrant ”collapse” where scenarios become minor variations of the same future, internally inconsistent causal logic across STEEPLE domains, and narratives that drift away from the quadrant blueprint. Intermediate artefacts (candidate axes, evaluations, quadrant blueprints, and grounding materials) are retained so results can be reviewed, compared over time, and improved.

We welcome feedback on our approach as we continue to refine and evolve our use of artificial intelligence in strategic foresight.

Continue online

Our suite of Strategic Intelligence tools are available to help you keep up to date across over 300 topics.

On the web

Visit Strategic Intelligence on your desktop or laptop. All modern browsers supported.

In the app stores

You can find our Strategic IQ app on the Apple App Store, Google Play Store or Huawei App Gallery.

Download on the App Store

GET IT ON Google Play

You can also follow Strategic Intelligence on Twitter.

Contributors

World Economic Forum	**Co-curator**

Acknowledgements

Content Providers featured in this briefing

Asian Development Bank

Geneva Centre for Security Policy (GCSP)

German Institute for International and Security Affairs

GovLab - Living Library

LSE Business Review

NextBillion

Project Syndicate

The Conversation

The Conversation (French)

The Conversation (Spanish)

World Economic Forum

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org