Bell Labs Consulting

NOKIA BELL LABS

Sovereign data center strategy

Outline of global practices in sovereign data center strategies and strategic recommendations

White paper

BUSINESS FINLAND

Abstract

Digital infrastructure has become as essential to national growth as transportation, power and water networks. Data centers are now critical national assets that enable governments to deliver secure citizen services, safeguard sensitive information, and foster digital economic growth. While many countries are rapidly progressing in their digital transformation journey, highlighting the critical role of data sovereignty and secure digital infrastructure is essential.

This whitepaper outlines global practices in sovereign data center strategies, particularly drawing lessons from Finland and around the world, and provides strategic recommendations.

Contents

Digitalization journey: Example from Finland

Finnish governmental digitalization is the result of a forward-looking regulatory framework and digital transformation journey that began in the 1990s. The transformation continues as novel technology enables the country to tackle existing and rapidly evolving challenges. The state of digitalization of Finnish governmental data management and services can be attributed to significant investments in infrastructure and e-government platforms in close collaboration between government, academia and business. This background gives a unique opportunity to share the experiences of the journey and help other nations to reach a more digitalized society.

Finland has a National Strategic Roadmap [1] aimed at advancing digitalization, aligned with the European Union's Digital Decade Program [2] towards 2030. Notably, Finland has either achieved or is nearing the fulfillment of numerous Digital Decade objectives ahead of the 2030 deadline.

The digitalization strategy includes the following key elements.

Skills

A focus on digital education has resulted in a highly digitally skilled population, supporting the broader digital economy. As of 2022, 79% of the Finnish population possessed at least basic digital skills, nearing the EU's 2030 target of 80% and surpassing the EU average of 54%.

Secure and sustainable digital infrastructure

Developing robust and environmentally sustainable digital infrastructure is a key priority. Investments are being made via public-private networks, fiber expansion and IPv6 adoption, while cybersecurity, green data centers and resilience measures are built into the infrastructure strategy. Finland's data center strategy is based on harnessing natural climate grid advantages for energy-efficient operations, pre-approved development zones, and public-private partnerships. Over 600 MW of capacity is currently under development across Finland, signaling strong investor interest. Finland promotes a hybrid sovereign model where government owns and operates "core" data centers for critical workloads where 100% of critical public sector data is stored domestically, while partnering with the private sector for non-classified workloads.

Digital transformation of businesses

As a result of promoting digital innovation and adoption in the business sector, nearly 82% of Finnish SMEs report basic digital adoption. Government-backed programs—such as AI adoption grants, the Industrial Internet initiative, and the "Lead Company" model—have helped scale digital innovation, particularly among smaller firms.

Digitalization of public services

Providing universal, seamless, secure digital access to public services for citizens and businesses has been a key priority. Finland leads in digital public services, with 92% of internet users engaging with e-government services, compared to the EU average of 65%. Finland focuses on the secure and reliable interoperability of government data as well as single sign-on and easy to use services for citizens and organizations.

> The Finnish model demonstrates how to enable a resilient digital infrastructure that supports strong economic and societal growth. They combine public policy with in-country ownership for critical systems with frameworks that allow public-private collaboration, innovation and scale, strategic investments, and a clear roadmap.

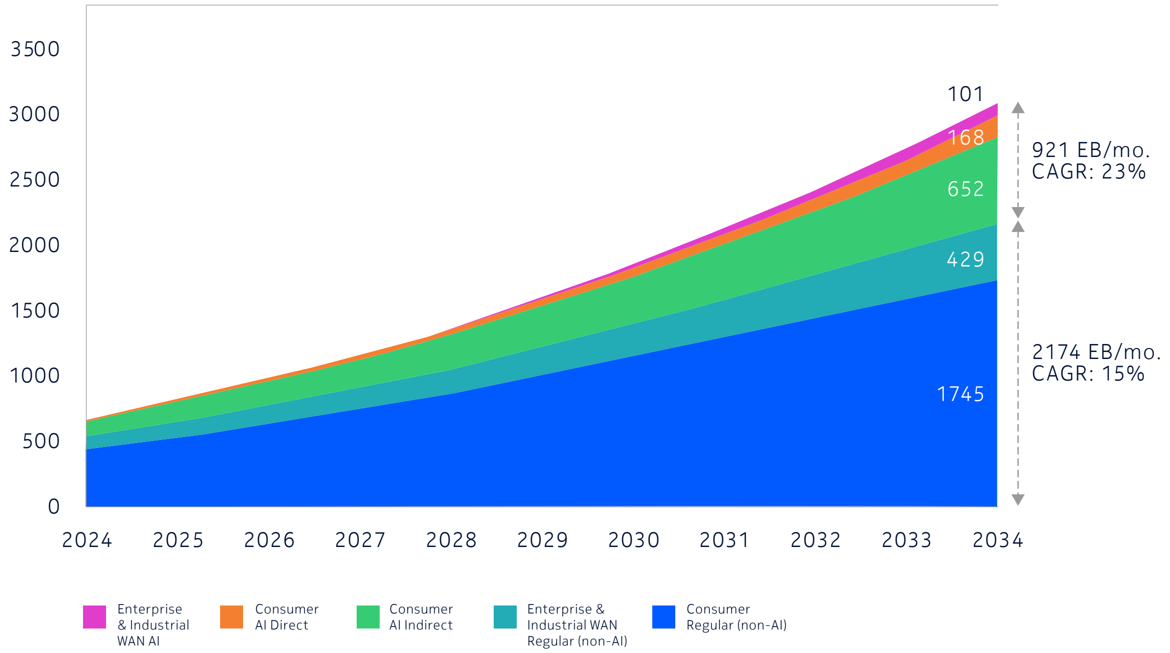
Key drivers for data center growth and impact

Rapid growth in data center demand is driven by several critical factors.

Artificial intelligence supercycle

The surge in AI workloads is fueling exponential growth in data center compute and interconnect demands. The urgency for this is highlighted by the dramatic increase in global network traffic. According to the Nokia Global Network Traffic Report (2025) [3], traffic is projected to reach 3,096 EB/month by 2033, growing at a 16% compound annual growth rate (CAGR). This surge is heavily driven by AI, with AI traffic alone expected to account for a massive 23% of global traffic at that time.

