Economic and Social Commission for Western Asia

Navigating the Future: Building Trust in Digital Public Services Through Emerging Technologies

Workshop on Building Trust in Digital Government Services, Beirut, 11-12 September 2023

UNITED NATIONS
الاسكوا
ESCWA

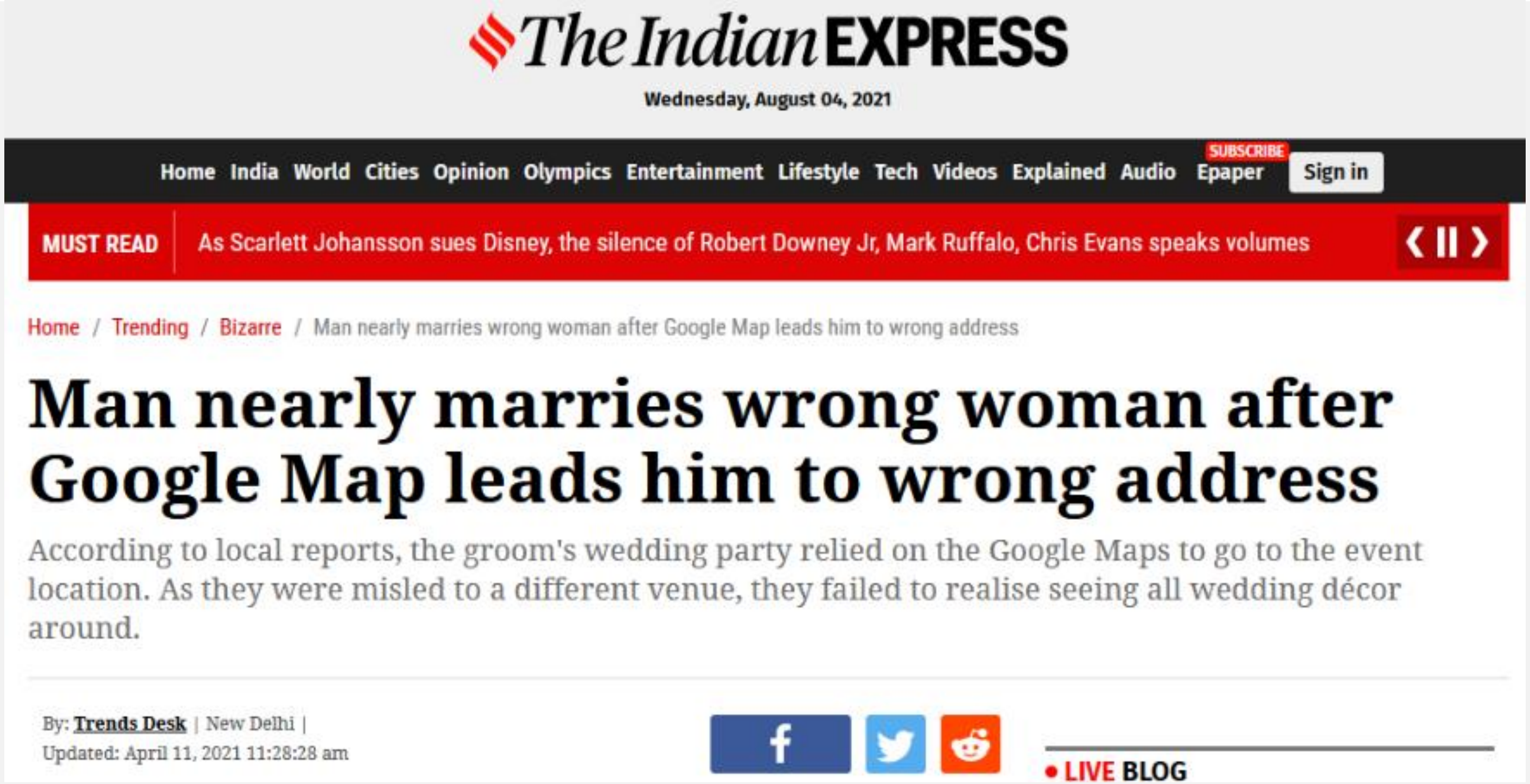
Shared Prosperity **Dignified Life**

AICTO

Internet Society

ITU

Why this topic?


The Indian EXPRESS
Home India World Cities Opinion Olympics Entertainment Lifestyle Tech Videos Explained Audio SUBSCRIBE Epaper Sign in
LIVE BLOG

Wednesday, August 04, 2021

MUST READ As Scarlett Johansson sues Disney, the silence of Robert Downey Jr, Mark Ruffalo, Chris Evans speaks volumes

Home / Trending / Bizarre / Man nearly marries wrong woman after Google Map leads him to wrong address

Man nearly marries wrong woman after Google Map leads him to wrong address

According to local reports, the groom's wedding party relied on the Google Maps to go to the event location. As they were misled to a different venue, they failed to realise seeing all wedding décor around.

By: **Trends Desk** | New Delhi |
Updated: April 11, 2021 11:28:28 am

https://indianexpress.com/article/trending/bizarre/man-nearly-marries-wrong-woman-after-google-map-leads-him-to-wrong-address-7266380/

Agenda

Digital Public Services

The Trust

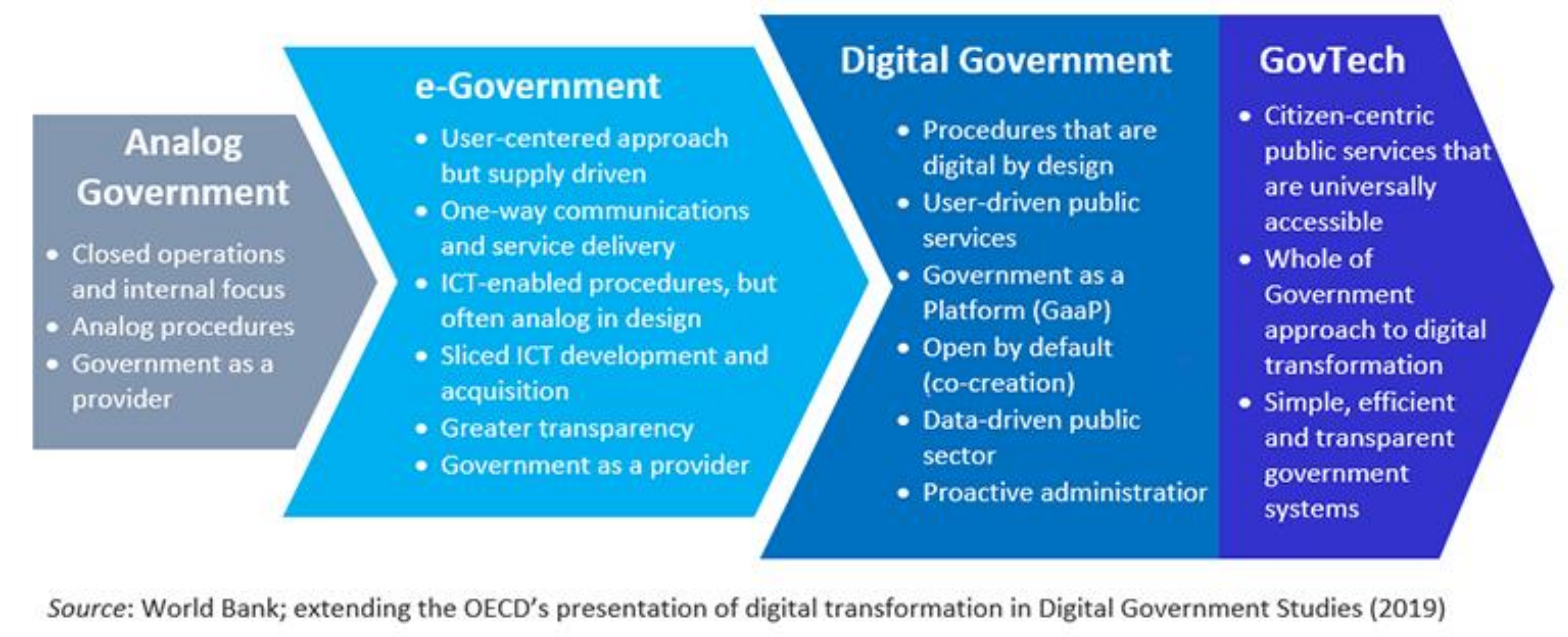
Emerging Technologies

Trust Through Emerging Technologies

Q&A

‘Digital’ Public Services

Digital Public Services



Analog Government

- Closed operations and internal focus
- Analog procedures
- Government as a provider

e-Government

- User-centered approach but supply driven
- One-way communications and service delivery
- ICT-enabled procedures, but often analog in design
- Sliced ICT development and acquisition
- Greater transparency
- Government as a provider

Digital Government

- Procedures that are digital by design
- User-driven public services
- Government as a Platform (GaaP)
- Open by default (co-creation)
- Data-driven public sector
- Proactive administratior

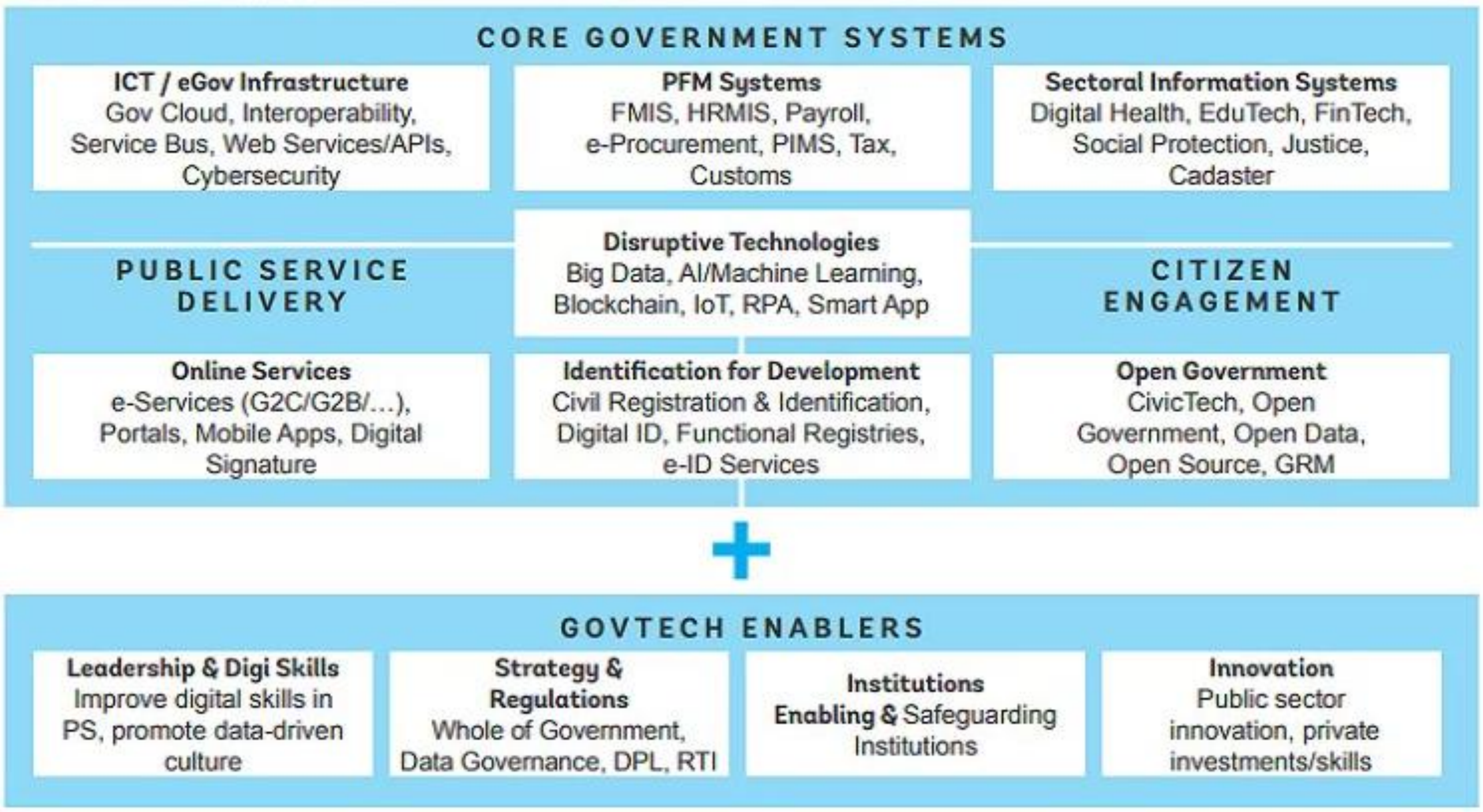
GovTech

- Citizen-centric public services that are universally accessible
- Whole of Government approach to digital transformation
- Simple, efficient and transparent government systems

