Europe’s CADA, AI and Strategic Control

Europe’s strategic control framework for Cloud & AI.

aruba.it

INTRODUCTION

For more than a decade, the European Union has built a regulatory architecture for trusted digital systems. **eIDAS 2.0** strengthens digital identity and trust services. **NIS2** raises the cybersecurity baseline. **DORA** requires operational resilience in financial services. The **AI Act** establishes obligations for the safe, transparent and accountable use of Artificial Intelligence.

Together, these frameworks establish a clear principle: digital systems must be secure, resilient, traceable and governable by design.

As organisations place core processes, sensitive data, critical services and AI-enabled workflows into cloud environments, the strategic question is no longer how those systems are regulated. It is whether the infrastructure beneath them can be controlled, secured, evidenced, recovered and evolved over time.

This is the context for the proposed **Cloud and AI Development Act–CADA**.

CADA seeks to strengthen the European cloud and AI ecosystem through infrastructure investment, data-centre development, innovation and a common sovereignty framework. Its proposed Union Assurance Levels introduce a more structured way to assess cloud and AI services according to where they operate, who controls them, how their software dependencies are governed and how exposed they are to third-country interference.

For organisations, CADA changes the cloud decision. Data residency remains important, but it is no longer sufficient. Crucial workloads require an assessment of ownership, jurisdiction, operational control, cybersecurity, software supply chains, recovery, portability and auditability.

Not every workload needs the same degree of sovereignty, and not every organisation needs to replace global cloud ecosystems. But organisations do need a credible European foundation for the workloads they cannot afford to leave to unexamined dependency.

At Aruba we provide a **Sovereign Core Architecture** for core processes, sensitive data, regulated workloads, crucial digital services and controlled AI environments.

This means bringing together the control layers that matter most:

- European infrastructure and cloud operations;
- clear operational accountability:
- cybersecurity and resilience;
- digital identity and qualified trust services;
- connectivity and data control;
- auditability and evidence;
- portability, recovery and exit capability;
- AI-ready compute and controlled deployment options.

A Sovereign Core Architecture does not mean building an isolated technology estate or requiring every component to be European. It establishes the verifiable conditions under which a crucial workload remains **compliant**, **governable** and **under your control**: known jurisdiction, accountable operations, protected data, controlled access, resilient infrastructure, auditable dependencies and a credible route to recovery or exit.

Regulation defines what trustworthy digital systems must be. CADA addresses the capacity required to operate them. Strategic Control is the ability to bring both **together**.

Summary

01 | **Europe's cloud moment** 5

02 | **What CADA brings** 7

03 | **Beyond data residency** 10

04 | **AI makes infrastructure strategic** 12

05 | **What CADA changes for organisations** 15

06 | **The new value of the independent cloud** 17

07 | **The Sovereign Core Architecture** 19

08 | **From compliance to strategic control** 22

09 | **CONCLUSIONS** 23

CHAPTER 01

Europe's cloud moment

From digital regulation to digital capacity

The first phase was about setting rules. Europe has built a comprehensive framework to ensure that digital services are trustworthy, secure and accountable.

Identity must be verifiable. Cyber risk must be managed. Critical services must remain operational. AI must be developed and deployed responsibly.

The second phase is about capacity. It asks whether Europe has enough cloud, datacenter, network and AI computing infrastructure to operate its most important digital services with a sufficient degree of autonomy and control.

This question has become urgent for three reasons.

First, **cloud infrastructure and services have increasingly been asked to manage core business applications, customer platforms, data environments, security services, collaboration systems and production workflows**.

The failure, unavailability or loss of control of those services can affect the continuity of the organisation itself.

Second, **AI is increasing the strategic importance of infrastructure**. AI requires large-scale compute, extensive data processing, high-performance networking, secure storage, specialist operational skills and significant energy. It is creating a new dependency chain beneath business processes and public services: from model to data, from data to cloud, from cloud to infrastructure, and from infrastructure to energy and operational control.