Figure 1. Global traffic projection, EB/month



By 2034, mobile traffic growth will diverge, influenced by AI and extended reality (XR) services. Mature markets will see moderate growth (CAGR): Western Europe with 11%, North America with 13%, and some segments at 15%. Growth will moderate as engagement slows and traffic shifts to higher resolutions and XR. Emerging markets, however, are projected for higher growth (CAGR), including Latin America at 20%, China, 10%, India, 18%, and APAC, 16%. This uptick will be fueled by digital inclusion, 5G and widespread AI-based content and HD video adoption. China's enterprise AI growth will be propelled by manufacturing automation, surveillance, retail analytics and immersive media. North America's momentum will come from mature industries and advanced cloud infrastructure.

Data sovereignty and localization

With increasing cyber threats and geopolitical tensions, countries are prioritizing control over their digital assets. Sovereign data centers allow governments to implement their own security protocols, avoid reliance on foreign jurisdictions and ensure sensitive information remains under national control. 17% of APAC government agencies already use sovereign cloud solutions, and nearly one-third plan to adopt them in next two years [4].

Cloud migration and digital economy expansion

Enterprises are rapidly shifting to the cloud for scalability and efficiency, with over 70% of workloads expected to run in cloud environments by 2028 [5]. Data centers fuel this growth by enabling SMEs to access affordable, low-latency cloud services locally, eliminating the need for overseas hosting. This boosts competitiveness, reduces operational costs and fosters innovation.

Transformation of citizen services

Governments worldwide are moving toward digital-first public services, hosting everything from online healthcare systems and e-government portals to national ID platforms in secure, reliable facilities. This ensures high uptime, minimal disruption and operational continuity during crises.

Global approaches to sovereign data centers

Many nations are adopting a hybrid data center strategy to balance challenges, opportunities and risks. These relate to security and control over their most sensitive data, high implementation costs, risk of vendor lock-in, complexity of integration with legacy systems, and to avoid slowing down innovation due to over-restriction. There are four key approaches adopted by governments.

Table 1. Global approaches and models to sovereign data centers [5]

Model	Description	Pros	Cons	Examples*
Full-state owned and operated with sovereignty-first approach	Maximizes data control and national security, with full ownership and operation for highly sensitive workloads where security and privacy are the primary pillar	Maximum data control and security Directly aligned to government strategic priorities	High operational costs Requires upskilling and in-house expertise	Saudi Arabia UAE Norway
Public-private partnerships that are sovereignty- aligned	Give priority to data sovereignty and control while leveraging the efficiency and financing of private sector e.g., France requires EU ownership, jurisdiction immunity, and local ops	Shared costs Leverage private expertise Faster time-to-market	Highly complex and heavy governance to ensure controls are strong Complex contract management	France [6] Singapore [7] Malaysia [8] Germany South Korea
Federated sovereign cloud	Balance sovereignty with openness, innovation and competition through common standards and regulation	Supports local champions Encourages innovation	Slower consensus building Complex governance	Switzerland Italy Spain
Innovation-first, regulated hyperscale model	Priority towards rapid deployment and relies on market-driven demand and innovation with some regulatory safeguards. Skeptical of sovereignty-heavy regulation.	Speed and scale Lower operating expenses, open to non-EU providers	Dependency on foreign entities Exposure to foreign jurisdiction laws Limited influence	Ireland Denmark

*Indicative and not definitively stated by government sources.

Singapore has taken a clear split approach, hosting sensitive government workloads in sovereign facilities while partnering with AI and data center providers for commercial AI services. This balance safeguards national security while fueling AI-driven economic activity, strengthening its position as a regional digital hub. South Korea has followed a similar path, blending sovereign data center builds with metro-edge public-private deployments to power emerging technologies and create high-value innovation clusters in key cities.

India has leveraged public-private partnerships and investment-friendly policies to attract major AI and data center providers, enabling rapid infrastructure expansion while maintaining strong regulatory oversight of local data. This influx of foreign capital and advanced cloud capabilities has significantly boosted the digital sector's share of GDP and created skilled jobs while stimulating ancillary industries from fiber networks to software services. In a similar way, the **UAE** has invested heavily in national facilities for government and defense workloads, while partnering with global cloud providers to expand AI, high-performance computing and commercial hosting driving economic diversification beyond oil.

In **Finland**, sovereign data centers are powered by renewable energy, reflecting its commitment to sustainability, while collaborations with international partners enable hosting of global AI research workloads. This dual focus on green technology and global tech integration enhances Finland's competitive edge in both environmental and digital economies. Across all these cases, a hybrid approach where sovereign builds for control, foreign investment for scale, and technology collaboration for capability has proven a catalyst for GDP growth, enabling the government to protect strategic interests while accelerating digital innovation.

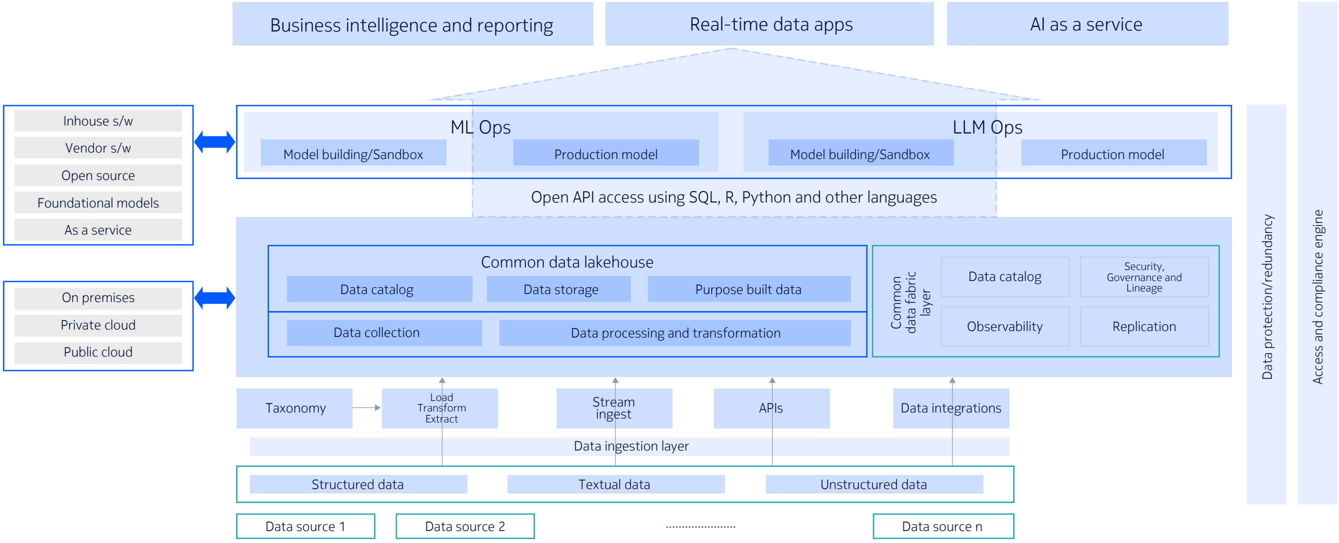
Bell Labs architecture framework: Key considerations for government DC deployment

With the rapid evolution of technology and AI, it is important to design and build the sovereign cloud with agility, security, scalability and future-proof digital infrastructure that optimizes operations, enforces compliance and accelerates digital transformation.

