IM_

Geopolitical shift in US–EU relations: Cloud services *risk analysis*

Position Brief by Michael de Fine Strand

European organisations face significant strategic vulnerability due to their extensive reliance on US-based cloud service providers. Approximately 70% of Europe's cloud infrastructure is controlled by three American companies – AWS, Microsoft, and Google – creating asymmetric dependencies that could be leveraged in trade disputes, regulatory disagreements, or broader geopolitical tensions.

While catastrophic service disruption remains a low-probability scenario, the potential impact on European digital infrastructure, economic competitiveness, and strategic autonomy warrants serious consideration.

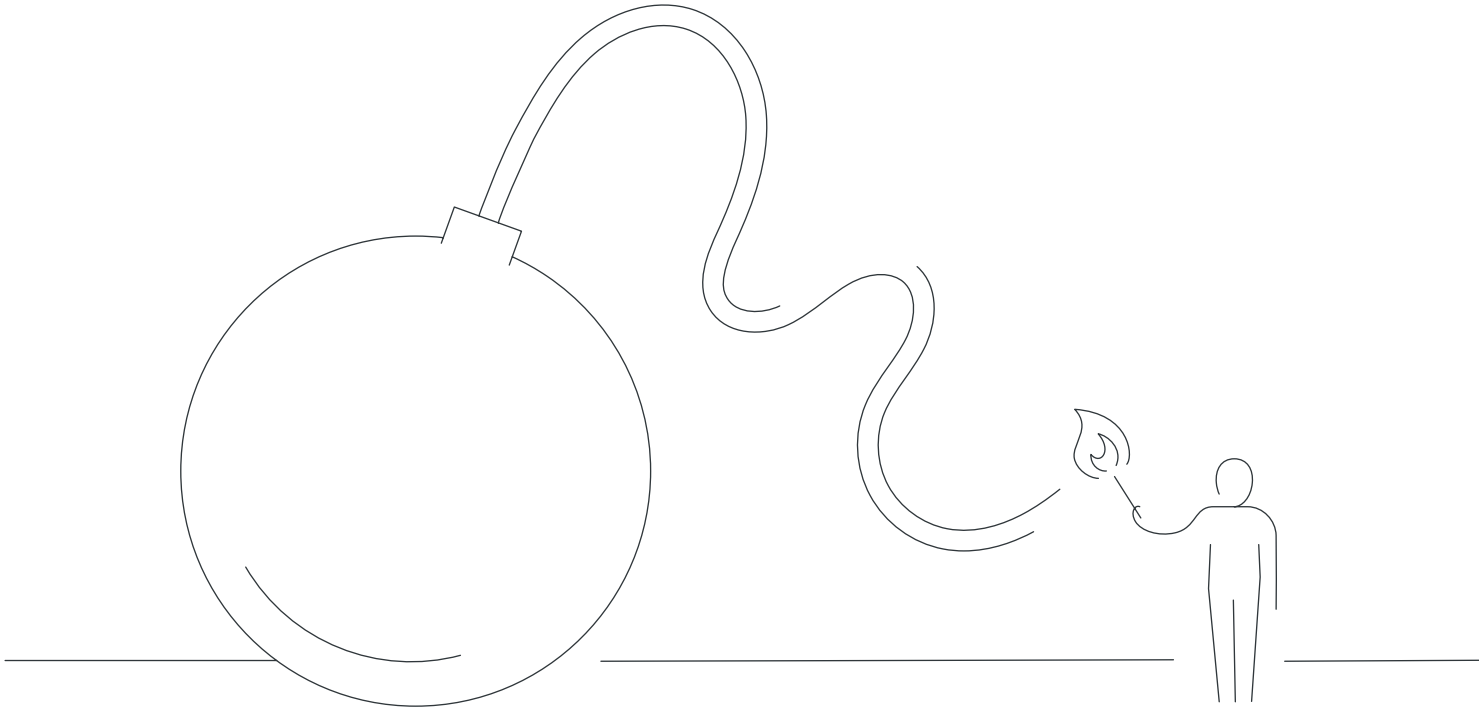
This assessment analyses potential risk scenarios, evaluates their impacts across sectors, and presents a comprehensive framework of mitigation strategies at both institutional and organisational levels. The most effective approach combines EU-level policy measures, technical architecture adaptations, and strategic business continuity planning. Organisations are encouraged to implement a risk-based approach that prioritises critical functions, enhances data sovereignty, diversifies cloud providers, and gradually reduces technical lock-in dependencies.