Source: World Bank; extending the OECD's presentation of digital transformation in Digital Government Studies (2019)

https://www.worldbank.org/en/programs/govtech/priority-themes

Focus Areas



CORE GOVERNMENT SYSTEMS

ICT / eGov Infrastructure
Gov Cloud, Interoperability, Service Bus, Web Services/APIs, Cybersecurity

PFM Systems
FMIS, HRMIS, Payroll, e-Procurement, PIMS, Tax, Customs

Sectoral Information Systems
Digital Health, EduTech, FinTech, Social Protection, Justice, Cadaster

PUBLIC SERVICE DELIVERY

Disruptive Technologies
Big Data, AI/Machine Learning, Blockchain, IoT, RPA, Smart App

CITIZEN ENGAGEMENT

Online Services
e-Services (G2C/G2B/…), Portals, Mobile Apps, Digital Signature

Identification for Development
Civil Registration & Identification, Digital ID, Functional Registries, e-ID Services

Open Government
CivicTech, Open Government, Open Data, Open Source, GRM

GOVTECH ENABLERS

Leadership & Digi Skills
Improve digital skills in PS, promote data-driven culture

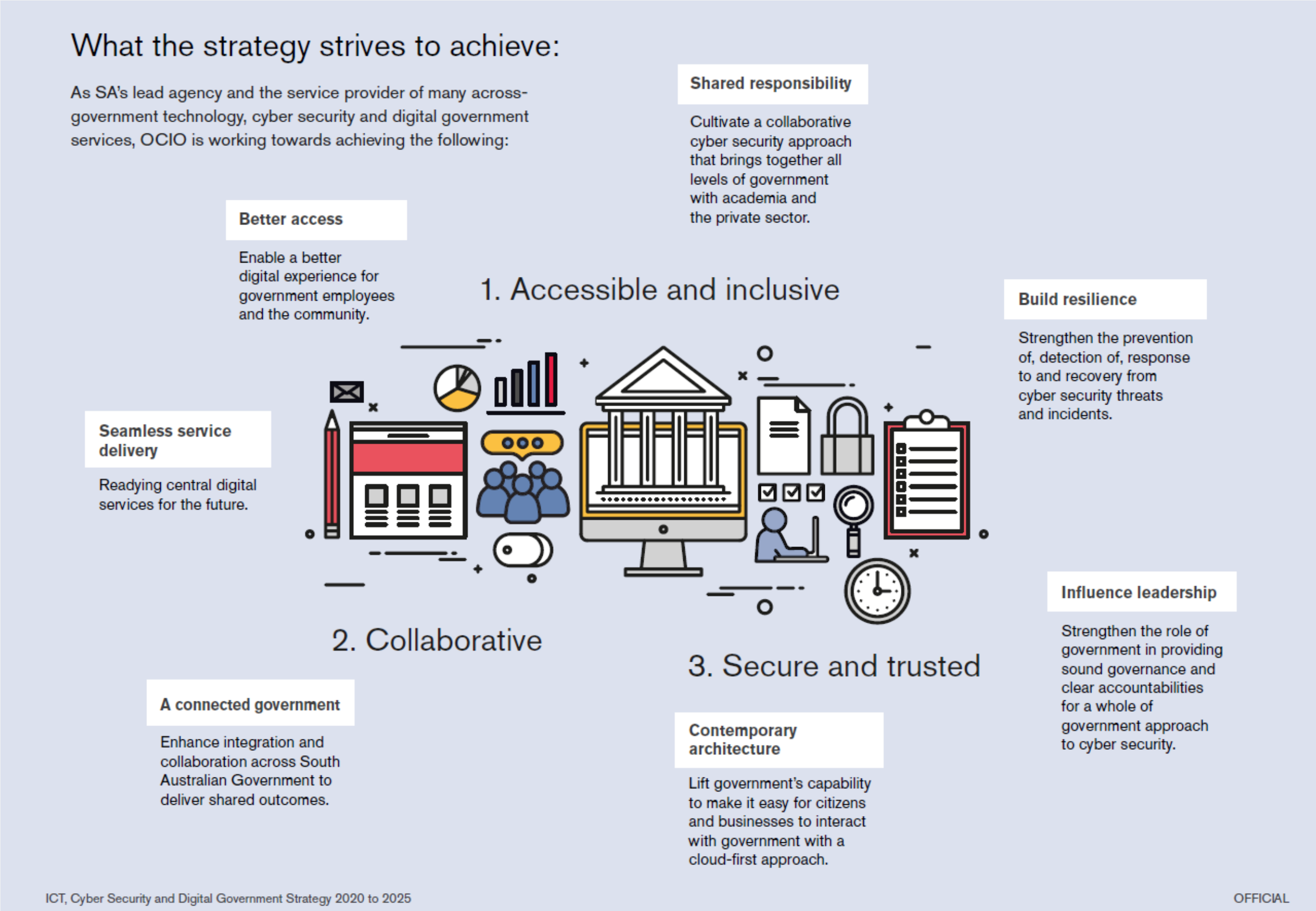
Strategy & Regulations
Whole of Government, Data Governance, DPL, RTI

Institutions
Enabling & Safeguarding Institutions

Innovation
Public sector innovation, private investments/skills

https://www.worldbank.org/en/programs/govtech/priority-themes

Digital Government Strategy – South Australia



What the strategy strives to achieve:

As SA's lead agency and the service provider of many across-government technology, cyber security and digital government services, OCIO is working towards achieving the following:

1. Accessible and inclusive

Better access

Enable a better digital experience for government employees and the community.

Shared responsibility

Cultivate a collaborative cyber security approach that brings together all levels of government with academia and the private sector.

Seamless service delivery

Readying central digital services for the future.

2. Collaborative

A connected government

Enhance integration and collaboration across South Australian Government to deliver shared outcomes.

3. Secure and trusted

Build resilience

Strengthen the prevention of, detection of, response to and recovery from cyber security threats and incidents.

Influence leadership

Strengthen the role of government in providing sound governance and clear accountabilities for a whole of government approach to cyber security.

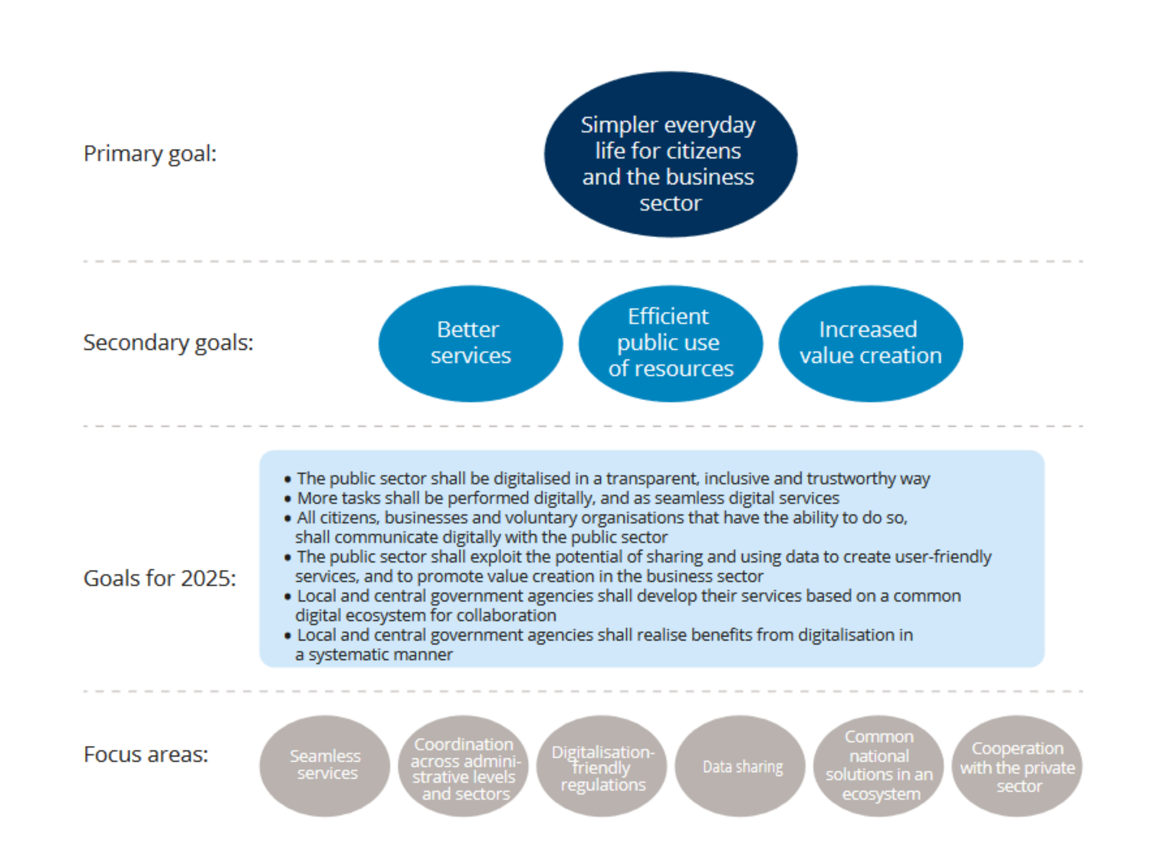
Contemporary architecture

Lift government's capability to make it easy for citizens and businesses to interact with government with a cloud-first approach.

ICT, Cyber Security and Digital Government Strategy 2020 to 2025

OFFICIAL

Digital Strategy for Public Sector - Norway



Primary goal:

Simpler everyday life for citizens and the business sector

Secondary goals:

Better services

Efficient public use of resources

Increased value creation

Goals for 2025:

- The public sector shall be digitalised in a transparent, inclusive and trustworthy way
- More tasks shall be performed digitally, and as seamless digital services
- All citizens, businesses and voluntary organisations that have the ability to do so, shall communicate digitally with the public sector
- The public sector shall exploit the potential of sharing and using data to create user-friendly services, and to promote value creation in the business sector
- Local and central government agencies shall develop their services based on a common digital ecosystem for collaboration
- Local and central government agencies shall realise benefits from digitalisation in a systematic manner

Focus areas:

Seamless services

Coordination across administrative levels and sectors

Digitalisation-friendly regulations

Data sharing

Common national solutions in an ecosystem

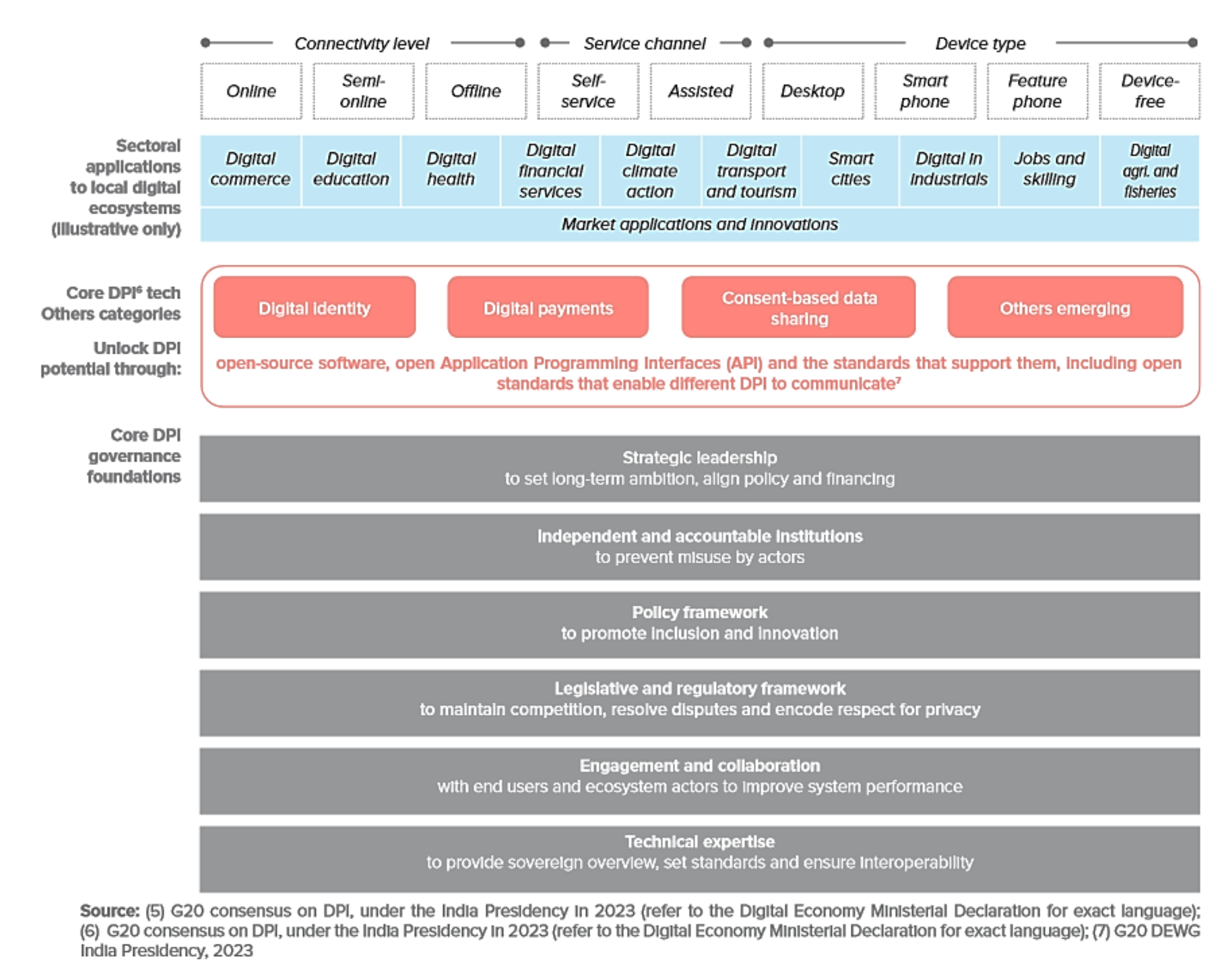
Cooperation with the private sector

One digital public sector, Digital strategy for the public sector 2019-2025, Ministry of Local Government and Modernisation, Norway