Distributed data architecture

The framework leverages data mesh principles, data lakehouse design and data fabric overlays to create a decentralized yet unified data environment. This enables seamless data flow across ministries and agencies, supporting real-time analytics, reducing silos and improving operational agility.

Figure 2. Distributed data architecture

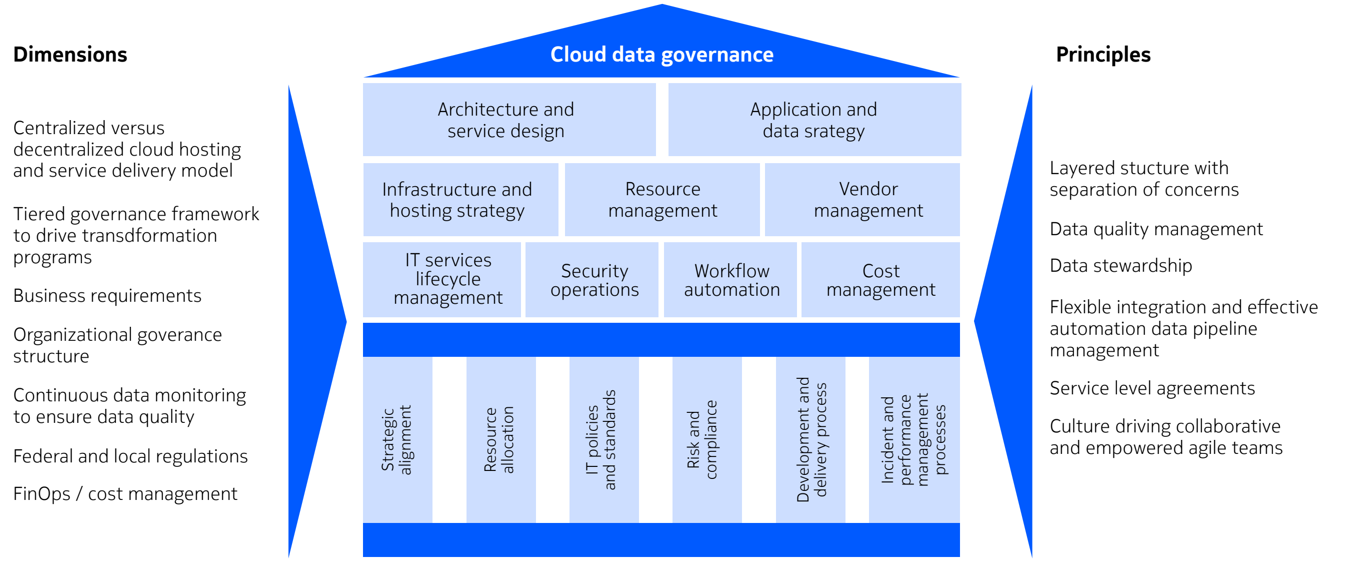


Globally, governments using distributed architectures overcome latency, integration and ownership challenges inherent in centralized systems.

Cloud data governance framework

A structured governance framework ensures data quality, consistency, integrity and compliance across all repositories. It provides clear policies for data access, sharing and regulatory adherence while supporting centralized oversight without centralizing ownership.

Figure 3. Cloud data governance framework


Dimensions
Centralized versus decentralized cloud hosting and service delivery model
Tiered governance framework to drive transdformation programs
Business requirements
Organizational goverance structure
Continuous data monitoring to ensure data quality
Federal and local regulations
FinOps / cost management
Cloud data governance
Architecture and service design
Application and data strategy
Infrastructure and hosting strategy
Resource management
Vendor management
IT services lifecycle management
Security operations
Workflow automation
Cost management
Strategic alignment
Resource allocation
IT policies and standards
Risk and compliance
Development and delivery process
Incident and performance management processes
Principles
Layered structure with separation of concerns
Data quality management
Data stewardship
Flexible integration and effective automation data pipeline management
Service level agreements
Culture driving collaborative and empowered agile teams

The cloud data governance framework addresses common challenges like poor data quality and regulatory gaps.

Cybersecurity and compliance

The architecture embeds security-by-design, defense-in-depth and zero-trust principles to protect critical data and digital services. Risk assessments and compliance mapping help prioritize protections and align with international standards.

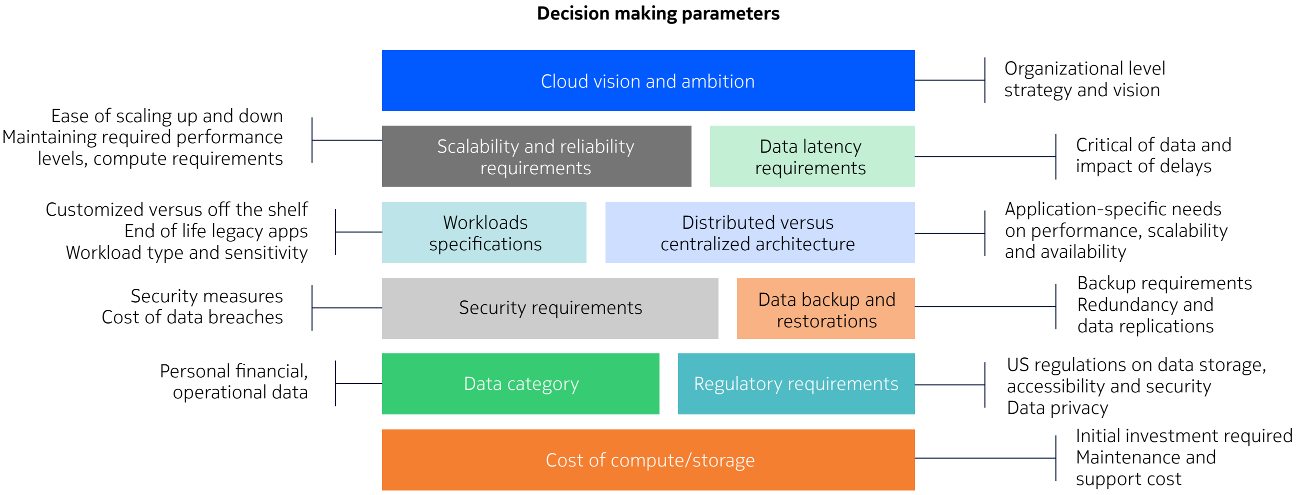
Governments use these insights to secure citizen information and critical infrastructure against cyber threats. Countries can adopt these measures to protect national digital ID systems, e-government platforms, and healthcare data while supporting regional cybersecurity collaboration.