Current state assessment

Dependency profile

European organisations have developed substantial dependencies on US cloud providers across the following dimensions:

Dependency Type	Description	Severity (1-5)
Market concentration	US providers control ~70% of European cloud market	5
Technical lock-in	Proprietary APIs and integrated services create high switching costs	4
Infrastructure gap	Limited presence of European-controlled hyperscale data centres	4
Innovation reliance	Dependence on US platforms for AI, analytics, and computing capabilities	3
Strategic sector penetration	Critical industries have embedded US services in core operations	5



Strategic vulnerability assessment

This asymmetric dependency creates leverage that could be exploited through:

- Negotiation leverage: Cloud access used as bargaining tool in trade or regulatory disputes
- Compliance pressure: Service continuation tied to alignment with US policy preferences
- Selective targeting: Restrictions against specific organisations or sectors to create pressure
- Undermining EU cohesion: Differential treatment creating divisions in European policy positions

Industry risk profiles

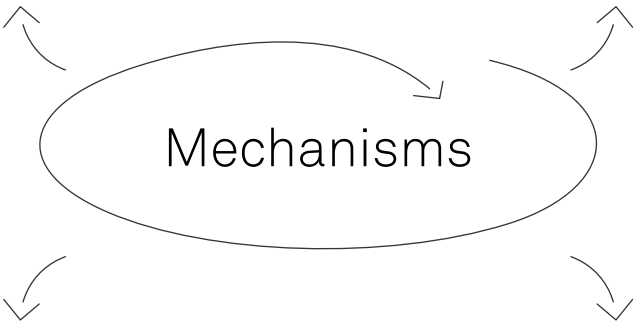
Sector	Dependency level (cloud services)	Vulnerability factors	Impact severity
Financial services	High	Customer data, transaction processing, regulatory reporting	Critical
Healthcare	High	Patient records, research data, operational systems	Critical
Manufacturing	Medium-High	Supply chain management, IoT infrastructure, design systems	Severe
Public administration	Medium	Citizen services, data management, interagency communication	Severe
Telecommunications	High	Network management, customer data, service delivery	Critical
Defense and Aerospace	Medium	Non-classified operations, logistics, administrative systems	Severe
Energy	High	Grid management, trading operations, distribution systems	Critical

Scenario 1: Selective industry targeting

The US strategically restricts cloud access for European industries through a layered approach of export controls and technical constraints. This creates economic pressure, technological disadvantages, and competitive imbalances in sectors deemed strategic competitors to US interests or relevant to national security priorities.

Scenario 2: Data sovereignty countermeasures

US deliberately implements overlapping compliance frameworks, creating irreconcilable legal conflicts with EU regulations. This forces European entities to choose between violating EU law or losing access to essential cloud services. The resulting legal deadlock makes compliance with both jurisdictions technically and operationally unfeasible.



Scenario 3: Strategic client restrictions

US leverages precision targeting of specific European entities to create asymmetric pressure while avoiding broader market disruption. This selective approach undermines EU regulatory enforcement capabilities, strategic digital initiatives, and technology development, while maintaining plausible deniability about systematic discrimination.

Scenario 4: Tiered access structures

The US implements a sophisticated differentiation system (the “Enhanced Mechanism”) that creates structural divisions within the EU by providing varied levels of service access based on bilateral agreements and policy alignment. This creates internal competitive imbalances between member states, undermines EU cohesion, and incentivises individual countries to make strategic concessions to maintain technology access.