> *“Governments of different creeds are struggling – and frequently failing – to meet the expectations of citizens, as evidenced by a lack of confidence in government institutions and events in recent political history.* ***New thinking*** *is needed to address changes in technology, media, and public expectations.”*

Eraneos, Doing Digital for Impact: Study on Digital Transformation in the Public Sector, Research Paper, Kings College London, 2022

G20 – Digital Public Infrastructure



Connectivity level			Service channel		Device type			
Online	Semi-online	Offline	Self-service	Assisted	Desktop	Smart phone	Feature phone	Device-free

Sectoral applications to local digital ecosystems (illustrative only)

Digital commerce | Digital education | Digital health | Digital financial services | Digital climate action | Digital transport and tourism | Smart cities | Digital in industrials | Jobs and skilling | Digital agri. and fisheries

Market applications and innovations

Core DPI[6] tech Others categories

Digital identity | Digital payments | Consent-based data sharing | Others emerging

Unlock DPI potential through:

open-source software, open Application Programming Interfaces (API) and the standards that support them, including open standards that enable different DPI to communicate[7]

Core DPI governance foundations

Strategic leadership
to set long-term ambition, align policy and financing

Independent and accountable institutions
to prevent misuse by actors

Policy framework
to promote inclusion and innovation

Legislative and regulatory framework
to maintain competition, resolve disputes and encode respect for privacy

Engagement and collaboration
with end users and ecosystem actors to improve system performance

Technical expertise
to provide sovereign overview, set standards and ensure interoperability

Source: (5) G20 consensus on DPI, under the India Presidency in 2023 (refer to the Digital Economy Ministerial Declaration for exact language); (6) G20 consensus on DPI, under the India Presidency in 2023 (refer to the Digital Economy Ministerial Declaration for exact language); (7) G20 DEWG India Presidency, 2023

Accelerating the SDGs through Digital Public Infrastructure: A Compendium of the Potential of Digital Public Infrastructure, G20 Summit India, UNDP, 2023

“The technology is often the easy part. It’s the ***humans****, business processes and institutions that are hard.”*

Eraneos, Doing Digital for Impact: Study on Digital Transformation in the Public Sector, Research Paper, Kings College London, 2022

The Trust

Trust

Digital Trust

Importance of Trust in Digital Public Services

What is Trust?

“A psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another.”

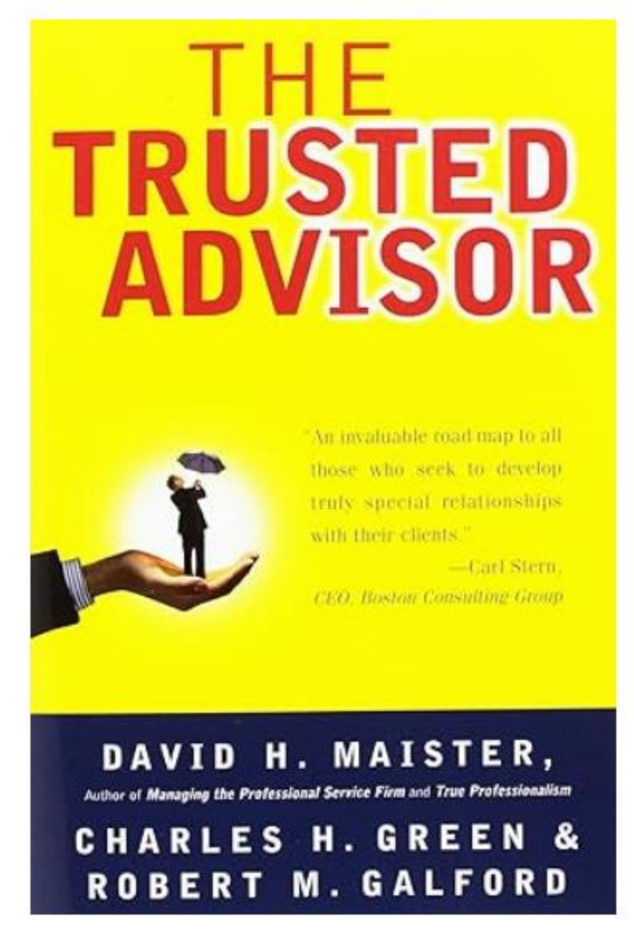
Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. (1998) Not So Different after All: A Cross-Discipline View of Trust. Academy of Management Review, 23, 393-404. http://dx.doi.org/10.5465/AMR.1998.926617

https://www.gslr-antiques.com/en/boutique/tableaux/kermesse-de-village-ecole-flamande-xviiie.php

INSURER 1
INS 2
INSU 3
BANK
INSURER 4
RER
URER

https://www.businesstoday.in/magazine/perspective/story/banks-as-insurance-brokers-will-improve-product-offering-131029-2013-08-26

Quantifying Trust


THE
TRUSTED
ADVISOR
"An invaluable road map to all those who seek to develop truly special relationships with their clients."
—Carl Stern,
CEO, Boston Consulting Group
DAVID H. MAISTER,
Author of Managing the Professional Service Firm and True Professionalism
CHARLES H. GREEN &
ROBERT M. GALFORD

$$T = \frac{C + R + I}{S}$$

T = Trustworthiness

C = Credibility

R = Reliability

I = Intimacy

S = Self-orientation

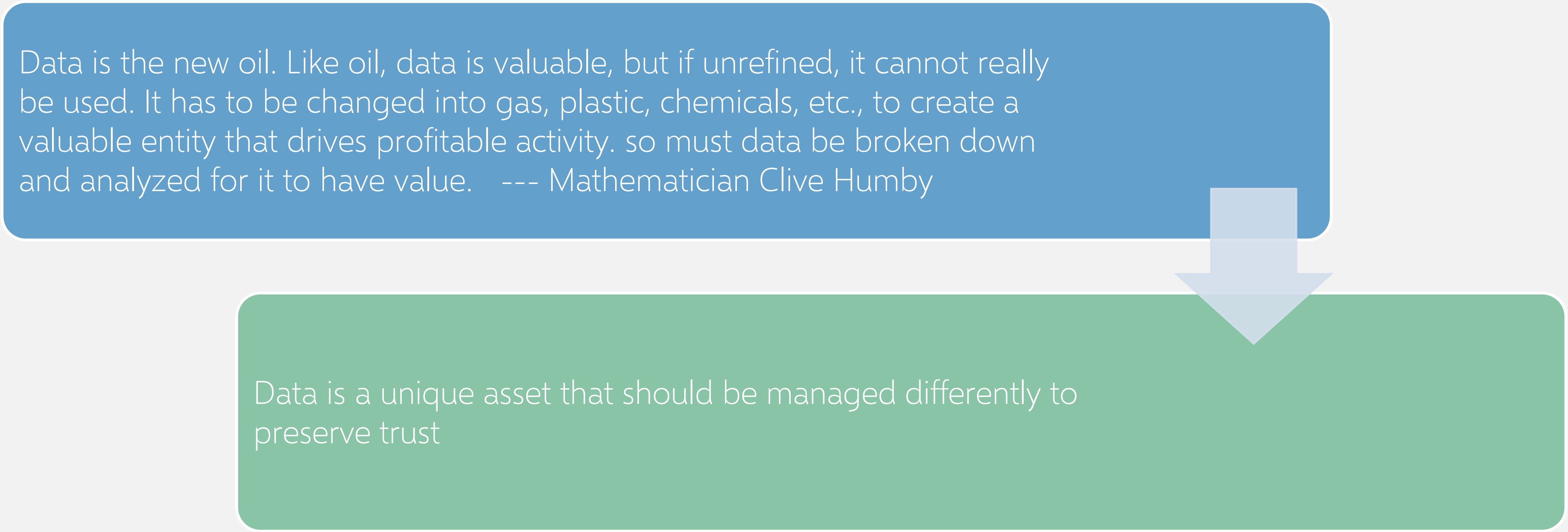
https://www.inc.com/wanda-thibodeaux/people-trust-technology-to-be-honest-study-finds-here-are-big-implications-of-that.html

(Human) Trust vs Digital Trust

Human trust is understanding what a person's motivations are and believing they've got your back.

Digital trust relies on competence as well as intent.

Digital Trust



Data is the new oil. Like oil, data is valuable, but if unrefined, it cannot really be used. It has to be changed into gas, plastic, chemicals, etc., to create a valuable entity that drives profitable activity. so must data be broken down and analyzed for it to have value.   --- Mathematician Clive Humby

Data is a unique asset that should be managed differently to preserve trust

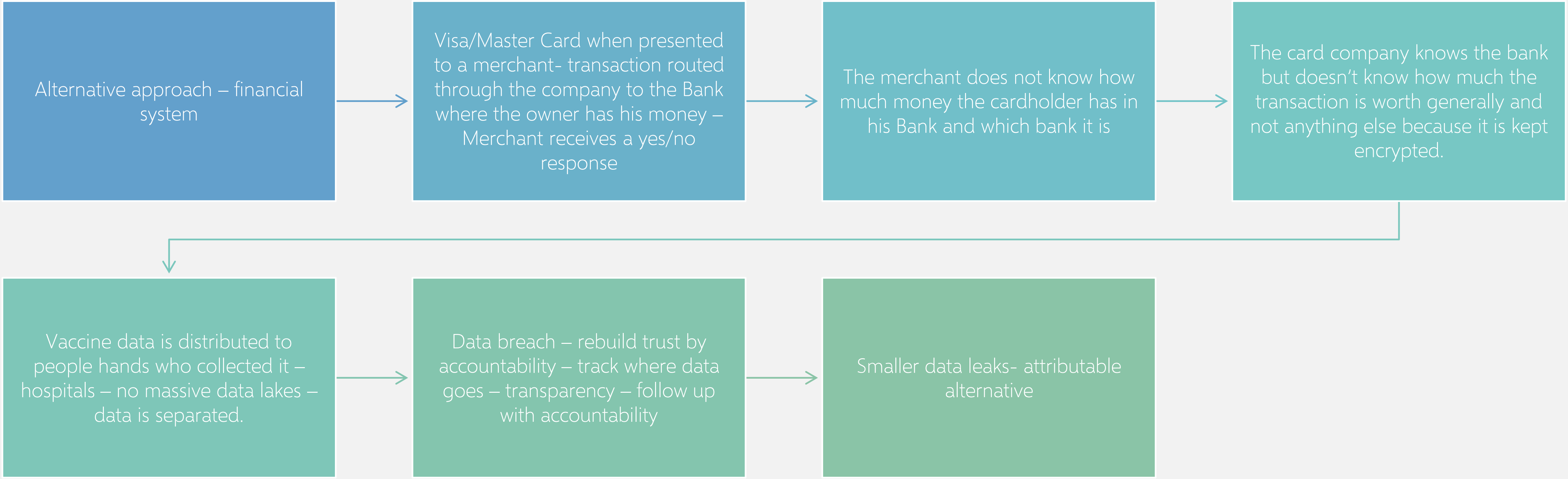
Data Lakes

Data lake – more data is exposed

Data Lakes – Covid 19 - vaccination records

National registries to support vaccine passport – major risk from a centralized data perspective

Alternative System



Alternative approach – financial system

Visa/Master Card when presented to a merchant- transaction routed through the company to the Bank where the owner has his money – Merchant receives a yes/no response

The merchant does not know how much money the cardholder has in his Bank and which bank it is

The card company knows the bank but doesn’t know how much the transaction is worth generally and not anything else because it is kept encrypted.