Data storage policy

The framework defines key parameters to create a robust data storage policy, aligning with cloud vision and ambition. It considers scalability, reliability, latency, workload needs, architecture (distributed vs centralized), security, data classification, compliance and cost.

This ensures critical data is stored efficiently, securely and in compliance with regulations. It guides ministries in managing digital assets for e-governance and digital ID programs while balancing accessibility, security, compliance and cost.

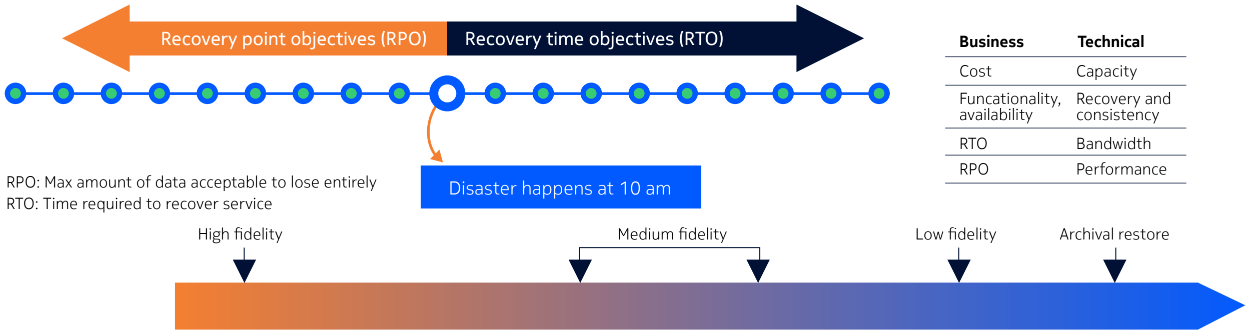
Figure 4. Decision-making parameters to define data storage policy


Decision making parameters
Cloud vision and ambition
Organizational level strategy and vision
Ease of scaling up and down
Maintaining required performance levels, compute requirements
Scalability and reliability requirements
Data latency requirements
Critical of data and impact of delays
Customized versus off the shelf
End of life legacy apps
Workload type and sensitivity
Workloads specifications
Distributed versus centralized architecture
Application-specific needs on performance, scalability and availability
Security measures
Cost of data breaches
Security requirements
Data backup and restorations
Backup requirements
Redundancy and data replications
Personal financial, operational data
Data category
Regulatory requirements
US regulations on data storage, accessibility and security
Data privacy
Cost of compute/storage
Initial investment required
Maintenance and support cost

Disaster recovery and business continuity

The framework defines recovery point objectives (RPO), recovery time objectives (RTO), backup strategies, and offsite replication to maintain continuity for mission-critical services. It highlights vulnerabilities and recommends scalable recovery mechanisms aligned with business priorities.

Figure 5. Considerations for disaster recovery


Recovery point objectives (RPO)
Recovery time objectives (RTO)
Disaster happens at 10 am

RPO: Max amount of data acceptable to lose entirely
RTO: Time required to recover service

Business	Technical
Cost	Capacity
Funcationality, availability	Recovery and consistency
RTO	Bandwidth
RPO	Performance

	High fidelity	Medium fidelity		Low fidelity	Archival restore
Approach	• Active-Active • Active-Standby with geo-failover	• Active-Standby • Warm/cold	• Replicated data • Other resources spun up	• Backup recovery from replicated data at geo-redundant site	• Local backup and restore
RPO/RTO	• Near real-time	• Minutes	• Minutes to hours	• Hours to days	• Hours to days
Protection granularity	• Entire workload	• Entire workload	• Entire workload	• Entire / partial workload	• Files, DBs, VMs
Cost	$$$$	$$$	$$	$	$

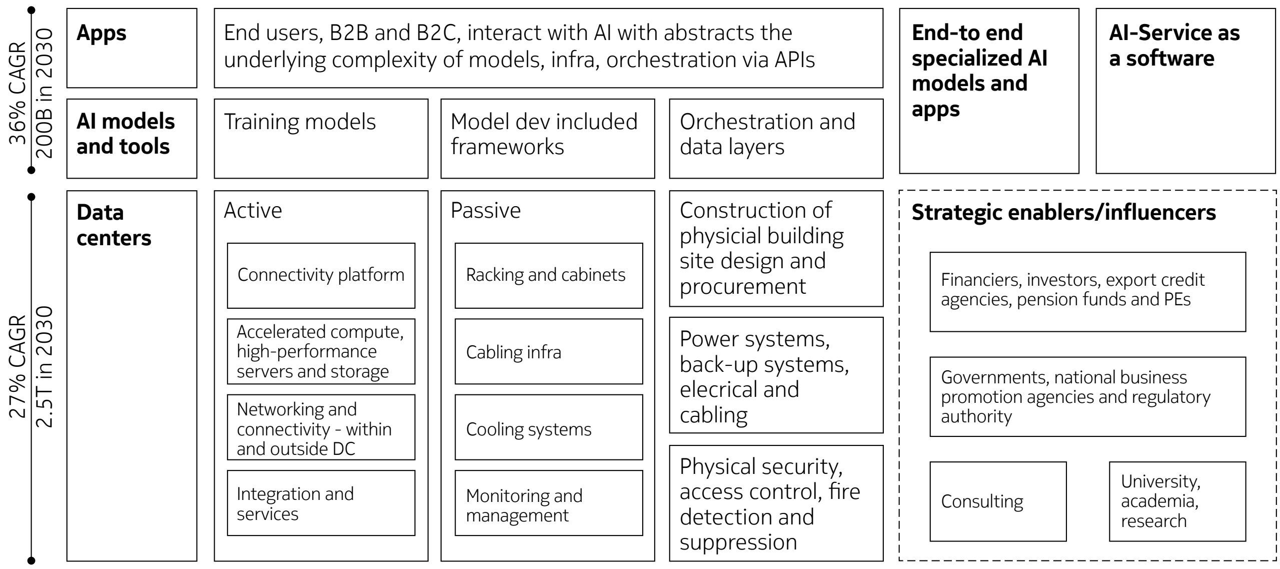
Globally, this ensures uninterrupted public services during outages or disasters. For example, it can secure continuity for e-government portals, national ID systems and emergency response platforms, minimizing downtime and protecting citizen data.