Third, **geopolitical, legal and supply-chain dependencies have become more visible**. The question is no longer only where data is stored. It is also who controls the service, which legal authorities can affect it, who can

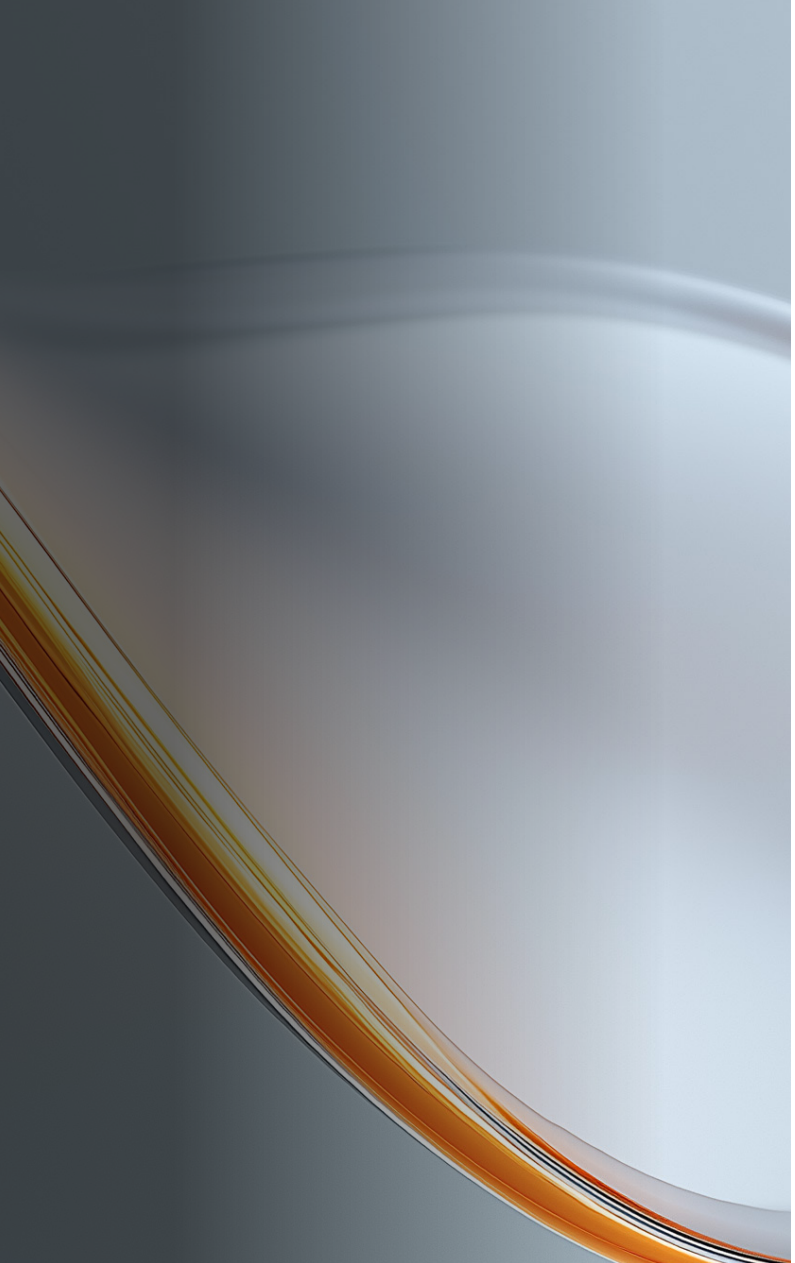
access or update it, what happens if a critical supplier fails and whether the organisation can recover or move the workload if required.

The proposed CADA responds to this context. It is intended to strengthen Europe's cloud and AI ecosystem, improve the conditions for capacity and investment, and create an EU-wide framework for assessing cloud and AI sovereignty.

This is not a call for technological isolation. Europe will remain interconnected with global technology ecosystems. Organisations will continue to use diverse providers, platforms, applications and specialist AI capabilities. But for crucial workloads, dependence can no longer be treated as an accidental by-product of cloud adoption.

It must be designed, managed and, where necessary, reduced.

Infrastructure choice has become part of resilience, governance and long-term operating strategy. An organisation may retain the same applications and cloud services, yet face a different level of business risk depending on whether it can evidence, recover, secure and, if required, move the environment that supports them.



CHAPTER 02

What CADA brings

Capacity, assurance and a new cloud debate

CADA is a proposed European regulation intended to strengthen the cloud and AI ecosystem across the Union.