Historical precedents

Scenario 1: Selective industry targeting

Similar approaches were implemented through the Entity List restrictions against Huawei in 2019, effectively cutting the company off from US technology suppliers and cloud services. The US has also previously used the International Emergency Economic Powers Act to restrict technology access for specific sectors in countries such as Russia and Iran. The Commerce Department's restrictions on semiconductor technology to China in 2022-2023 demonstrated the capability to target specific technical capabilities within an industry.

Scenario 2: Data sovereignty countermeasures

The CLOUD Act (2018) created direct conflicts with GDPR by requiring US-based companies to provide data regardless of where it was stored. The invalidation of Privacy Shield by the Schrems II decision highlighted how US surveillance laws created fundamental incompatibilities with EU data protection requirements. Similar conflicts arose when the US demanded access to SWIFT financial data despite EU privacy concerns, creating compliance dilemmas for financial institutions.

Scenario 3: Strategic client restrictions

The Office of Foreign Assets Control (OFAC) has implemented entity-specific sanctions against companies like Kaspersky Lab, restricting their access to US services. The Treasury Department's targeted financial sanctions against specific Russian entities demonstrated the ability to isolate individual organisations. The Commerce Department's restrictions against specific Chinese technology companies, such as ZTE, showed how individual entities can be effectively targeted with service disruptions.

Scenario 4: Tiered access structures

The Five Eyes intelligence alliance creates different levels of information sharing between the US and European countries. The US has implemented preferential technology access through bilateral agreements with countries such as the UK and Australia (e.g., AUKUS), which exclude other allies. Visa Waiver Program requirements have been used to create differential treatment between EU countries based on bilateral security agreements. Defense technology transfers have historically varied based on country-specific agreements, creating capability disparities.

Impact

Scenario 1:

Selective industry targeting

2

Impacted sectors	Potential impact
• **Aerospace:** Flight systems, manufacturing automation, supply chain • **Defense:** R&D infrastructure, logistics systems, non-classified operations • **Automotive:** Connected vehicle services, autonomous driving development • **Pharmaceuticals:** Clinical trials data, research collaboration platforms • **Energy:** Grid management, trading operations, exploration data processing	• Significant operational disruption requiring rapid response measures • Substantial R&D capability reduction affecting innovation pipelines • Competitiveness decline from AI/ML capability limitations • Supply chain visibility disruption affecting just-in-time manufacturing • Considerable emergency migration costs for affected enterprises • Strategic programme delays affecting key industrial initiatives

Scenario 2:

Data sovereignty countermeasures

3

Impacted sectors	Potential impact
• **Financial Services:** Banking systems with personal data handling • **Healthcare:** Patient medical records in cloud environments • **Insurance:** Client data and risk assessment infrastructure • **Public Administration:** Government services databases • **Retail:** Customer data management systems • **Education:** Student record systems and research databases	• Compliance deadlock forcing service discontinuation • Regulatory penalties from inability to satisfy conflicting requirements • Legal uncertainty creating operational paralysis • Trust degradation in digital service delivery

Scenario 3:

Strategic client restrictions

1

Impacted sectors	Potential impact
• **EU regulatory bodies:** DMA/DSA enforcement agencies • **Competition authorities:** Entities investigating US tech companies • **Digital sovereignty proponents:** Organisations developing EU alternatives • **Technology challengers:** Companies competing with US tech giants • **Research institutions:** Advanced technology development centres	• Regulatory enforcement capability reduction • Strategic initiative disruption • Competitive disadvantage for targeted organisations • Chilling effect on regulation and competition policy

Scenario 4:

Tiered access structures

2

Access tiers	Potential impact
• **Premium:** Full service for compliant countries • **Standard:** Limited functionality with additional monitoring • **Restricted:** Significant limitations on advanced capabilities	• Undermining EU cohesion through differential treatment • Competitive imbalance between EU member states • Pressure on individual countries to make bilateral concessions • Innovation disparity based on service tier access