Experience in building and managing data centers

This is crucial for successful deployment and operation. A deep understanding of the unique security, compliance and regulatory requirements that govern the storage and processing of sensitive data is required. In addition, as the data center will be used for essential public services, efficiency, scalability and reliability are key attributes of the design.

As the number of stakeholders involved in the data centers increases, there are some key steps to take, starting with finding the right partner to provide the right connectivity within the data center as well as between data centers. Other steps include providing efficient cooling infrastructure, a full data center security framework and partnering with recognized actors in the market who can federate others around an overall solution.

Figure 6. Holistic data center technology stack as a blueprint for ecosystem development strategy



36% CAGR
200B in 2030
27% CAGR
2.5T in 2030
Apps
End users, B2B and B2C, interact with AI with abstracts the underlying complexity of models, infra, orchestration via APIs
End-to end specialized AI models and apps
AI-Service as a software
AI models and tools
Training models
Model dev included frameworks
Orchestration and data layers
Data centers
Active
Connectivity platform
Accelerated compute, high-performance servers and storage
Networking and connectivity - within and outside DC
Integration and services
Passive
Racking and cabinets
Cabling infra
Cooling systems
Monitoring and management
Construction of physicial building site design and procurement
Power systems, back-up systems, elecrical and cabling
Physical security, access control, fire detection and suppression
Strategic enablers/influencers
Financiers, investors, export credit agencies, pension funds and PEs
Governments, national business promotion agencies and regulatory authority
Consulting
University, academia, research

Design flexibility and emerging technology enablement

As data centers continue to evolve, it is essential to consider the impact of emerging technologies such as AI and quantum computing on future design and operations. For example, the data center fabric is already evolving to consider the change in traffic flow and requirements triggered by AI workloads. Additional work is being done to validate Ethernet-based fabrics with data center compute and storage, creating a future proof blueprint and minimizing deployment and operational risks.

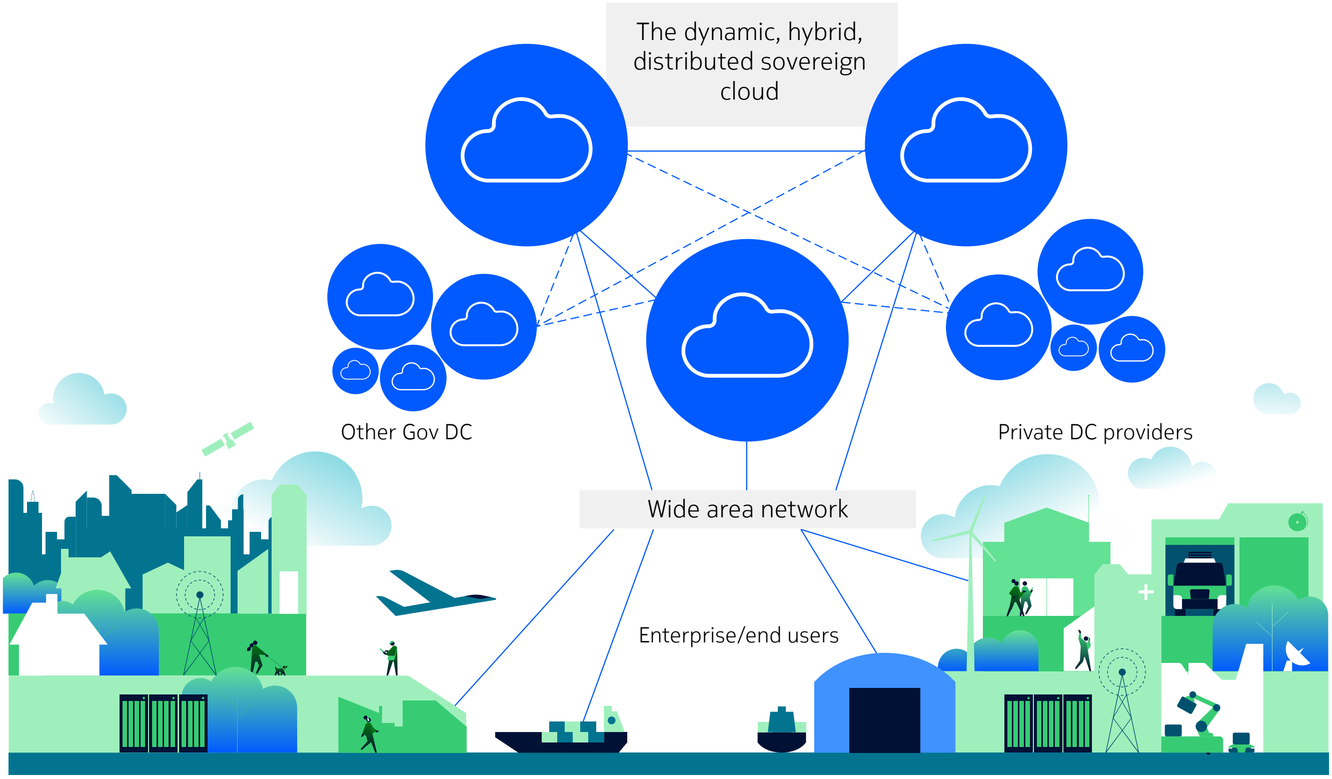
Quantum computing is emerging as the next evolution in computing after CPUs and GPUs. Considering early exposure to quantum computing capability can enable countries to be ahead of the curve and maintain a competitive advantage in the global economy. With time, as quantum computing becomes mature, more complex systems such as climate models, economic systems and social networks can be simulated, enabling the government to model and predict their behavior.

Data center interconnection

There is “no cloud without connectivity”. Just as you wouldn’t build a 100,000-seat stadium accessible only by a single-lane country road, you shouldn’t deploy massive computing and AI capabilities without ensuring your network pipes can handle the traffic flow in both directions. Given the diverse geography of states, as well as the evolution of traffic flow, the sovereign data center needs to be connected to:

- Other sovereign data centers
- Commercial data centers for back up and/or offering complementary service
- Edge clouds
- Enterprise/end users.