CADA remains a proposal. Its final text, implementation arrangements, assurance criteria and timetable may change during the legislative process. But its strategic direction is clear.

Europe intends to increase cloud and AI capacity while developing a more consistent way to assess sovereignty and risk.

Four elements are important. The first two (capacity and the proposed assurance framework) are direct features of the Commission proposal. The organisational and procurement implications described below are Aruba's interpretation of the direction of travel and should not be read as a statement of final legal requirements.

Capacity and infrastructure

CADA recognises that cloud and AI capability depends on physical infrastructure. Data centres, compute capacity, storage, networking, energy, cooling and connectivity are not secondary considerations.
The Commission has stated an ambition to at least triple EU data-centre capacity within five to seven years, while improving the conditions for sustainable deployment, permitting and integration with the energy system.
For organisations, this means that cloud infrastructure is becoming a **strategic capacity** question, not only a procurement choice.

A common sovereignty framework

CADA proposes four Union Assurance Levels - UAL1 to UAL4 - to assess cloud and AI sovereignty. The framework is intended to apply to individual services rather than being a generic label for an entire provider.

UNION ASSURANCE LEVEL	PLAIN-ENGLISH INTERPRETATION
UAL1	Data is processed and stored on infrastructure located in the Union.
UAL2	The service demonstrates stronger independence from third countries and greater transparency over the software supply chain.
UAL3	The provider is owned and controlled from the EU and meets additional operational conditions, including requirements related to personnel.
UAL4	The provider demonstrates full transparency and effective control over its software supply chain, with no third-country interference.

The framework creates a more granular assessment of the control characteristics of a service: where it runs, who controls it, who operates it, which dependencies matter and how those dependencies can be evidenced.

CADA does not make a service sovereign because it carries a label. It makes the conditions of sovereignty more **visible** - and increasingly based on **evidence**.

Demand and procurement

CADA is likely to make sovereignty increasingly relevant in public-sector cloud selection, particularly for highly critical use cases. The Commission describes the proposal as including a public-sector adoption mechanism based on risk assessment, while maintaining an open market for the large majority of use cases.

Over time, the same questions will become relevant for private organisations in critical sectors, regulated industries and complex enterprise environments:

- **is there excessive concentration risk?**
- **can the provider be audited?**
- **is there a credible exit path?**
- **what is the operational and jurisdictional exposure?**
- **can the service support critical processes during disruption?**

Ecosystem and innovation

CADA connects cloud policy with European innovation, interoperability and open-source capability, strengthening the ecosystem that develops, operates and governs cloud and AI services. This matters because capacity without capability creates another form of dependency.

Europe requires infrastructure, but it also needs the operating skills, security practices, software control, platform services and trusted ecosystems that make infrastructure useful.