Probability

- Lower numbers (1) represent low probability/severity
- Mid-range numbers (2-3) represent medium probability/severity
- Higher numbers (4-5) represent high probability/severity

Cloud provider response capabilities

Legal and contractual countermeasures

Cloud providers have several mechanisms that could potentially limit or delay implementation of government restrictions:

Contractual shields:

- Government interference clauses with notification requirements
- Service continuity guarantees with financial penalties
- Multi-jurisdictional contract structures creating procedural hurdles

Litigation strategies:

- Constitutional challenges on First Amendment and Commerce Clause grounds
- Administrative appeals and judicial review to delay implementation
- Industry consortium legal challenges amplifying resistance

Technical implementation barriers

Architecture adaptations:

- Sovereignty-preserving technical designs
- Distributed processing systems
- Regional isolation capabilities

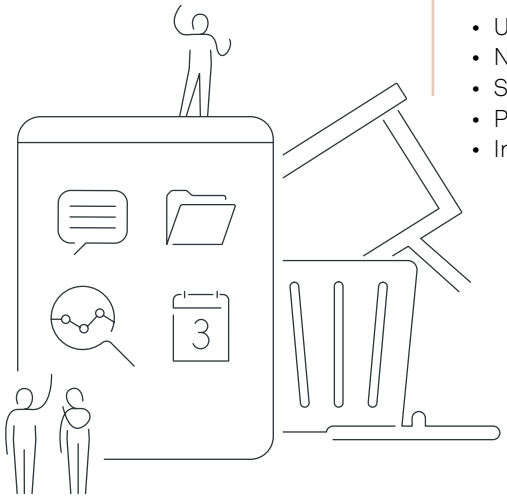
Data protection enhancements:

- Zero-knowledge infrastructure reducing access capabilities
- Client-controlled encryption key management
- European-specific technology stacks with reduced US dependencies

Limitations assessment

Despite these potential countermeasures, significant constraints exist:

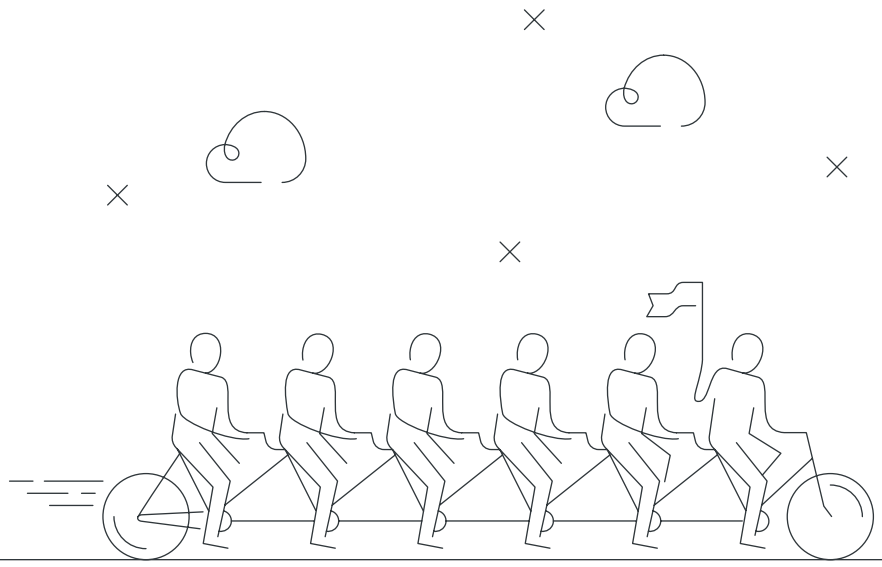
- US-based entities must ultimately comply with lawful government orders
- National security justifications typically override commercial considerations
- Severe penalties for non-compliance create strong compliance incentives
- Public companies face fiduciary obligations limiting resistance capacity
- Individual vendor resistance may be undermined by competitor compliance