Vaccine data is distributed to people hands who collected it – hospitals – no massive data lakes – data is separated.

Data breach – rebuild trust by accountability – track where data goes – transparency – follow up with accountability

Smaller data leaks- attributable alternative

FEARS OVER PERSONAL AND NATIONAL DATA SECURITY

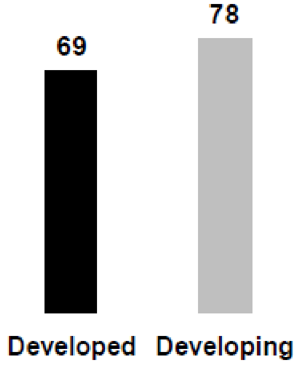
Percent who worry

I worry about **my data privacy** (avg)

My online behavior being tracked without consent
My data used against me
My data used to deny me a job, insurance, or credit

Global 15

73%

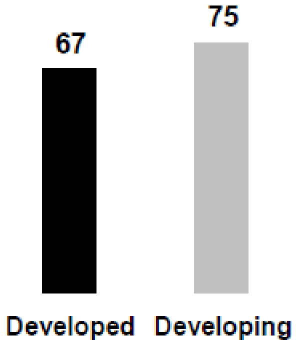


I worry about **cybersecurity** (avg)

Hackers, cyber-attacks, cyber-terrorism
Foreign tech companies compromising our national security
Domestic tech companies providing military products to others

Global 15

71%



Edelman Trust Barometer 2022, Special report: Trust in Technology

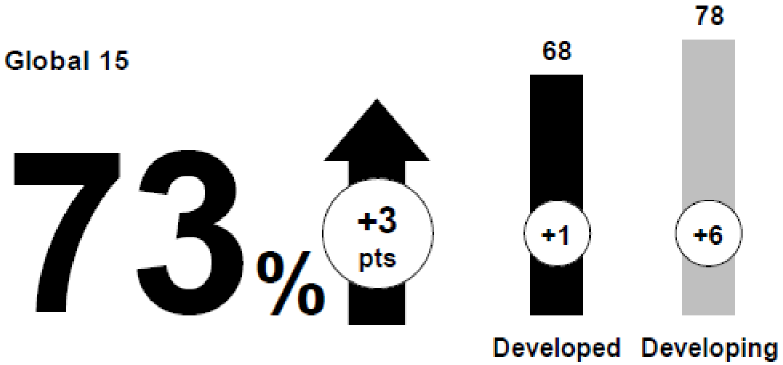
FEARS OF MISINFORMATION AND DEEPFAKES CONTINUE TO RISE OVER LAST 18 MONTHS

Percent who agree

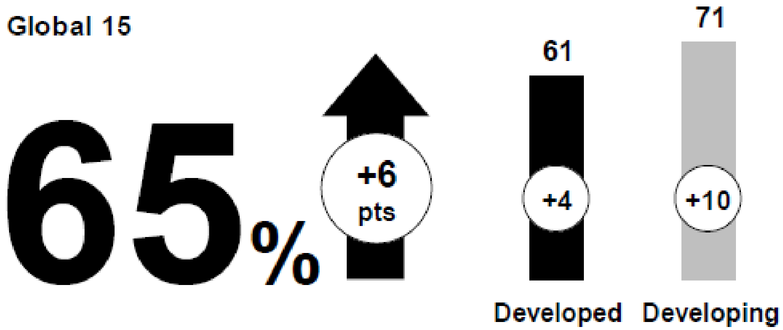
- 0 +

Change, Jan 2021 to Oct 2022

I worry about **false information or fake news being used as a weapon**



I worry **technology will make it impossible to know** if what people are seeing or hearing **is real**

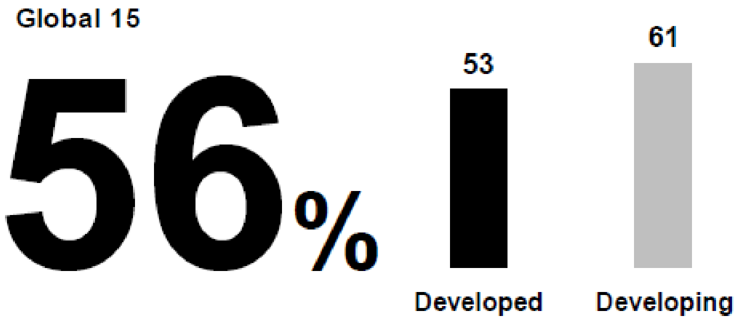


Edelman Trust Barometer 2022, Special report: Trust in Technology

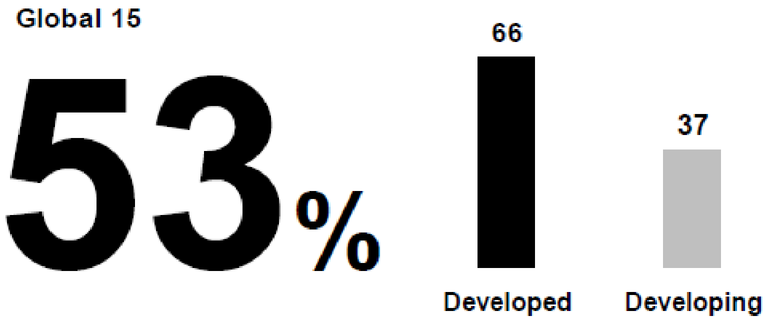
NEITHER GOVERNMENT NOR TECH PLATFORMS TRUSTED AS WATCHDOG

Percent who agree

Government regulators **do not have adequate understanding of emerging technologies** to regulate them effectively



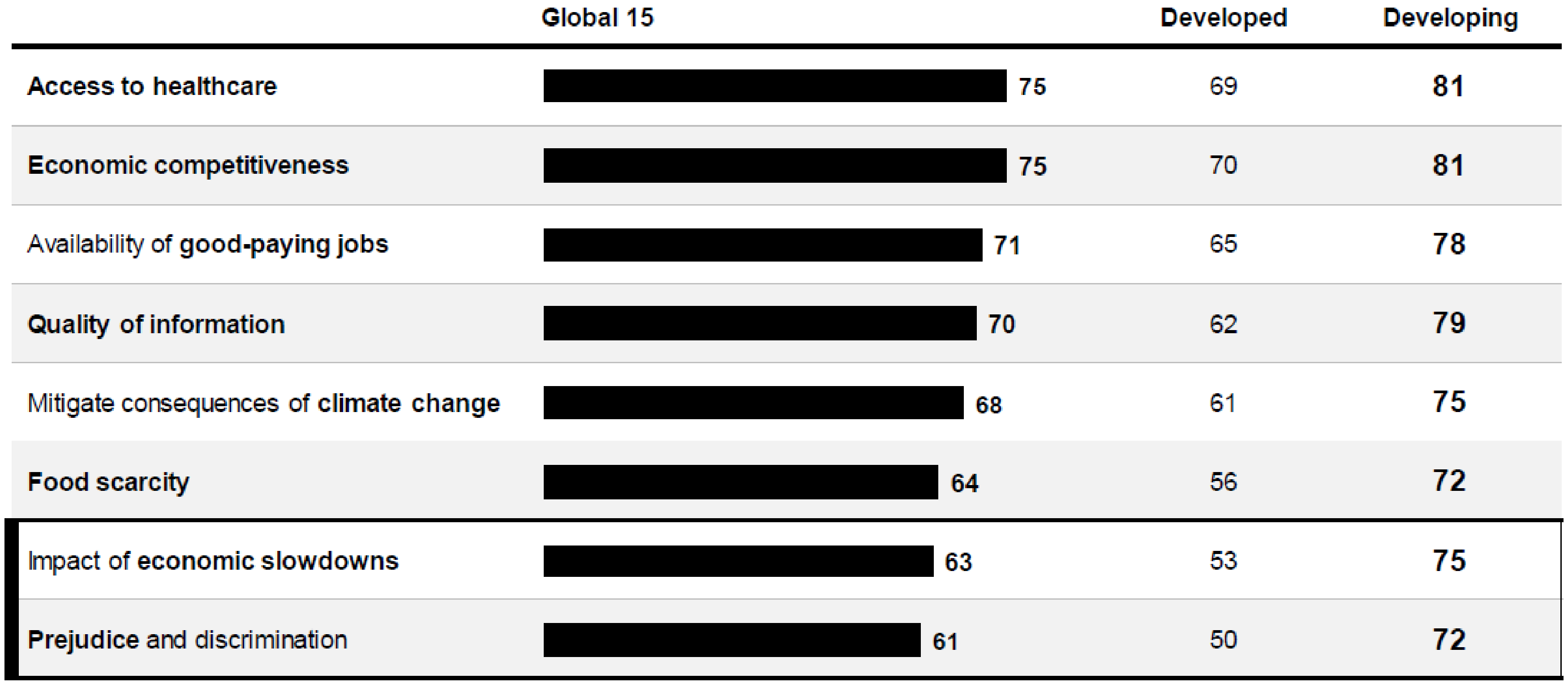
I **do not trust platforms** to **regulate their online content** (avg)



Edelman Trust Barometer 2022, Special report: Trust in Technology

MAJORITY CONVINCED TECHNOLOGY CAN SOLVE URGENT SOCIETAL CHALLENGES

Percent who say technological innovations will have a positive impact on solving each challenge



	Global 15	Developed	Developing
Access to healthcare	75	69	**81**
Economic competitiveness	75	70	**81**
Availability of **good-paying jobs**	71	65	**78**
Quality of information	70	62	**79**
Mitigate consequences of **climate change**	68	61	**75**
Food scarcity	64	56	**72**
Impact of **economic slowdowns**	63	53	**75**
Prejudice and discrimination	61	50	**72**

20+ point gaps between developed and developing countries

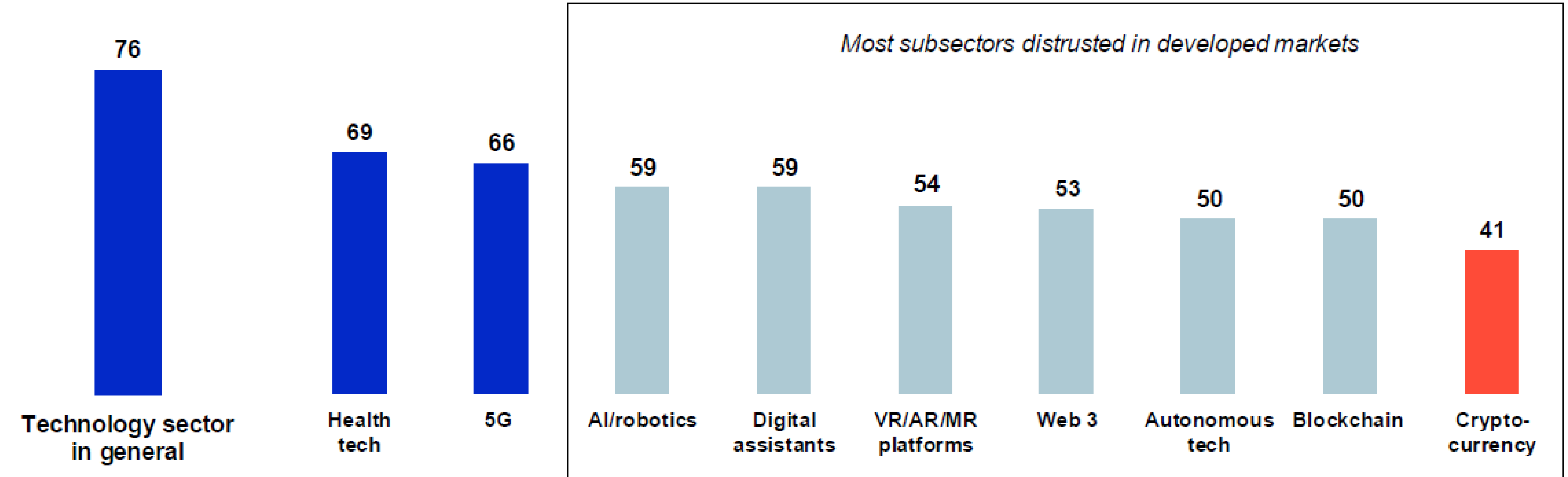
Edelman Trust Barometer 2022, Special report: Trust in Technology