CHAPTER 03

Beyond data residency

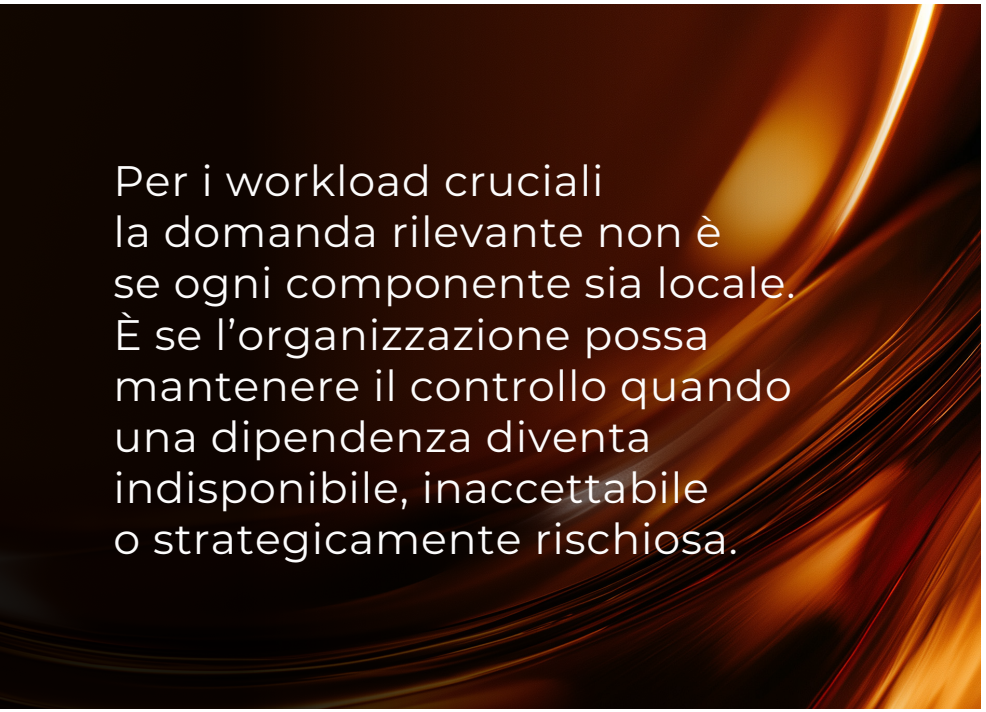
The real meaning of sovereignty

Data residency is often the first question in cloud strategy. Organisations need to know where their data is stored, processed, backed up and recovered. But data residency alone does not establish sovereignty.

A workload may be located in Europe while still depending on a provider controlled elsewhere. Its management plane may be operated from another jurisdiction. Privileged access may be exercised by administrators outside the EU. Critical software components may be updated or maintained through external channels. Incident response may rely on teams beyond European operational control. The workload may be difficult to recover independently or migrate to another environment.

Meaningful sovereignty is the demonstrated ability to **govern**, **operate**, **secure**, **recover** and **evolve** a service without unacceptable external dependency.

CONTROL DIMENSION	THE QUESTION ORGANISATIONS SHOULD ASK
Ownership	Who ultimately owns and controls the provider?
Jurisdiction	Which legal authorities may affect the service or its operator?
Infrastructure	Where are compute, storage, network, backup and recovery resources operated?
Operations	Who administers the service, provides support and responds to incidents?
Software	Who controls updates, remote access, roadmaps and critical dependencies?
Security	Can the provider detect, contain, investigate and evidence cyber events?
Continuity	Can the service remain operational during a disruption or provider failure?
Portability	Can workloads and data be recovered, moved or exited in practice?
Evidence	Can the provider demonstrate these claims through auditable evidence?



For boards and executive teams, these questions translate directly into **continuity** and **accountability**. If a crucial service cannot be independently operated, recovered or moved, the organisation may be carrying a dependency it cannot adequately govern.

Modern cloud environments depend on international hardware, software, open-source components, specialist services and complex supply chains. Sovereignty does not require an isolated technology estate. Organisations should distinguish between controllable dependencies, governed external dependencies and critical dependencies that cannot be audited, substituted or operated independently.

Aruba groups this capability into five dimensions of **Strategic Control**:

- **jurisdictional control**: where infrastructure operates, who owns and governs it, and which legal authorities can affect it;
- **operational control**: who administers the service, exercises privileged access and responds when conditions deteriorate;
- **data and AI control**: where data, models and workflows run, how access is authorised and how actions are traced;
- **resilience and reversibility**: whether services can be recovered, moved or operated through an independent path;
- **technology and ecosystem control**: whether material software, standards, interfaces and supply-chain dependencies remain visible and governable.

CADA's proposed assurance levels and the European regulatory architecture do not require every component to be European; they require material dependencies to be **understood**, **evidenced** and **proportionate** to workload risk.

CHAPTER 04

Artificial Intelligence makes infrastructure strategic

The AI model is not the whole system

The visible part of AI is the model: the assistant, application, agent or interface that users interact with. But **every AI system depends on a deeper stack of infrastructure, software, data, identity, security and operations**.

That stack includes:

- compute capacity for training and inference;
- CPU and GPU resources;
- data storage and data pipelines;
- model access and orchestration;
- identity, permissions and authentication;
- logging, monitoring and traceability;
- cybersecurity controls;
- backup, resilience and recovery;
- energy and network capacity;
- human administration and support.

The AI Act introduces a risk-based approach to AI, with increasingly stringent obligations for higher-risk systems. Its requirements include risk management, data quality, activity logging, documentation, human oversight, robustness, cybersecurity and accuracy.