EU response capabilities

Regulatory framework enhancements

Measure	Description	Implementation timeframe	Effectiveness (1-5)
Digital sovereignty legislation	Comprehensive legal framework requiring critical data and services to remain under EU jurisdiction	Medium-term	4
Service continuity requirements	Mandatory operational continuity regardless of foreign intervention	Short-term	3
Multi-vendor mandates	Requirements for critical sectors to maintain service redundancy	Medium-term	4
Digital Services Act expansion	Strengthened regulations including infrastructure resilience	Medium-term	3
Foreign technology assessment	Formal evaluation process for non-EU technology dependencies	Short-term	2



Strategic infrastructure development

Measure	Description	Implementation timeframe	Effectiveness (1-5)
Digital sovereignty legislation	Comprehensive legal framework requiring critical data and services to remain under EU jurisdiction	Medium-term	4
Service continuity requirements	Mandatory operational continuity regardless of foreign intervention	Short-term	3
Multi-vendor mandates	Requirements for critical sectors to maintain service redundancy	Medium-term	4
Digital Services Act expansion	Strengthened regulations including infrastructure resilience	Medium-term	3
Foreign technology assessment	Formal evaluation process for non-EU technology dependencies	Short-term	2

Economic and trade measures

- Reciprocal market access mechanisms creating consequences for discriminatory actions
- Sovereign cloud certification with procurement advantages
- Digital services taxation funding European alternatives
- Strategic technology alliances with like-minded nations
- Coordinated public sector procurement maximising negotiating power

International diplomatic initiative

- Digital trade agreements with binding service continuity guarantees
- Technology neutrality treaties establishing non-discrimination principles
- Multi-stakeholder governance of critical digital infrastructure
- Specialised arbitration frameworks for service disruption disputes
- International reporting requirements for government interference

Public/private organisation response

Technical architecture adaptations

Container-based architecture implementation: Containerisation offers significant advantages for reducing cloud provider lock-in by creating portable application packages that can run consistently across different environments.

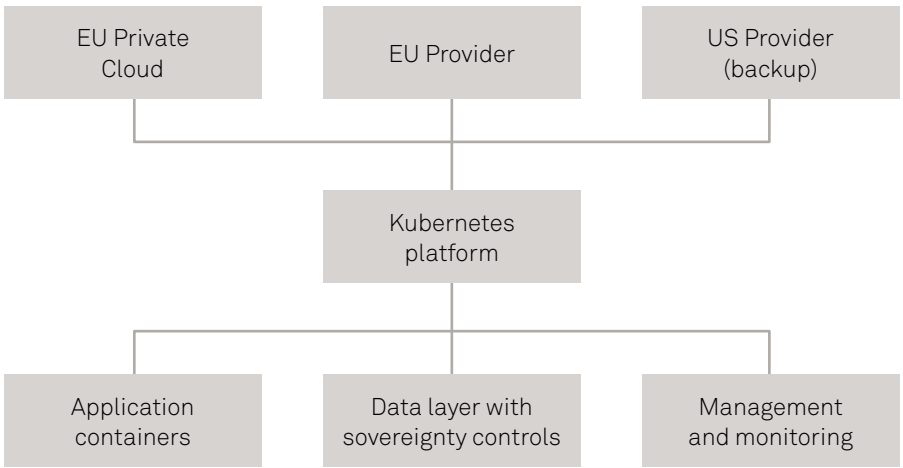
Key benefits:

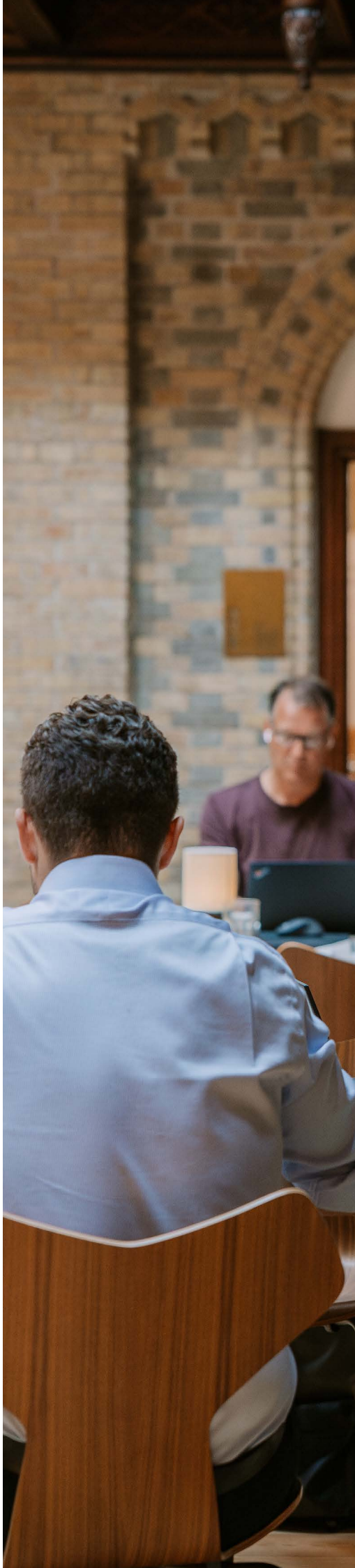
- Infrastructure abstraction reducing direct dependencies
- Consistent management layer across environments
- Rapid workload migration capabilities
- Standardised runtime environment across providers
- Operational continuity during transitions

Implementation approach:

- Standardise on Kubernetes for cross-environment orchestration
- Implement container registries within EU jurisdiction
- Develop deployment pipelines supporting multiple targets
- Document configuration requirements to ensure consistent operation
- Maintain infrastructure-as-code templates for environment replication
- Establish container security and compliance verification

Technical diagram





Contractual and legal protections

- Provider diversification policy requiring multiple providers with different jurisdictional exposure
- Exit strategy documentation with continuously updated migration procedures
- Service continuity clauses with specific requirements and penalties
- Data repatriation rights ensuring contractual guarantees for data transfer
- Force majeure exclusions specifically addressing government actions

Operational resilience measures

- Regular continuity exercises simulating provider unavailability
- Alternative provider readiness with active relationships
- Technical skills development for multi-provider environment management
- Critical workload protection with enhanced safeguards
- Strategic data localisation within EU jurisdiction

Risk management framework

Digital dependency assessment:

- Comprehensive analysis of exposure to non-EU infrastructure
- Critical function identification with impact evaluation
- Technical lock-in measurement across systems
- Regulatory compliance conflict analysis
- Transition capability evaluation

Business continuity planning:

- Geographic and jurisdictional backup diversity
- Offline operational modes for critical functions
- Recovery time objectives for different disruption scenarios
- Technology escrow arrangements securing critical components
- Alternative processing arrangements with EU-based providers