Figure 7. Sovereign national data center connectivity vision

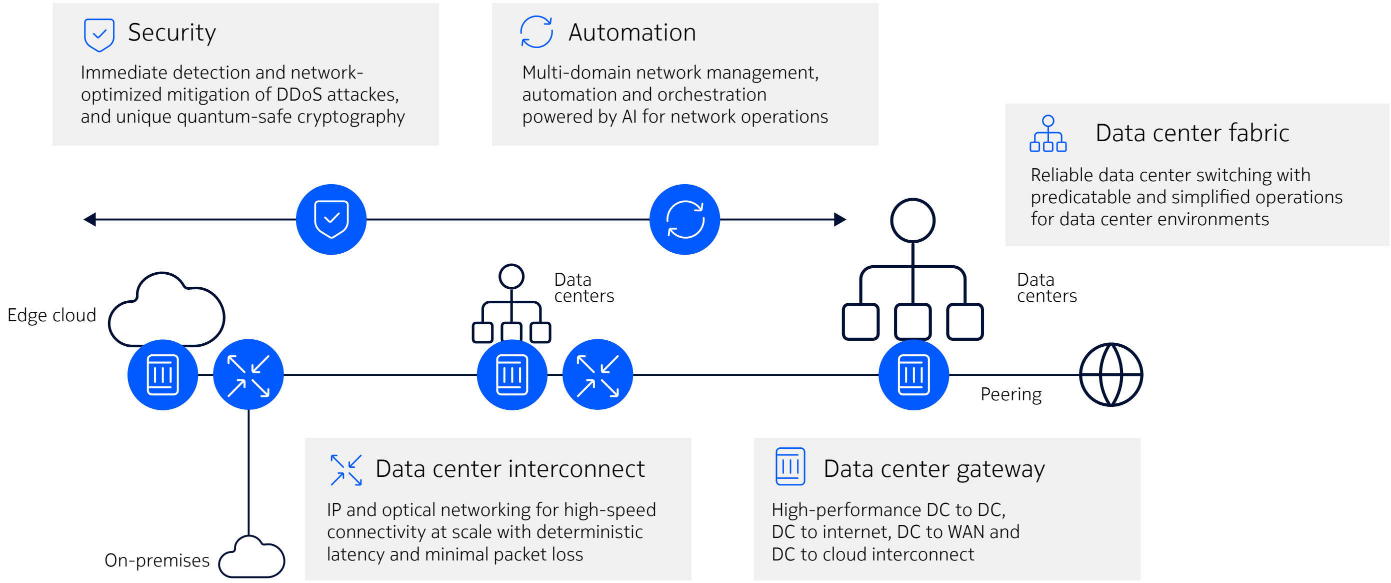


The following capabilities are current best practice in the industry:

- Data center interconnection, which, given the diverse geography of states, can be a mix of terrestrial and subsea capabilities, as well as hybrid models between owned and leased fiber
- Data center gateways can provide complementarity for service agility and flexibility
- As sovereign data centers are expected to handle more AI workloads, deploying a data center fabric from day one is required to handle more demanding intra- and inter-data center connectivity; terminating with a reliable data center fabric ensures predictable and simplified operations in the data center environment

- As quantum computing is still evolving, deploying a quantum-safe network from day one should be a key requirement to safeguard agencies against harvest-now-decrypt-later threats while ensuring the sovereign network is prepared and ready to answer cyber threats at any time, even for the day quantum computing becomes mature and widely available to bad actors
- Distributed denial of service (DDoS) attacks being on the rise and increasingly sophisticated and with the expected scale and decentralization of data centers, it is imperative to deploy a scalable DDoS detection and mitigation solution.

Figure 8. Reliable, automated and secure cloud networking



Security
Immediate detection and network-optimized mitigation of DDoS attackes, and unique quantum-safe cryptography

Automation
Multi-domain network management, automation and orchestration powered by AI for network operations

Data center fabric
Reliable data center switching with predicatable and simplified operations for data center environments

Data center interconnect
IP and optical networking for high-speed connectivity at scale with deterministic latency and minimal packet loss

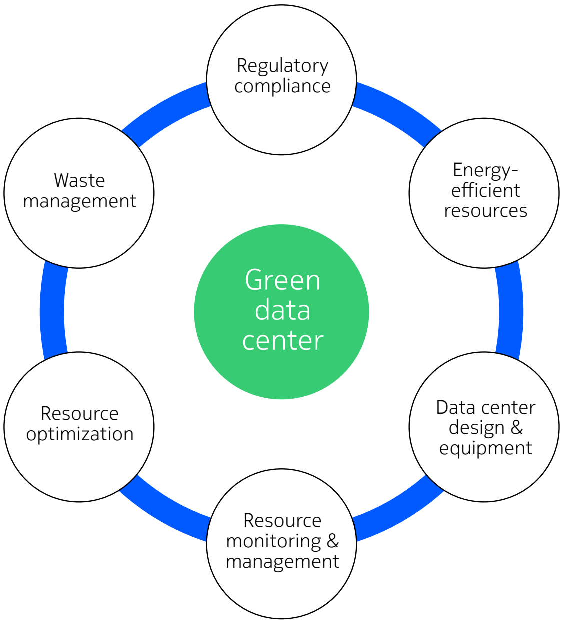
Data center gateway
High-performance DC to DC, DC to internet, DC to WAN and DC to cloud interconnect

Environment sustainability

The IT industry, particularly data centers, is increasingly recognizing the need for sustainability due to their high energy consumption, carbon emissions and environmental impact. As data processing demand grows, traditional data centers face challenges, including carbon emissions, electronic waste and water usage. Green data centers, designed and operated according to international standards, minimize environmental impact by optimizing hardware, infrastructure and resource management while maximizing operational efficiency and energy performance. Key practices include energy efficiency, renewable energy usage, waste management, monitoring and regulatory compliance.

Globally, energy-efficient data centers lead to cost savings, environmental sustainability and scalability while supporting regulatory compliance and climate goals. Metrics such as power usage effectiveness (PUE), carbon emission intensity, renewable energy usage, water usage effectiveness (WUE), and electronic waste recycling rate help governments measure performance and guide improvements. With growing digital infrastructure and national climate targets, sustainable data centers can reduce energy costs, lower carbon footprint and promote renewable energy adoption. Metrics like PUE, data center efficiency (DCE) and greenhouse gas (GHG) emissions provide insights for agencies to track efficiency and align with broader goals under national energy and climate policies.

Figure 9. Facets of green data centers


Regulatory compliance
Energy-efficient resources
Data center design & equipment
Resource monitoring & management
Resource optimization
Waste management
Green data center

Energy-efficient technologies such as free cooling, liquid cooling and smart temperature management improve sustainability and operational performance. Globally, monitoring and analyzing environmental metrics enable data-driven improvements and support responsible resource usage. Applying these practices can guide public and private sector data centers to meet energy efficiency targets, contribute to national sustainability initiatives and provide a benchmark for countries' digital infrastructure.