But these requirements presume that the infrastructure beneath the AI system can itself be controlled and evidenced.

An organisation cannot establish reliable traceability if the relevant data flows are unclear. It cannot demonstrate robust cybersecurity if model weights, training data and inference pipelines are not protected.

It cannot guarantee human oversight if identities and authority models are weak. It cannot maintain continuity if the AI workload depends on infrastructure that cannot be recovered or moved.

The Commission has positioned the proposed Act as supporting more sovereign, resilient and competitive European AI solutions, while creating better conditions for businesses, researchers and public administrations to invest in AI and cloud technologies.

AI makes infrastructure **strategic** because it amplifies every dependency beneath it.

This creates the **Compute–Compliance Paradox**. Organisations need access to increasingly powerful and specialised compute, yet higher-impact uses also increase the need for jurisdictional clarity, compliance, data protection, traceability, cybersecurity and operational accountability. Treating these objectives as opposites forces an unnecessary choice between capability and control.

The architectural task is to resolve the paradox: combining global model innovation with infrastructure and operating conditions proportionate to the risk of the use case.

This requires more than private infrastructure.
It requires the ability to choose and orchestrate models according to the sensitivity, performance and economics of each use case.
A controlled AI environment may combine private and open-weight models, customer-selected proprietary models and, where appropriate, access to external frontier models without surrendering governance of the underlying data, identities and workflows.

The objective is controlled choice, workload by workload: private and open-weight models where sovereignty or sensitivity requires them, and external frontier models where they provide superior capability-connected through governed routing, identity, logging and policy controls.

Model choice is therefore itself an element of Strategic Control. Organisations should be able to determine which models operate within a controlled European environment, which may be accessed externally and how requests are routed between them.

This preserves access to innovation while reducing unnecessary dependency on any single model or provider.

The more significant the AI use case, the more important the questions become:

- where does the model run?
- where is data processed?
- who can access the environment?
- which third parties control critical components?
- how are actions logged and attributed?
- can the workload be recovered?
- can the organisation move to another environment if required?
- is the AI service deployed on infrastructure proportionate to its risk?

Aruba provides secure, compliant European foundations on which organisations can deploy AI with greater control: compute, cloud, security, identity, trust, connectivity and auditability. Aruba's AI Platform is being developed as a multi-model environment built on Aruba Cloud and operated within Aruba's European data-centre infrastructure. Its architecture is designed to support private and open-weight models, bring-your-own-model deployment, model training and controlled access to external frontier models, allowing organisations to combine AI capability with infrastructure, data and operational control.

Aruba's AI platform is structured across **three connected layers**: European cloud and compute foundations; an enablement layer combining private, open and external models with modular tools, agents and orchestration; and an application layer exposing these capabilities through APIs, vertical solutions, widgets and controlled enterprise assistants.

Above this foundation, orchestration capabilities and modular AI tools can support functions such as knowledge-base access, document processing, OCR, text management, model comparison and automated routing. This allows organisations to use specialised capabilities where appropriate rather than directing every task to a general-purpose model.

The platform's enablement layer extends beyond model access. Modular tools and agents can provide specialised capabilities, connect models to enterprise knowledge and processes, route tasks to the most appropriate model, compare outputs and interact with trusted digital services.

This creates a path from generic model infrastructure to governed, domain-specific AI.

CHAPTER 05

What CADA changes for organisations

From cloud selection to control design

CADA changes the cloud decision from a sourcing exercise into a **control-design exercise**.

Price, performance, scalability, functionality and developer experience will remain central to cloud selection. But for crucial workloads, organisations are increasingly assessing whether they can remain in control of the digital environment over time.

Not every workload requires maximum assurance. Applying the highest sovereignty standard to every application would be costly, unnecessary and potentially counterproductive.