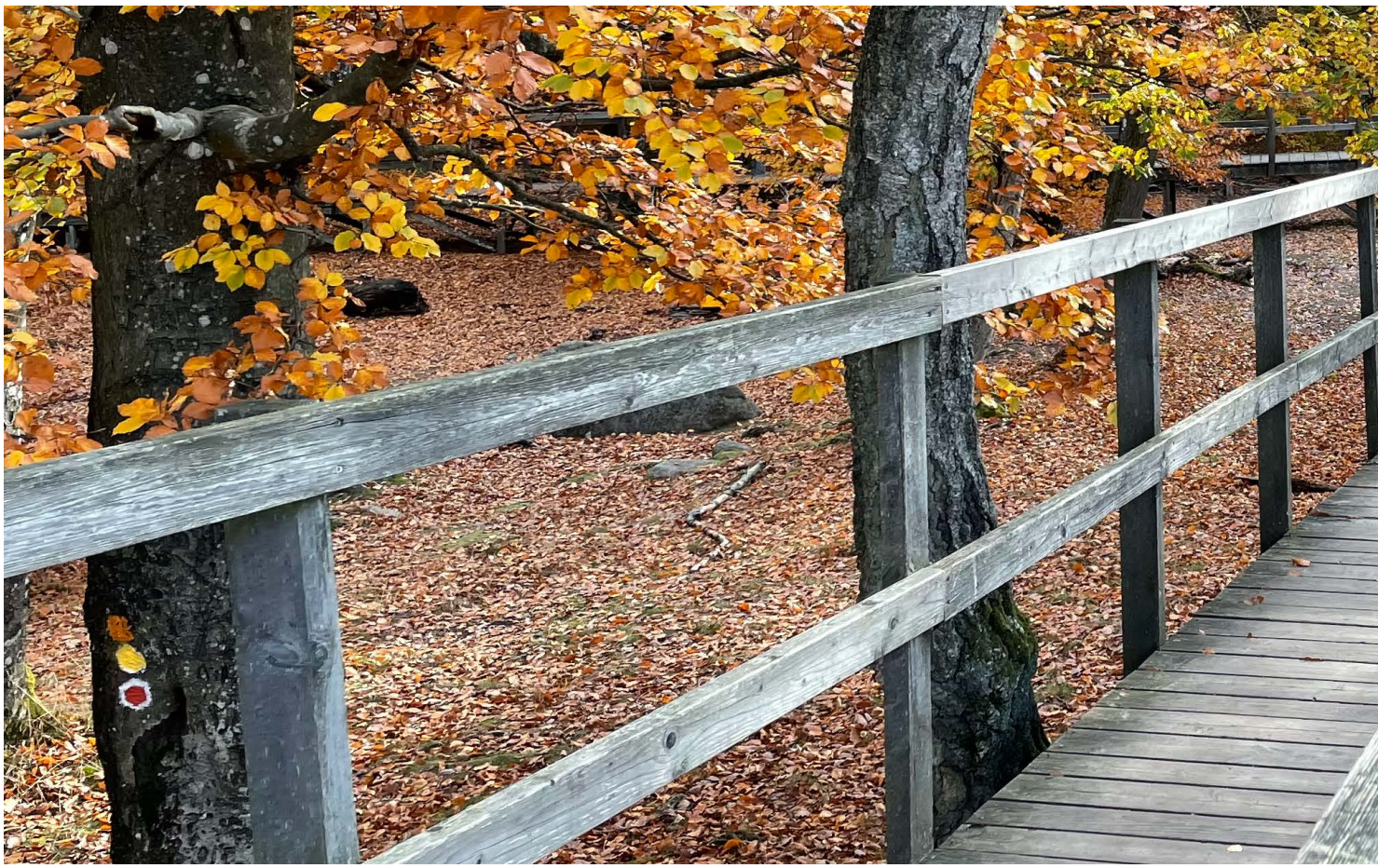
Implementation roadmap

Immediate actions (0-6 months)

- Complete digital dependency assessment
- Identify critical systems requiring priority protection
- Develop initial migration plans for highest-risk workloads
- Review and enhance contractual protections
- Begin staff capability development for multi-cloud management

Short-term measures (6-18 months)

- Implement container-based architecture for critical workloads
- Establish data sovereignty controls for sensitive information
- Deploy initial multi-cloud capabilities for priority systems
- Conduct provider disruption simulation exercises
- Develop comprehensive continuity procedures.



Medium-term strategy (18-36 months)

- Expand containerisation across broader application portfolio
- Implement comprehensive multi-cloud management
- Reduce proprietary feature dependencies
- Pilot European provider alternatives for suitable workloads
- Develop automated migration capabilities

Long-term vision (36+ months)

- Achieve balanced provider distribution minimising concentration risk
- Establish complete operational independence from any single provider
- Implement full sovereign control over critical data and processes
- Contribute to development of European cloud ecosystem
- Maintain strategic flexibility adapting to evolving geopolitical landscape

Contact

For more information, please contact:

Michael de Fine Strand
Implement Consulting Group
+45 2320 0471
mist@implement.dk