EMERGING TECHNOLOGY SUBSECTORS DO NOT BENEFIT FROM HIGH TRUST IN TECH SECTOR

🟥 Distrust ▨ Neutral 🟦 Trust

Percent trust

Global 15



	Technology sector in general	Health tech	5G	AI/robotics	Digital assistants	VR/AR/MR platforms	Web 3	Autonomous tech	Blockchain	Crypto-currency
Developed	67	60	55	46	45	40	38	37	35	26
Developing	87	79	80	74	75	70	70	65	67	59

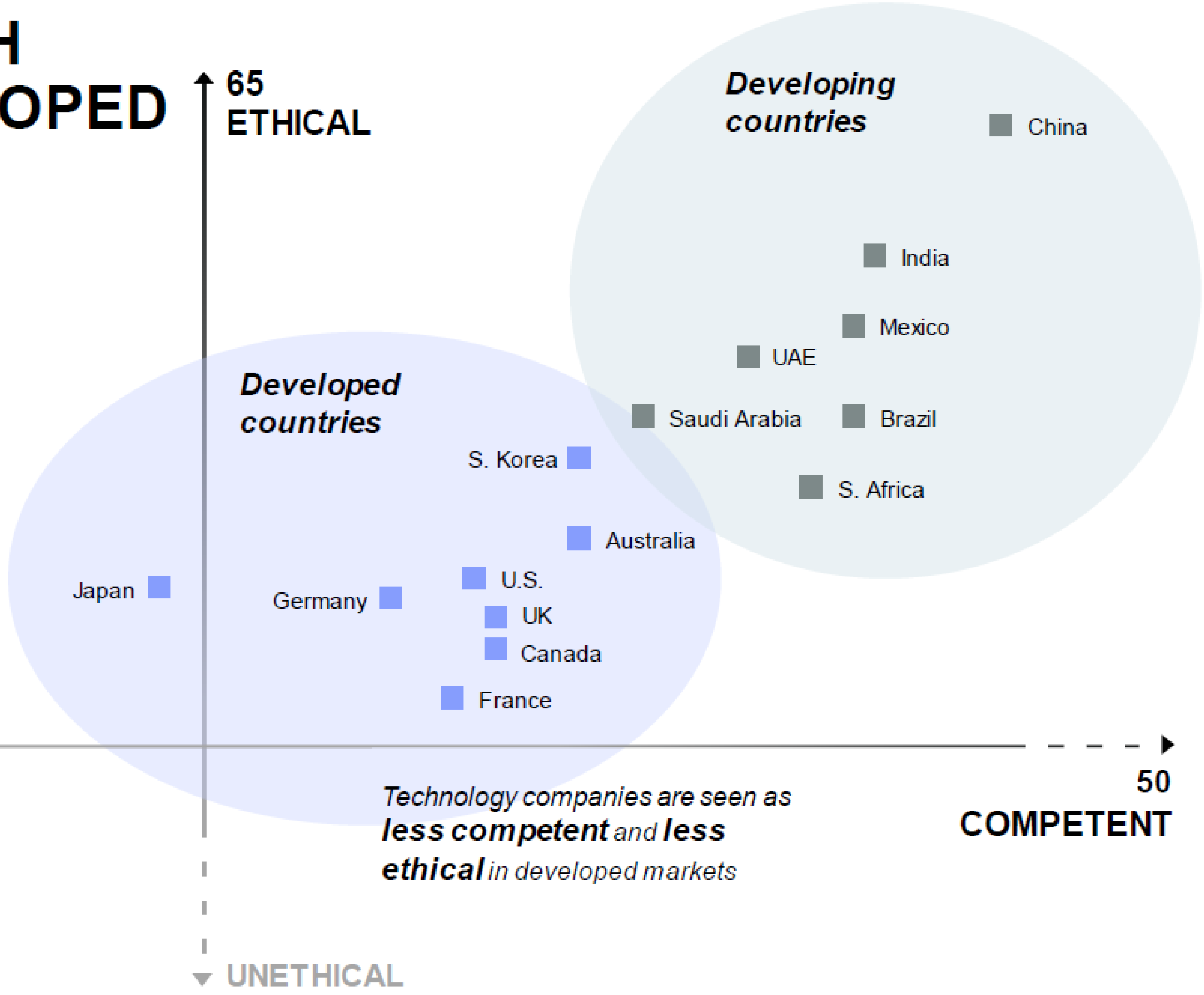
Edelman Trust Barometer 2022, Special report: Trust in Technology

HEADWINDS FOR TECH STRONGEST IN DEVELOPED COUNTRIES

Rating for technology companies by respondents in each market:

(competence score, net ethical score)

Competence and ethics are the two primary dimensions of trust



Technology companies are seen as ***less competent*** *and* ***less ethical*** *in developed markets*

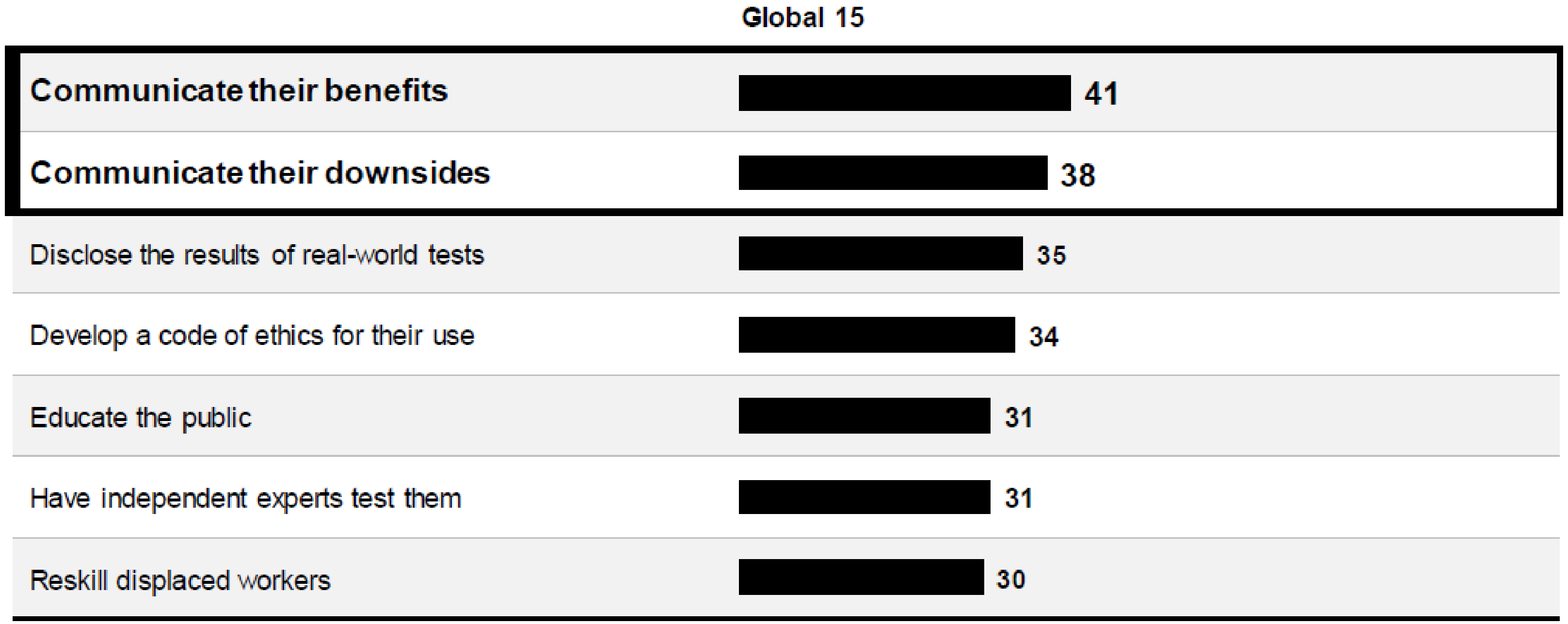
Edelman Trust Barometer 2022, Special report: Trust in Technology

TELL ME THE BENEFITS *AND* THE DOWNSIDES

Percent who say

To **increase my trust in new technologies**,
tech companies must…

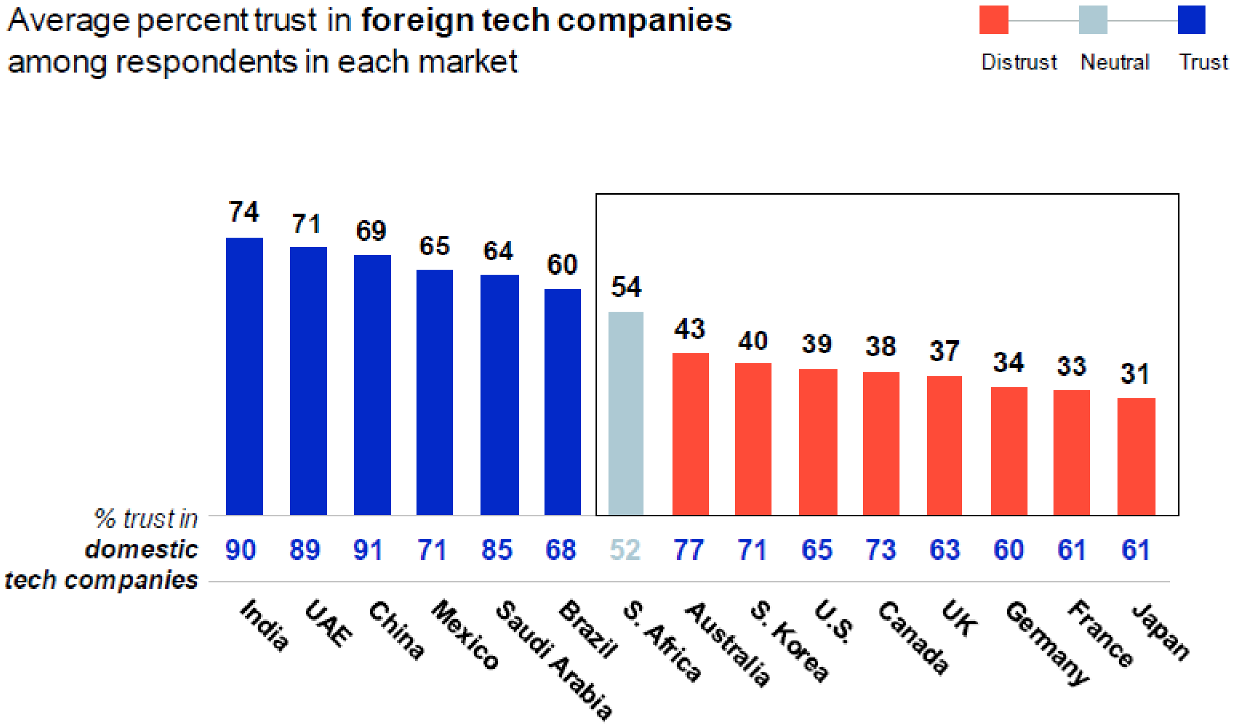
(showing actions with 30% or higher agreement)



Edelman Trust Barometer 2022, Special report: Trust in Technology

CONCERNS OVER FOREIGN GOVERNMENTS LIMIT TRUST IN FOREIGN TECH

Average percent trust in **foreign tech companies** among respondents in each market



PRODUCT CONCERNS NOT AMONG TOP 3 REASONS FOR DISTRUSTING FOREIGN TECH COMPANIES

*Among those who **distrust** tech companies headquartered in foreign countries, top 3 reasons why*

I don't trust **their governments**	**54**
I don't trust **their data protection laws**	**44**
Their governments might **use data against us**	**42**

Edelman Trust Barometer 2022, Special report: Trust in Technology

DATA IN DETAIL

REASONS FOR NOT TRUSTING FOREIGN TECH COMPANIES

Among those who do not trust tech companies from at least one foreign market, reasons why

	Global 15	Australia	Brazil	Canada	China	France	Germany	India	Japan	Mexico	Saudi Arabia	S. Africa	S. Korea	UAE	UK	U.S.
I do not trust the governments of those countries	**54**	65	60	66	40	53	61	43	53	50	39	59	45	38	65	57
I don't trust the data security/protection laws and procedures in those countries	**44**	55	42	56	32	46	50	41	36	42	37	45	33	42	49	45
If our country had a conflict with those countries, I worry that their governments would use the data their technology companies have collected against us	**42**	49	39	50	36	40	38	46	38	35	30	46	40	37	47	44
I believe the technology companies in these countries share user data with the government	**36**	43	40	44	27	34	37	40	29	37	30	41	22	43	39	37
The technology companies in these countries have unfair and exploitative labor practices	**31**	40	31	40	21	38	37	29	22	37	23	34	20	28	36	30
The technology companies in these countries are known to steal product ideas and technologies from other companies	**30**	37	24	36	22	27	30	39	34	29	22	32	26	30	33	29
I don't think the companies in these countries offer good, reliable products and services	**25**	28	27	27	20	25	24	31	23	31	29	30	22	29	18	19
The technology companies in these countries do not have good environmental practices	**24**	26	21	30	20	32	35	26	12	28	23	24	17	23	25	19
The technology produced by companies in these countries isn't leading edge	**16**	16	13	15	21	14	17	27	11	16	21	23	14	24	11	14
None of the above	**8**	8	7	6	8	11	10	4	15	4	9	3	8	4	7	10