WORKLOAD CATEGORY	PRIMARY CONCERN	APPROPRIATE CLOUD RESPONCE
Standard production workloads	Performance, agility, reliability and cost predictability	A robust production-cloud platform with strong automation and operational quality
Core business processes	Continuity, operational control and evidence	A European operating environment with enhanced governance and resilience
Sensitive or regulated data	Jurisdiction, auditability, identity and security	A higher-assurance service profile with transparent operations
Critical recovery environments	Independence, resilience and exit	An independent cloud environment for backup, DR and cyber recovery
Sensitive AI workloads	Controlled compute, data governance and traceability	Secure AI infrastructure with strong identity, logging and operational control

For sensitive AI workloads, the required control profile may extend beyond infrastructure location. It may include model selection, routing policies, protection of prompts and knowledge bases, tool permissions, agent behaviour and the ability to evidence which model or component performed a particular action. Organisations should begin by asking:

- which processes would materially disrupt the business if unavailable?
- which data requires stronger jurisdictional, legal or security control?
- which systems support regulatory, financial, healthcare, public-sector or critical-infrastructure obligations?
- which applications cannot be recovered effectively if the primary provider becomes unavailable?
- which AI use cases make consequential decisions, access sensitive information or connect to core systems?
- which services depend on technology components that the organisation cannot meaningfully audit or replace?

The issue therefore is not so much about sovereignty but more about assessing which workloads require which level of control.

Organisations can begin with a six-stage **Strategic Control Assessment**:

1. classify the processes, data and AI use cases whose failure, exposure or loss of control would create material consequences.

2. map infrastructure, software, identity, operational, contractual and jurisdictional dependencies.

3. set the control profile required for each workload rather than applying a single sovereignty label to the provider or estate.

4. design the target architecture, including where a European primary environment, hybrid deployment, controlled AI environment or independent recovery platfor is justified.

5. test resilience and reversibility through recovery exercises, portable artefacts, compatible target environments and executable exit runbooks.

6. maintain evidence so that operating locations, access, dependencies, security events and recovery readiness can be demonstrated over time.

In this environment, strategic control becomes valuable because it reduces uncertainty. It makes critical systems more resilient, procurement more informed, audits more efficient and AI adoption more governable.

CHAPTER 06

The new value of the independent cloud

Resilience, recovery and credible exit

CADA reinforces an important shift in cloud strategy: resilience increasingly requires **independence**.
For many organisations, the question is not whether to replace a hyperscaler. Global cloud platforms will remain important for specialist applications, platform services, developer ecosystems and large-scale innovation. The more relevant question is whether the organisation is too dependent on one provider, one geography, one control plane or one technical ecosystem.

An independent cloud environment can support:

- backup and data replication
- cyber recovery;
- disaster recovery;
- critical application recovery;
- data sovereignty;
- regulated landing zones;
- portability and repatriation;
- exit planning;
- separate operational failure domains;
- selected production workloads.

This should not be framed as "second cloud" in a subordinate sense. It is better understood as a control environment: a separate platform that gives the organisation more options when resilience, recovery or strategic independence are required.

A second copy of data is not necessarily an independent recovery capability. Backup, recovery, administration and production may remain tied to the same provider, management plane, privileged-access path, jurisdiction or critical technology dependency.

In that case, the organisation has redundancy but may still retain a single point of strategic failure. Independence must be designed into architecture, operations, identity and recovery testing.

An independent cloud control environment should be assessed against four questions:

CONTROL QUESTION	WHAT IT MEANS IN PRACTICE
Is it operationally separate?	Recovery can be administered and activated without relying on the same control plane or privileged access path as the primary environment.
Is it jurisdictionally distinct where required?	The recovery environment has a defined European operating model appropriate to the workload's legal and governance needs.
Is it technically recoverable?	Data, configurations, identities and application dependencies can be restored through tested runbooks, not only through contractual promises.
Is it commercially credible as an exit path?	The organisation has a viable destination, resources, process and time frame to move or restart crucial workloads if needed.

An independent cloud control environment becomes a resilience instrument for boards and executive teams. It helps reduce concentration risk, supports business-continuity planning, strengthens cyber recovery and turns exit provisions from theoretical rights into operational options.

Aruba can play three complementary roles:

- a primary production-cloud provider for workloads well suited to its platform;
- a European control layer alongside global cloud providers;
- an independent recovery, portability and exit environment for organisations seeking to reduce concentration risk.

The same platform can be consumed at different levels: as infrastructure and compute, through APIs and model-as-a-service capabilities, or through configured enterprise assistants, widgets and vertical applications.