Financing

Sovereign data centers represent long-term infrastructure investments that require significant upfront capital and sustained operational funding. It requires that the financing mechanisms balance urgent digitalization needs and sovereignty mandates with sustainable business cases and ensure that the funding covers needs related to planning, construction, operation and upgrades.

To this end, the Finnish government along with its funding partners and the EU is highly motivated to support the other governments' digital infrastructure plans and strategy. In addition to funding the key ecosystem players, it has planned project financing options with the European Investment Bank (EIB), Finnvera, Finnfund and Export Development Canada (EDC).

Export credit agencies (ECAs) are increasingly critical enablers of sovereign data center strategies, bridging the gap between policy ambition and financial execution. Finnvera is Finland's export credit agency and can support the project with guarantees, project financing, and buyers' credits if the data center strategy involves purchasing equipment, services or solutions from Finnish companies.

EDC offers project finance and debt solutions that can underpin large-scale infrastructure investments, ensuring governments have access to competitive capital for building secure, sovereign compute environments. Beyond financing, EDC's mandate allows it to catalyze broader impact by facilitating partnerships that integrate Canadian technology solutions into the stack—reinforcing resilience, compliance and innovation. By combining financial instruments with strategic technology engagement, ECAs like EDC and Finnvera help governments accelerate deployment while safeguarding sovereignty objectives, particularly when done with ECAs from EU or EU-friendly nations.

Finnfund is a development financier and impact investor of the Finnish government. Finnfund puts special emphasis on sectors that are critical to sustainable development like renewable energy, sustainable forestry, sustainable agriculture, financial institutions and digital infrastructure and solutions. It can provide lower-cost capital, technical assistance grants, co-invest equity or debt investments.

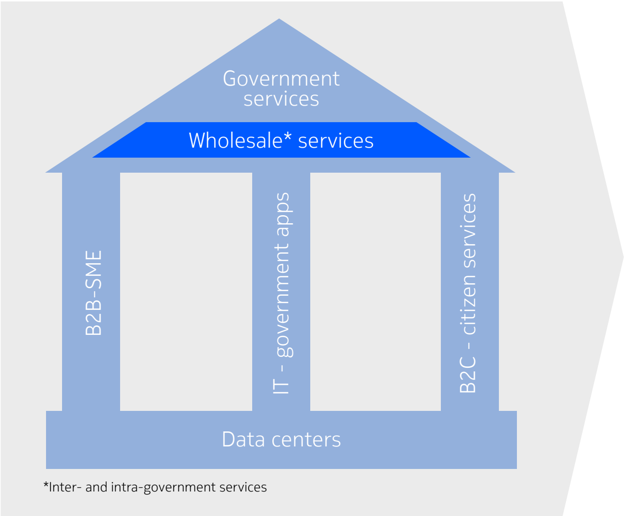
The European Investment Bank (EIB) is one of the biggest multilateral financial institutions in the world and one of the largest providers of climate finance. The available financial instruments could be applied either directly to a project or by financing the public share in a public private partnership structure. This financing solution would allow the EIB to request grant financing from the budget of the EU to support the project, which could be used, for example, to complete studies on detailed engineering design and capacity building activities as well as other uses that can be identified in coordination with the concerned party.

Bell Labs Consulting and Business Finland have extensive experience and can support governments to select the right financial instruments in line with strategic priorities.

Models for operating and building sovereign data centers

Adopting this model means the government can build sovereign facilities for critical workloads while leveraging global partnerships to accelerate AI and commercial capacity. This will ensure compliance with national regulations, support for SMEs, digital inclusion and sustainable growth, all of which are key government objectives. The decision to select a data center deployment option combines demand, qualitative and financing aspects.

Figure 10. Data center deployment model for governments



*Inter- and intra-government services

1 Business drivers
- Government mandats and policies
- Citizen services and digital transformation
- Data sovereignty and security requirements
- Support to SME industry

2 Demand
- Timeframe: Short-/long-term
- Large-scale storage
- High data security
- Number of rackes
- Rack density (kW/rack)
- Area (m^2)
- Power (MW)

3 Implementation options
- Build
- Partnership
- Leased

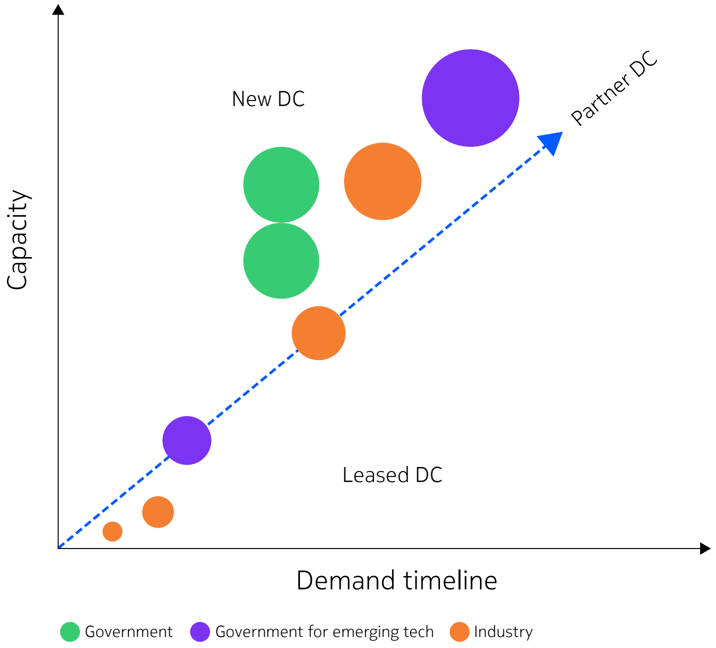
4 Decision framework
- Decision tree (go/no go) analysis
- Financial analysis - investment risk, business case analysis
- Qualitative analysis
- Partnership analysis

Governments can adopt three main deployment models:

- Build, where the state directly develops and operates the facilities
- Partner, where investment and operation are shared with private or foreign entities
- Lease, where data center capacity is rented from third-party providers.

The optimal choice depends on workload type, strategic importance, scalability needs and the desired level of operational oversight.