Edelman Trust Barometer 2022, Special report: Trust in Technology

LOCALIZE YOUR STRATEGY

Playbooks for engagement, trust building, and societal leadership must vary across geographies

In developed markets…		In developing markets…
Skeptical of impact	*Tech Sentiment*	Enthusiastic about the promise
Updates to familiar favorites	*Product Strategy*	Test new innovations
Family, friends, workplace	*Effective Spokespeople*	Experts
Sustainability, misinformation	*Societal Impact*	Jobs, data security, misinformation
Show societal leadership	*CEO Remit*	**Show societal leadership**

Edelman Trust Barometer 2022, Special report: Trust in Technology

10 YEAR TREND: TRUST IN TECH BY MARKET

Percent trust in the technology sector

🟥 Distrust ▨ Neutral 🟦 Trust

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	Oct 2022
China	88	88	87	84	90	88	91	91	90	77	90	92
India	83	87	91	89	88	92	89	89	92	87	89	92
UAE	81	79	85	84	85	83	81	88	83	80	88	89
Mexico	87	87	86	84	90	87	89	90	85	78	82	87
Brazil	83	80	82	81	83	82	86	87	85	75	80	86
Saudi Arabia	-	-	-	-	-	-	-	81	79	80	83	83
S. Africa	-	-	80	80	78	79	76	79	76	73	75	82
S. Korea	75	72	75	67	69	68	75	76	81	71	74	74
Australia	74	65	73	71	72	71	68	72	66	61	63	71
Canada	77	71	74	73	72	72	71	76	68	60	59	68
Germany	58	60	62	61	63	63	64	68	64	60	61	67
Japan	74	67	68	63	62	63	60	66	68	56	60	65
U.S.	78	70	75	73	73	75	74	73	66	57	54	65
UK	71	71	74	72	69	69	64	69	64	56	61	64
France	74	68	69	65	71	70	67	73	63	57	61	60

Edelman Trust Barometer 2022, Special report: Trust in Technology

WEF Digital Trust

How can leaders make better, more trustworthy decisions regarding technology?

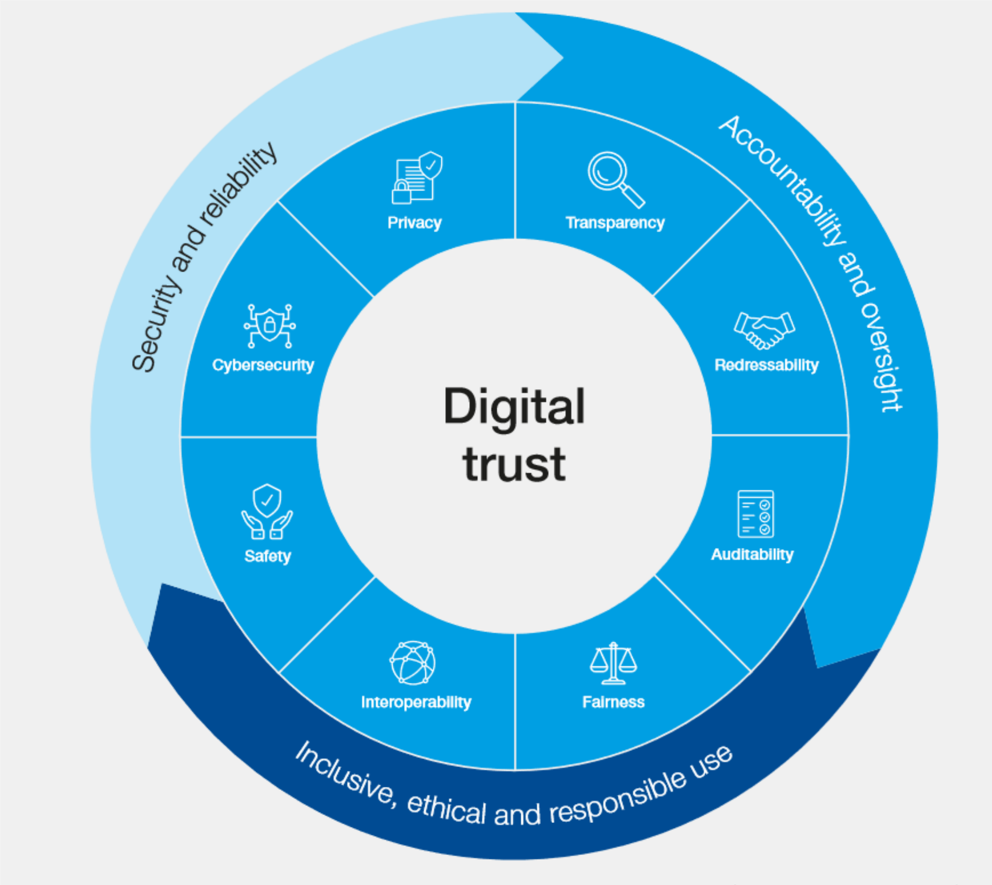
Earning Digital Trust: Decision-Making for Trustworthy Technologies, World Economic Forum, Nov 2022

WEF’s Digital Trust

Digital trust is individuals’ expectation that digital technologies and services – and the Organizations providing them – will protect all stakeholders’ interests and uphold societal expectations and values

Earning Digital Trust: Decision-Making for Trustworthy Technologies, World Economic Forum, Nov 2022

Digital Trust Framework



The framework defines the dimensions against which the trustworthiness of digital technologies can be operationalized and evaluated.

Earning Digital Trust: Decision-Making for Trustworthy Technologies, World Economic Forum, Nov 2022

Emerging Technologies

Evangelos Kalampokis, Nikos Karacapilidis, Dimitris Tsakalidis, and Konstantinos Tarabanis. 2023. Understanding the Use of Emerging Technologies in the Public Sector: A Review of Horizon 2020 Projects. Digit. Gov.: Res. Pract. 4, 1, Article 4 (March 2023), 28 pages. https://doi.org/10.1145/3580603

Shutterstock

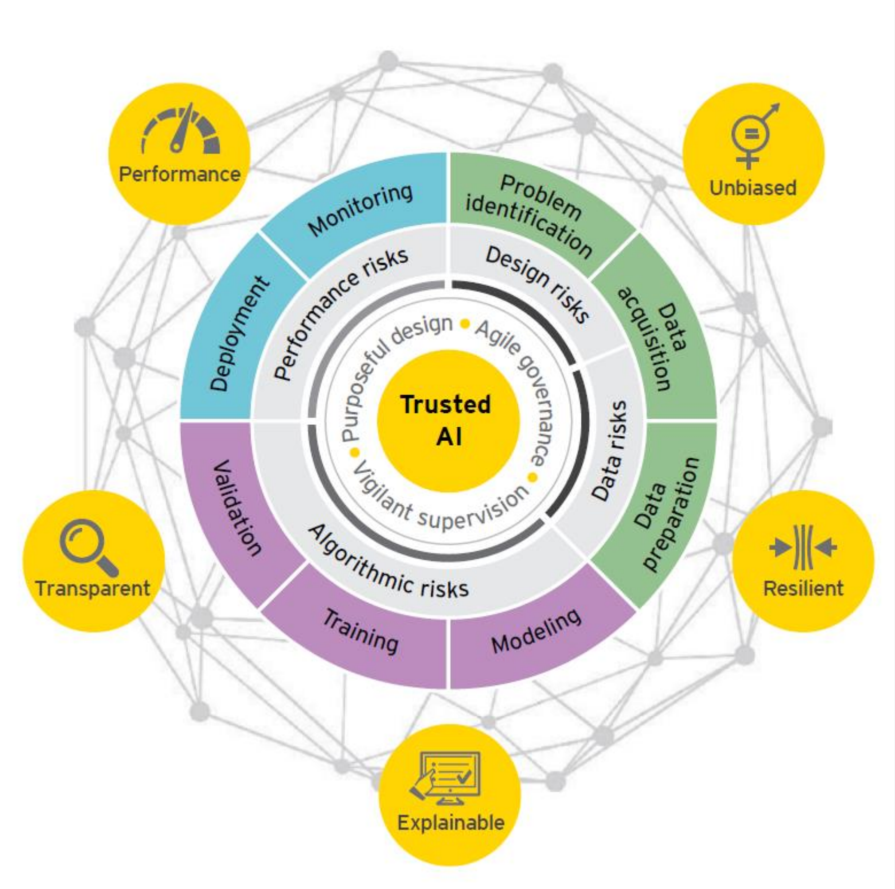
Emerging Technologies - Definition

Emerging technologies is a dynamic concept comprising an evolving list of ICTs that continuously reshape human action and interaction.

From an organization science point of view, emerging technologies do much more than automate and inform, thus posing a series of challenges that distinguish them from prior technologies.

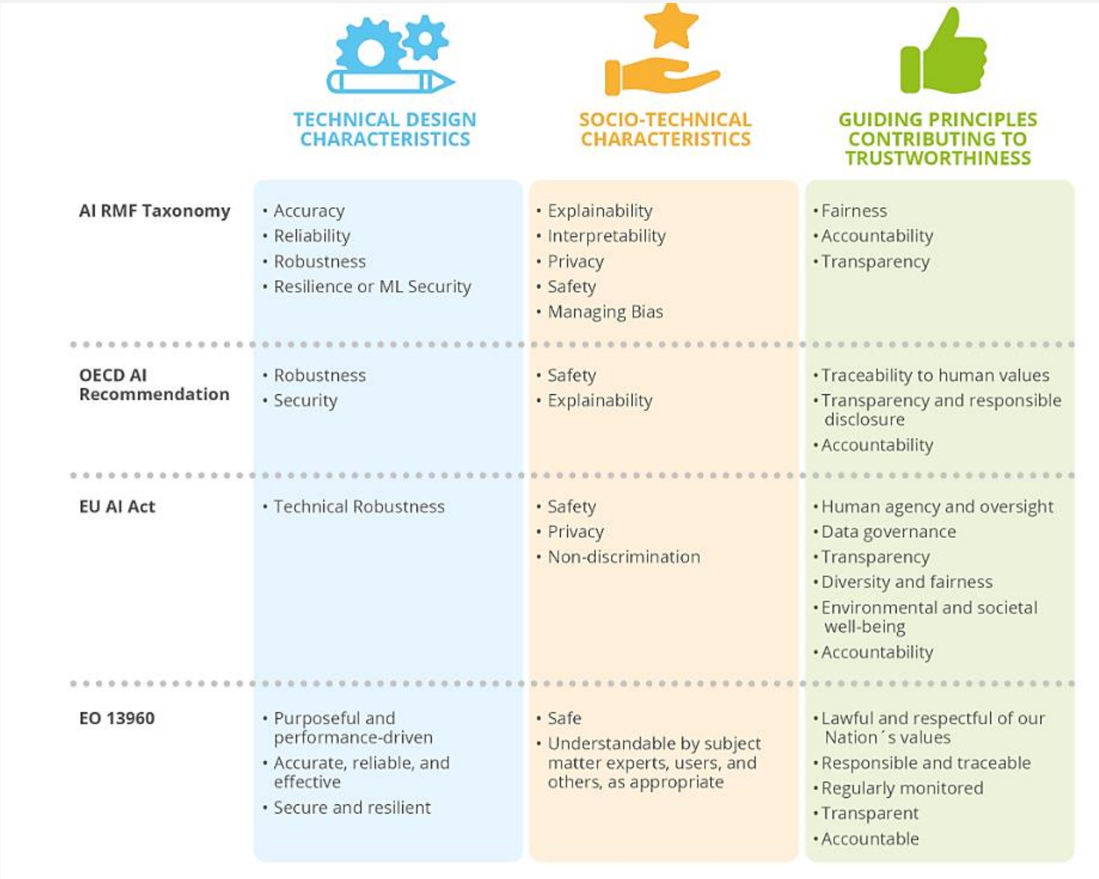
Trust in AI

EY’s trusted AI framework emphasizes five attributes necessary to sustain trust:



How do you teach AI the value of trust?, Ernst & Young (EY)