Multi-cloud is not simply the use of several providers. It is the deliberate design of independence where independence has business value.

For regulated organisations, this is relevant to the accountability principles already reinforced by NIS2 and DORA: reliance on third parties does not remove the organisation's responsibility for continuity, security or operational oversight.

The strategic value of an independent cloud lies in helping turn that continuing responsibility into a recoverable operating model.

CHAPTER 07

The Sovereign Core Architecture

Aruba for crucial workloads

Most organisations need something achievable and useful: a **Sovereign Core Architecture** for the workloads that matter most. It is the set of infrastructure, operating, security, trust and recovery conditions that allow a crucial workload to remain governable under normal conditions and under stress.

The workload may still connect to global applications, partners, models or ecosystems. But the organisation must be able to establish who operates it, where it runs, how it is protected, how its dependencies are governed and how it can be recovered or moved if circumstances demand.

It is the ability to establish a credible level of control over crucial processes, sensitive data, regulated services, trusted transactions and AI environments. For these workloads, a viable Sovereign Core Architecture should include:

- infrastructure operated within a European framework;
- clear accountability for cloud operations;
- security operations able to detect, respond and provide evidence;
- resilience, recovery and business-continuity capability;
- identity and access controls;
- trusted digital transaction services;
- visibility over critical software and operational dependencies;
- transparent data and support arrangements;
- a credible route to portability and exit;
- cloud and compute capability suitable for controlled AI deployment;
- model choice, orchestration and controlled access to private, open and external AI capabilities.

Aruba brings together European cloud and data-centre infrastructure, cybersecurity operations, connectivity, digital identity and qualified trust services within an integrated operating model. Through its qualified trust providers, Actalis and ArubaPEC, Aruba also provides services such as electronic signatures, timestamps, certified electronic delivery and digital identity capabilities,

important elements where cloud services intersect with trusted and legally significant digital processes.

CRUCIAL WORKLOAD REQUIREMENT	ARUBA FOUNDATION
European cloud infrastructure	Cloud and proprietary data-centre capability operated within a European framework
Operational accountability	An integrated provider model with clear responsibility for core service layers
Cybersecurity	SOC operations, managed detection and response, security services and monitoring
Resilience	Datacenter, connectivity, recovery and operational-continuity capabilities
Identity and trust	Qualified trust services, digital identity, signatures, timestamps and trusted delivery
AI control	European cloud and compute foundations, multi-model deployment, orchestration and modular AI tools for controlled AI use
Evidence	Architecture, operational documentation, logging and audit-supporting controls
Portability and exit	Hybrid, multi-cloud, migration, recovery and independent-environment approaches

Aruba can extend the platform through an ecosystem of domain partners whose expertise, data and workflow knowledge can be embedded into specialised tools and agents. This creates vertical solutions that combine Aruba's infrastructure and controls with recognised sector or functional expertise.

Aruba can support the control foundation with evidence drawn from operating capabilities rather than from sovereignty claims alone. Examples include ACN QC3-qualified Hosted Private Cloud and Virtual Private Cloud services for eligible Italian public-sector use cases; ArubaKube's contribution to Liqo for open, multi-cluster and multi-provider orchestration; participation in European interoperability initiatives such as SECA and Gaia-X; qualified trust services through Actalis and ArubaPEC; and cloud, data-centre, connectivity, recovery and cybersecurity operations delivered within the Aruba group.
The applicability of each proof point depends on the selected service, sector and contract and must be validated during solution design. No current capability should be presented as having achieved a specific CADA assurance level before the final framework and its audit arrangements apply.

Aruba's integrated operating model is designed to reduce the coordination burden across these layers. It enables organisations to place selected workloads on a European foundation where operational control, security, trust and resilience can be treated as connected capabilities rather than separate procurement categories.

Aruba's differentiation lies in combining **European infrastructure**, **cloud**, **compute**, **security**, **identity**, **trusted services** and **AI enablement** in a modular full-stack model. Customers can adopt the complete architecture or use individual layers - compute, models, tools, APIs, applications or recovery capabilities - according to their needs.