Figure 11. Data center deployment strategy trends



Summary

A strong global data center plan needs a hybrid approach, carefully balancing a country's control with the ability to innovate quickly. This plan is built on two main ideas:

1. Government-run data centers are used for important national tasks. These DC's make sure that sensitive applications like online government services, national ID systems and public AI projects are controlled, private and secure. This not only protects vital information but also helps the country's economy grow over time and builds local skills in engineering, operations and construction.
2. The strategy involves targeted partnerships with large global tech companies to handle very big, AI-driven and fast-growing business needs. These collaborations attract foreign investment, often channeled through global financial institutions and banks, introduce advanced technologies and share global best practices. This approach significantly reduces capital expenditure and speeds up deployment.

This dual method allows for more data center capacity and abilities. Also, by using outside expertise within clear rules and operational guidelines, countries do not risk national security or financial stability.

Most importantly, building this infrastructure must be closely tied to the overall plan for the country's digitalization journey, including managing data and keeping it safe. Data centers are the foundation of a nation's digital future. Decisions must be guided by important use cases, such as national AI projects needing special computer power, smart city systems requiring local computing power, or digital health records needing very secure storage that follows rules. This approach, driven by specific use cases, ensures that money is spent wisely and optimized for the greatest benefit to society and the economy, while also fostering a vibrant partnership ecosystem for data center development, which includes the government, local and global technology companies, universities, start-up businesses and established companies.

In conclusion, this hybrid approach of combining government-led data center development and partnerships with technology companies will enable advanced data center infrastructure for national digitalization plans. This comprehensive, ecosystem-focused model fosters significant socio-economic growth by empowering new businesses and small-to-medium enterprises (SMEs), attracting global talent and investment, creating jobs, enhancing public services and ultimately positioning the nation at the forefront of the global digital economy for sustained technological leadership and societal prosperity.

Abbreviations

A2A	Application-to-application
AI	Artificial intelligence
AIaaS	AI as a service
AI-Ops	AI operations
AMD	Advanced Micro Devices
APAC	Asia/Pacific
API	Application programming interface
ARPU	Average revenue per user
AWS	Amazon Web Services
CAGR	Compound annual growth rate
CSP	Communications service provider
CX	Customer experience
DC	Data center
DDoS	Distributed denial of service
DCE	Data center efficiency
DCIM	Data center infrastructure management
ECAs	Export credit agencies
EDC	Export Development Canada
EB	Exabytes
EIB	European Investment Bank
EU	European Union
FCS	Frame check sequence
GDP	Gross domestic product
GHG	Greenhouse gas
GPU	Graphics processing unit
GPUaaS	Graphics processing unit as a service
GSMA	Global System for Mobile Communications Association
HD	High definition
IHME	Institute for Health Metrics and Evaluation
IoT	Internet of things
IP	Internet Protocol
IPv6	Internet Protocol version 6
IVP	Intravenous pyelogram
LANs	Local area networks
LLMs	Large language models
MAC	Media access control
MCP	Multi-cloud platform
MW	Megawatts
OECD	Organisation for Economic Co-operation and Development
OTT	Over the top
PBXs	Private branch exchanges
PUE	Power usage effectiveness
RPO	Recovery point objectives
RTO	Recovery time objectives
SD-WAN	Software-defined wide area network
SFD	Start frame delimiter
SME	Small-to-medium enterprise
SMS	Short message service
TAM	Total addressable market
UAE	United Arab Emirates
UN	United Nations
UX	User experience
WUE	Water usage effectiveness
XR	Extended reality

References

[1] Finnish Government, “Finland’s National Roadmap. EU Digital Decade Policy Programme 2030,” Publication of the Finnish Government, Jul 2024. Available: https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/c193a20b-672a-4314-bc7a-fe6908b0dc8c/content

[2] EU, “Europe’s digital decade,” Shaping Europe’s digital future. Available: https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

[3] Nokia, “2025 global traffic report,” 1 Dec 2025. Available: https://www.nokia.com/asset/213660/

[4] L. Francis and R. Sharma, “State of sovereign and industry cloud investment by Asia/Pacific governments,” IDC eBook, 2024. Available: https://info.idc.com/rs/081-ATC-910/images/IDC-State-of-Sovereign-and-Industry-Cloud-Investment-by-AsiaPacific-Governments-eBook.pdf

[5] Gartner, “Forecast analysis: Sovereign cloud IaaS worldwide,” Gartner web site, 25 Oct 2024. Available: https://www.gartner.com/en/documents/5863580#

[6] NumSpot, “About NumSpot,” NumSpot website. Available: https://numspot.com/en/about-us/

[7] GovTech Singapore, “Government on Commercial Cloud,” GovTech website. Available: https://www.tech.gov.sg/products-and-services/for-government-agencies/software-development/government-on-commercial-cloud/

[8] TM One, “TM One poised to offer comprehensive data centre and data sovereignty for the Government’s digital transformation,” TM One press release, 15 Jul 2022. Available: https://www.tmone.com.my/press-release/data-services-for-the-government-digital-transformation/

BUSINESS
FINLAND

Bell Labs Consulting

About Business Finland

We help our customer companies grow and succeed globally, develop solutions for the future and renew their business operations boldly. We promote collaboration between companies and research groups, so that new endeavors can develop into international business ecosystems. We are developing Finland into the most attractive and competitive innovation environment and the most enticing investment and travel destination in the world.

About Bell Labs Consulting

Bell Labs Consulting is the advisory arm of Nokia Bell Labs, providing evidence -based guidance to help organizations realize the full economic, social, and human potential of future technologies. Our cross-disciplinary, global team of seasoned experts combines deep industry knowledge with advanced analytical and technoeconomic modeling to craft actionable, client specific strategies across Business & Services Strategy, Network & Cloud Infrastructure, and Operations & Transformation.

We partner with governments, communications service providers, webscalers, and enterprises to support decision-making, optimize deployments and operations, and accelerate digital transformation. As part of the world-renowned Nokia Bell Labs—whose innovations have earned nine Nobel Prizes and five Turing Awards—we bring a unique research heritage and proprietary toolset to more than 300 engagements worldwide, delivering implementable solutions that drive market leadership, superior service reliability, and sustainable growth.

Contacts

Gaurav Korde, Sr. Partner at Bell Labs Consulting (Gaurav.korde@bell-labs-consulting.com) Tarunava Konar, DMTS at Bell Labs Consulting (Tarunava.konar@bell-labs-consulting) Jeetika Lamba, Head of Ecosystem Development (jeetika.lamba@nokia.com), Nina Jacoby, Project Lead International Business Innovations, Business Finland (nina.jacoby@businessfinland.fi).

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, we’re advancing connectivity to secure a brighter world.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID215164 (December)