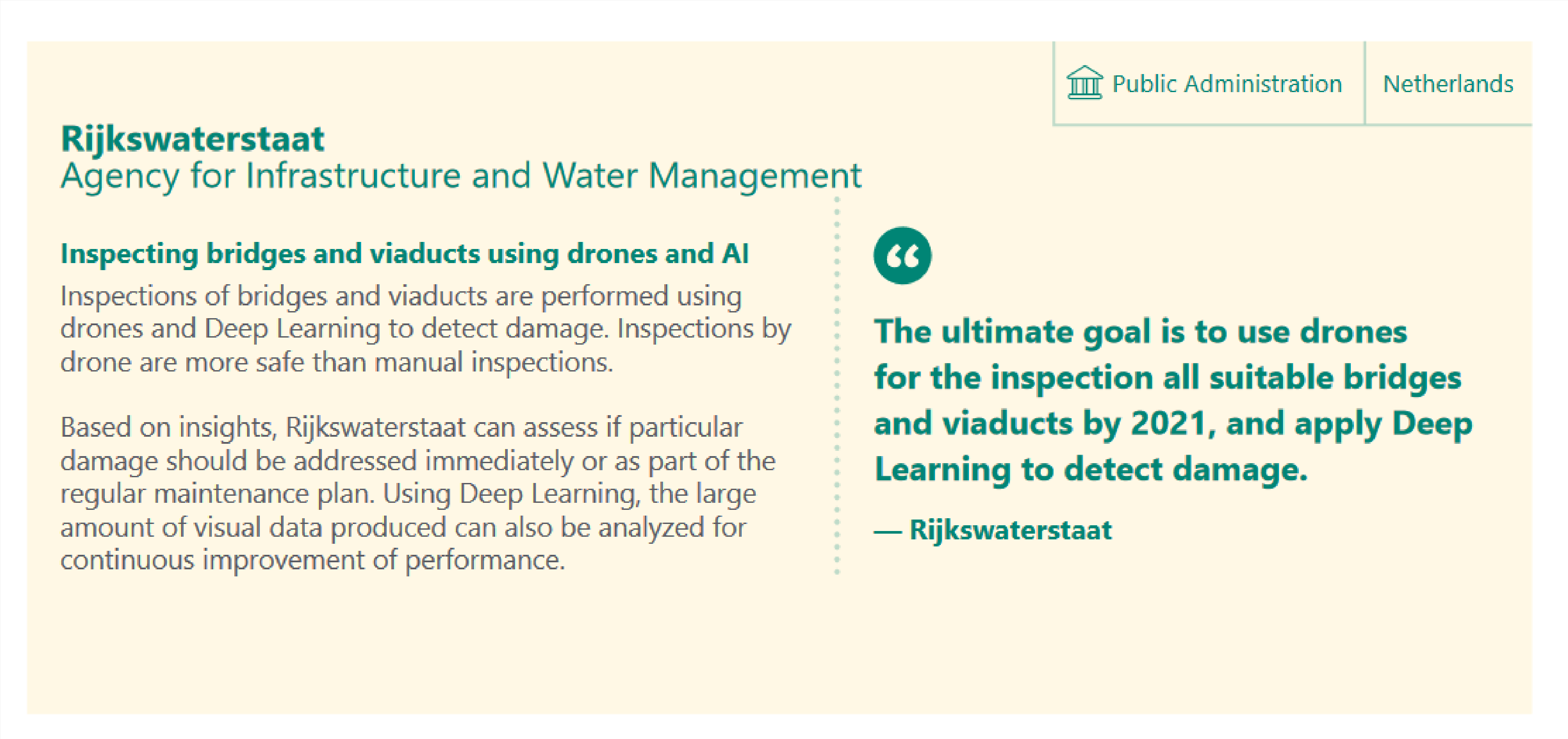
Achieving AI Trustworthiness



	TECHNICAL DESIGN CHARACTERISTICS	SOCIO-TECHNICAL CHARACTERISTICS	GUIDING PRINCIPLES CONTRIBUTING TO TRUSTWORTHINESS
AI RMF Taxonomy	• Accuracy • Reliability • Robustness • Resilience or ML Security	• Explainability • Interpretability • Privacy • Safety • Managing Bias	• Fairness • Accountability • Transparency
OECD AI Recommendation	• Robustness • Security	• Safety • Explainability	• Traceability to human values • Transparency and responsible disclosure • Accountability
EU AI Act	• Technical Robustness	• Safety • Privacy • Non-discrimination	• Human agency and oversight • Data governance • Transparency • Diversity and fairness • Environmental and societal well-being • Accountability
EO 13960	• Purposeful and performance-driven • Accurate, reliable, and effective • Secure and resilient	• Safe • Understandable by subject matter experts, users, and others, as appropriate	• Lawful and respectful of our Nation´s values • Responsible and traceable • Regularly monitored • Transparent • Accountable

A multilayer framework for good cybersecurity practices for AI, The European Union Agency for Cybersecurity, ENISA, Jun 2023

Trust through AI



Public Administration | Netherlands

Rijkswaterstaat

Agency for Infrastructure and Water Management

Inspecting bridges and viaducts using drones and AI

Inspections of bridges and viaducts are performed using drones and Deep Learning to detect damage. Inspections by drone are more safe than manual inspections.

Based on insights, Rijkswaterstaat can assess if particular damage should be addressed immediately or as part of the regular maintenance plan. Using Deep Learning, the large amount of visual data produced can also be analyzed for continuous improvement of performance.

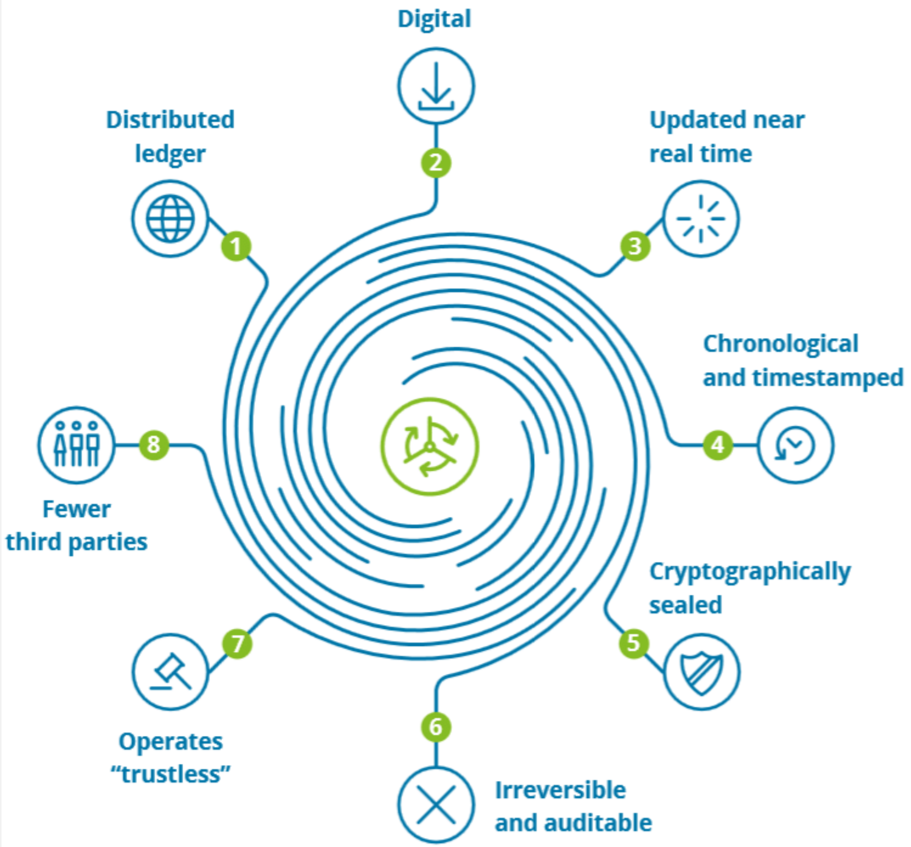
> **The ultimate goal is to use drones for the inspection all suitable bridges and viaducts by 2021, and apply Deep Learning to detect damage.**
>
> **— Rijkswaterstaat**

Artificial Intelligence in the Public Sector, European Outlook for 2020 and Beyond, EY

Blockchain

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those over-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world

Features of Blockchain

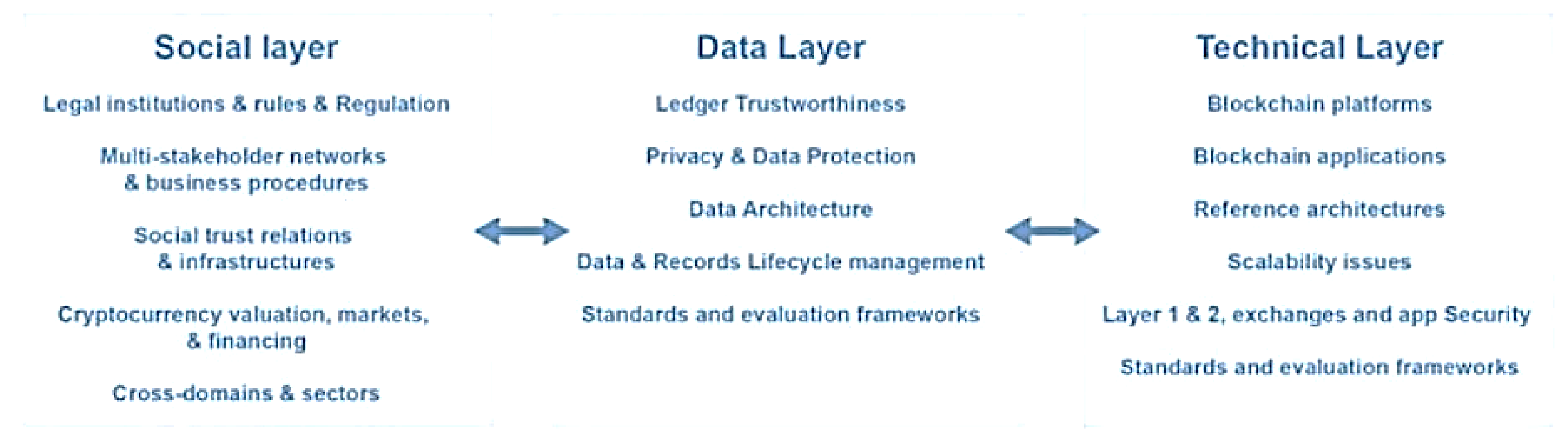


https://www.researchgate.net/figure/Blockchain-Key-Features-24_fig3_333511632

Trust in Blockchain

- Inaccurate or Malicious Data
- Governance Issues
- Smart Contracts
- Security
- Legal Aspects

Trust Through BC



Social layer

Legal institutions & rules & Regulation

Multi-stakeholder networks & business procedures

Social trust relations & infrastructures

Cryptocurrency valuation, markets, & financing

Cross-domains & sectors

Data Layer

Ledger Trustworthiness

Privacy & Data Protection

Data Architecture

Data & Records Lifecycle management

Standards and evaluation frameworks

Technical Layer

Blockchain platforms

Blockchain applications

Reference architectures

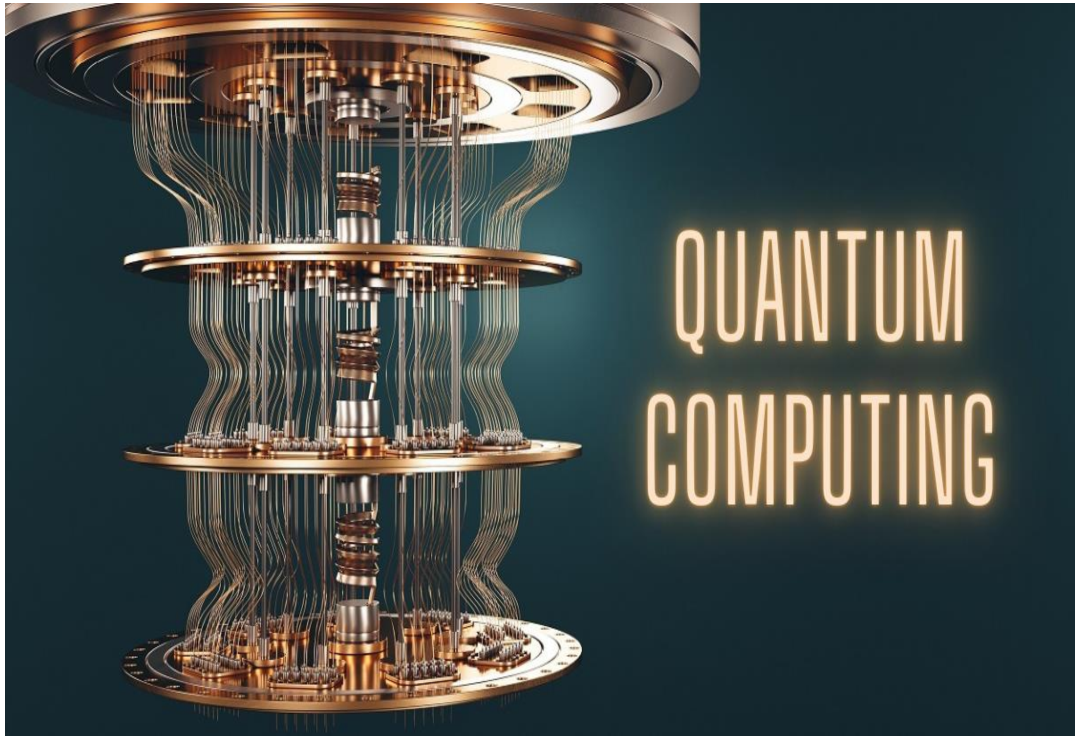
Scalability issues

Layer 1 & 2, exchanges and app Security

Standards and evaluation frameworks

https://blogs.worldbank.org/governance/blockchain-technology-has-potential-transform-government-first-we-need-build-trust