In AI, this integrated model extends from the physical and cloud foundations to the

enablement layer above them. Models, specialised tools and agentic capabilities can be exposed through APIs or assembled into controlled applications, corporate assistants and vertical services, while maintaining a clearer line of accountability across infrastructure, data, identity and operations.

ENABLE

Establish European-native foundations across infrastructure, cloud, connectivity, trust and security.

ENHANCE

Combine managed and orchestrated services to reduce fragmentation and clarify accountability.

EMPOWER

Co-design the control profile and architecture for specific crucial workloads, recovery requirements and AI use cases.

EVOLVE

Use open standards, portability and participation in European ecosystems to preserve future choice as regulation and technology change.

For crucial workloads, **Aruba provides European operating foundations and enables strategic control and future choice.**

CHAPTER 08

From compliance to strategic control

One European control architecture

CADA does not stand alone. It connects to the European regulatory architecture already shaping how organisations design digital systems.

Identity makes actions attributable.
Security protects the environment.
Resilience keeps services operational.
AI governance manages automated decision-making.

CADA adds the capacity and sovereignty layer beneath them all.

FRAMEWORK	CENTRAL QUESTION	STRATEGIC CONTROL REQUIREMENT
eIDAS 2.0	Can the organisation prove who acted and whether a digital transaction can be trusted?	Digital identity, qualified trust services and verifiable transactions
NIS2	Can the organisation manage and demonstrate cybersecurity risk?	Security operations, incident response and evidence
DORA	Can critical financial services continue under disruption?	Resilience, third-party governance, recovery and exit capability
AI Act	Can AI systems be operated safely, transparently and accountably?	Traceability, security, human oversight and controlled infrastructure
CADA	Does Europe have the cloud and AI capacity to support critical workloads with appropriate sovereignty?	European infrastructure, operational control and service-level assurance

Infrastructure, cloud, cybersecurity, identity, trust and connectivity are not separate conversations. For crucial workloads, they are parts of the same operating model.

The same underlying identity, security, resilience and evidence capabilities may contribute to several regulatory and operational requirements, subject to the organisation's role, sector, implementation and legal assessment.

A qualified identity layer can support trusted transactions and attributable AI workflows. Security operations can contribute evidence relevant to NIS2, DORA and AI protection. Resilient European infrastructure can support continuity, sovereignty and cloud assurance. Strategic Control does not guarantee compliance; it makes overlapping obligations more operable as a shared architectural problem.

CADA gives this proposition new relevance. It shifts the European conversation from compliance with individual rules toward the capacity to operate a **trusted** digital economy in practice.

aruba.it

CONCLUSIONS

Europe's Cloud Future: Global Collaboration, while preserving Strategic Control.

Europe's cloud trends are not about withdrawing from global technology, but rather about recognising that certain processes, data and AI-enabled services are too important to operate on foundations that organisations cannot sufficiently understand, govern, recover or replace.

CADA signals a shift from rules to capacity: from defining what trusted digital systems should look like to ensuring that Europe can build and operate the infrastructure on which those systems depend.

For organisations, the response should be practical:

- identify crucial workloads and sensitive data;
- map cloud, software and operational dependencies;
- assess concentration and jurisdictional risk;
- match assurance levels to workload criticality;
- build credible recovery and exit capability;
- demand operational evidence, not only contractual assurances;
- use independent European infrastructure where control matters most.

Aruba's role is to make that shift practical. Not by promising sovereignty for every workload, and not by treating sovereignty as a label. But by enabling strategic control through time, by providing a Sovereign Core Architecture for the workloads where control is strategic: European infrastructure, accountable operations, cybersecurity, trust, resilience and evidence in one integrated model.

The future value of cloud will depend not only on what it can do, but on whether organisations can remain in **control** of what it does.

About Aruba

Aruba, founded in 1994, is Italy's Cloud Champion and one of Europe's leading providers of digital infrastructures and platforms based on proprietary assets. The company designs and manages the entire technology stack: from the design and construction of data centers to cloud platforms, from trust and cybersecurity services to connectivity and software solutions that support digital strategies and AI-based applications.

With entirely Italian capital, Aruba serves 16 million users from over 100 countries and operates an infrastructure distributed across 8 data centers, hosting thousands of customers' IT infrastructures.

Copyright © Aruba. All rights reserved.
Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it