State of Quantum Computing: Building a Quantum Economy, Insight Report, WEF, Sep 2022



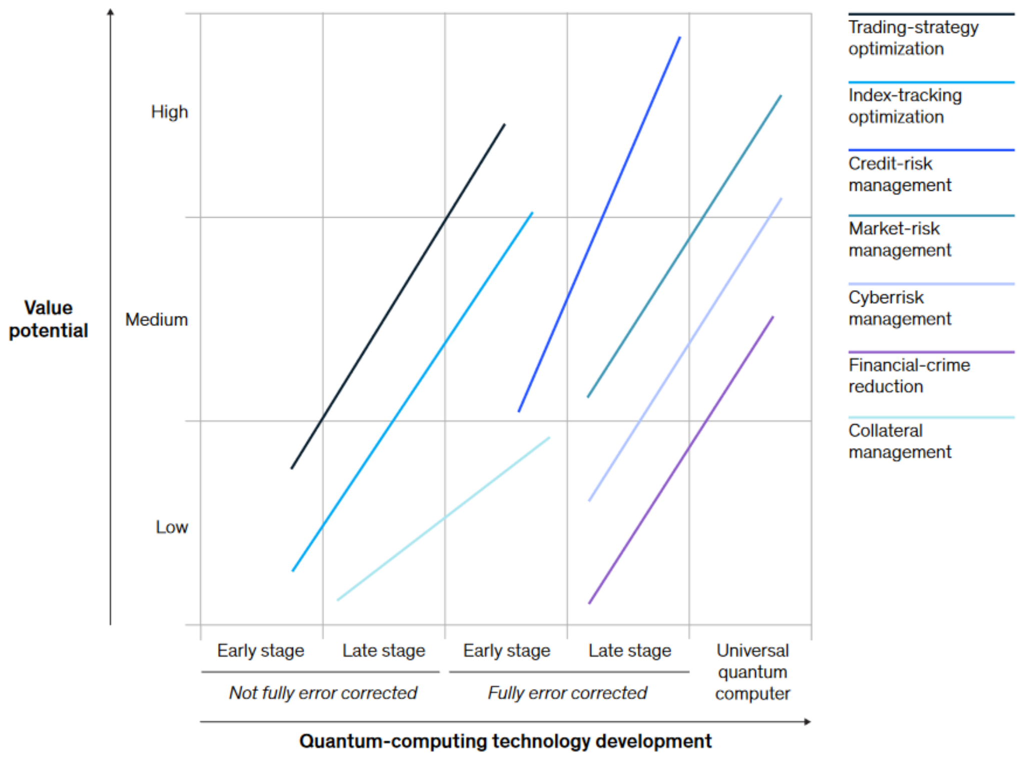
https://gmo-research.com/news-events/articles/future-quantum-computing

Trust in QC

- Molecular simulation and discovery in materials science and biology
- Optimization and risk management in complex systems
- A bi-directional impact on existing technology areas such as AI, security and blockchain.

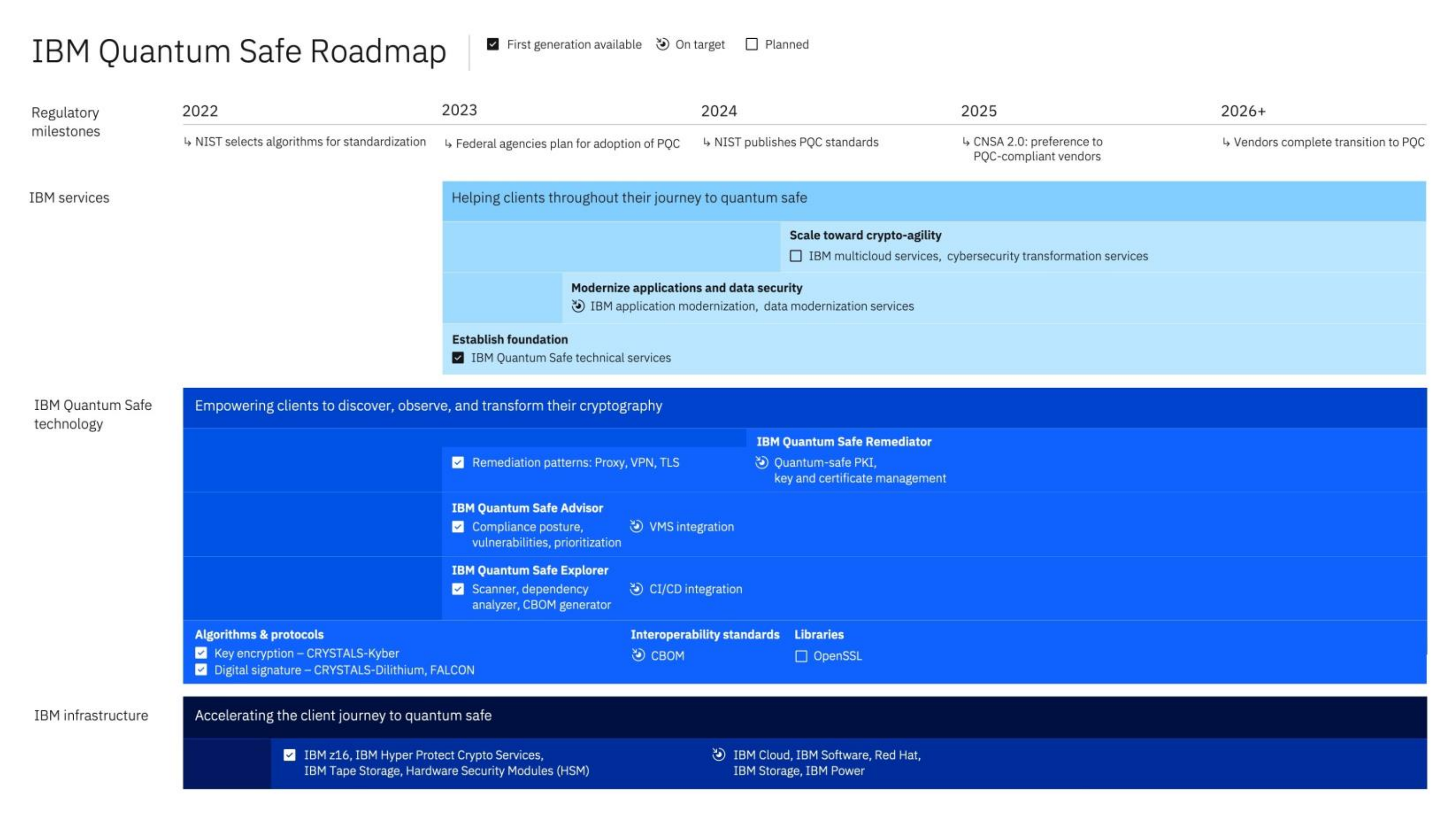
QC Use Cases in Finance

Finance has many computationally intense tasks that could benefit from quantum computing.



McKinsey & company, Quantum computing an emerging ecosystem and industry use cases, Dec 2021

Trust Through QC



IBM Quantum Safe Roadmap

☑ First generation available ↻ On target □ Planned

Regulatory milestones

- 2022 ↳ NIST selects algorithms for standardization
- 2023 ↳ Federal agencies plan for adoption of PQC
- 2024 ↳ NIST publishes PQC standards
- 2025 ↳ CNSA 2.0: preference to PQC-compliant vendors
- 2026+ ↳ Vendors complete transition to PQC

IBM services

Helping clients throughout their journey to quantum safe

Scale toward crypto-agility
□ IBM multicloud services, cybersecurity transformation services

Modernize applications and data security
↻ IBM application modernization, data modernization services

Establish foundation
☑ IBM Quantum Safe technical services

IBM Quantum Safe technology

Empowering clients to discover, observe, and transform their cryptography

☑ Remediation patterns: Proxy, VPN, TLS

IBM Quantum Safe Remediator
↻ Quantum-safe PKI, key and certificate management

IBM Quantum Safe Advisor
☑ Compliance posture, vulnerabilities, prioritization
↻ VMS integration

IBM Quantum Safe Explorer
☑ Scanner, dependency analyzer, CBOM generator
↻ CI/CD integration

Algorithms & protocols
☑ Key encryption – CRYSTALS-Kyber
☑ Digital signature – CRYSTALS-Dilithium, FALCON

Interoperability standards
↻ CBOM

Libraries
□ OpenSSL

IBM infrastructure

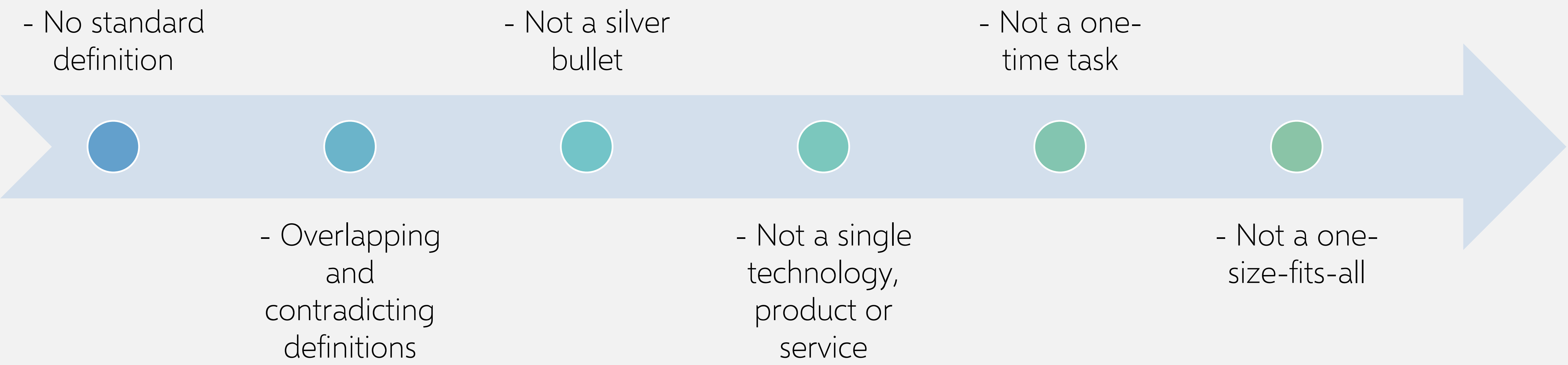
Accelerating the client journey to quantum safe

☑ IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)

↻ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power

https://www.ibm.com/quantum/quantum-safe

Public Services – Critical Infra: Zero Trust



- No standard definition

- Overlapping and contradicting definitions

- Not a silver bullet

- Not a single technology, product or service

- Not a one-time task

- Not a one-size-fits-all

The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment, Community Paper, World Economic Forum, Aug 2022

Zero Trust

- Philosophy or mindset to build a defensible security model encompassing a variety of different safety measures, capabilities, best practices and technological bricks.

- Shift in the security approach on how to dynamically and holistically establish trust with “an unknown”, whether a human or a machine.

- Principle-based and data-centric model that enforces continuous verification and visibility of trust based on risk.

The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment, Community Paper, World Economic Forum, Aug 2022

Zero Trust - Benefits

- More successful in stopping or limiting security events in contrast to the very structured but increasingly ineffective perimeter-based security models

- A more structured and risk-based approach

- Better protection of data and infrastructure

- Improved compliance with regulations and standards

Zero Trust - Challenges

- Requires detailed inventory of applications, data assets, devices, networks, access rights, users and other resources

- Inevitably necessitates a change of mindset and needs support from all the stakeholders

- Requires financial and non-financial resources

Workshop on Building Trust in Digital Government Services, Beirut, 11-12 September 2023

Dr. Pankaj Pandey
Research Scientist
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway
Email: pankaj.pandey@ntnu.no