



Il CADA europeo, l'AI e il controllo strategico

Il quadro europeo di controllo strategico per Cloud e AI.

INTRODUZIONE

Da più di un decennio l'Unione Europea costruisce un'architettura normativa per sistemi digitali affidabili. **eIDAS 2.0** rafforza l'identità digitale e i servizi fiduciari. **NIS2** alza la soglia minima di cybersecurity. **DORA** impone la resilienza operativa nei servizi finanziari. L'**AI Act** stabilisce obblighi per un uso sicuro, trasparente e responsabile dell'AI.

Insieme, questi quadri normativi affermano un principio chiaro: i sistemi digitali devono essere sicuri, resilienti, tracciabili e governabili by design.

Man mano che le organizzazioni portano nel cloud processi core, dati sensibili, servizi critici e workflow abilitati dall'Intelligenza Artificiale, la domanda strategica non è più come questi sistemi siano regolati. È se l'infrastruttura che li sostiene possa essere controllata, protetta, documentata, ripristinata e fatta evolvere nel tempo.

È questo il contesto della proposta di regolamento **Cloud and AI Development Act (CADA)**.

Il CADA punta a rafforzare l'ecosistema europeo del cloud e dell'AI attraverso investimenti infrastrutturali, sviluppo dei data center, innovazione e un quadro comune di sovranità. Gli Union Assurance Levels proposti introducono un modo più strutturato di valutare i servizi cloud e AI in base a dove operano, a chi li controlla, a come sono governate le loro dipendenze software e a quanto sono esposti a interferenze di paesi terzi.

Per le organizzazioni il CADA cambia la decisione sul cloud. La residenza del dato resta importante, ma non è più sufficiente. I workload cruciali richiedono una valutazione di proprietà, giurisdizione, controllo operativo, cybersecurity, catene di fornitura del software, ripristino, portabilità e verificabilità.

Non tutti i workload richiedono lo stesso grado di autonomia, e nessuna organizzazione deve sostituire gli ecosistemi cloud globali. Serve però una base europea credibile per i workload che non ci si può permettere di lasciare a una dipendenza non esaminata.

In Aruba forniamo una **Sovereign Core Architecture** per i processi core, i dati sensibili, i workload regolamentati, i servizi digitali cruciali e gli ambienti AI controllati.

Significa mettere insieme i livelli di controllo che contano di più:

- infrastruttura e operations cloud europee;
- responsabilità operativa chiara;
- cybersecurity e resilienza;
- identità digitale e servizi fiduciari qualificati;
- connettività e controllo dei dati;
- verificabilità ed evidenze;
- portabilità, ripristino e capacità di uscita;
- compute pronto per l'AI e opzioni di deployment controllato.

Una Sovereign Core Architecture non significa costruire un patrimonio tecnologico isolato né richiedere che ogni componente sia europeo. Stabilisce le condizioni verificabili in cui un workload cruciale resta **conforme, governabile e sotto il vostro controllo**: giurisdizione nota, operations responsabili, dati protetti, accessi controllati, infrastruttura resiliente, dipendenze verificabili e un percorso credibile di ripristino o uscita.

La regolamentazione definisce come devono essere i sistemi digitali affidabili. Il CADA affronta la capacità necessaria per operarli. Il controllo strategico è la capacità di tenere **insieme** le due cose.

Sommario

01 Il momento cloud dell'Europa	5
02 Che cosa porta il CADA	7
03 Oltre la residenza del dato	10
04 L'AI rende strategica l'infrastruttura	12
05 Che cosa cambia il CADA per le organizzazioni	15
06 Il nuovo valore del cloud indipendente	17
07 La Sovereign Core Architecture	19
08 Dalla conformità al controllo strategico	22
09 CONCLUSIONI	23

CAPITOLO 01

Il momento cloud dell'Europa

Dalla regolamentazione digitale alla capacità digitale

La prima fase riguardava le regole. L'Europa ha costruito un quadro completo per garantire che i servizi digitali siano affidabili, sicuri e responsabili.

L'identità deve essere verificabile. Il rischio cyber deve essere gestito. I servizi critici devono restare operativi. L'AI deve essere sviluppata e utilizzata in modo responsabile.

La seconda fase riguarda la capacità. Chiede se l'Europa disponga di infrastrutture cloud, data center, rete e calcolo

per l'AI sufficienti a operare i propri servizi digitali più importanti con un grado adeguato di autonomia e controllo.

La domanda è diventata urgente per tre ragioni.

Primo, **alle infrastrutture e ai servizi cloud è stato chiesto sempre più spesso di gestire applicazioni core, piattaforme per i clienti, ambienti dati, servizi di sicurezza, sistemi di collaborazione e flussi produttivi.**

Il guasto, l'indisponibilità o la perdita di controllo di quei servizi possono incidere sulla continuità dell'organizzazione stessa.

Secondo, **l'AI aumenta l'importanza strategica dell'infrastruttura.** L'AI richiede compute su larga scala, elaborazione dati estesa, networking ad alte prestazioni, storage sicuro, competenze operative specialistiche e molta energia. Sta creando una nuova catena di dipendenze sotto i processi di business e i servizi pubblici: dal modello al dato, dal dato al cloud, dal cloud all'infrastruttura e dall'infrastruttura all'energia e al controllo operativo.

Terzo, **le dipendenze geopolitiche, giuridiche e di filiera sono diventate più visibili.** La domanda non è più solo dove sono conservati i dati. È anche chi controlla il servizio, quali autorità giuridiche possono incidere su di esso,

chi può accedervi o aggiornarlo, che cosa accade se un fornitore critico viene meno e se l'organizzazione è in grado di ripristinare o spostare il workload.

La proposta di CADA risponde a questo contesto. Punta a rafforzare l'ecosistema europeo del cloud e dell'AI a migliorare le condizioni per capacità e investimenti e a creare un quadro europeo per valutare la sovranità di cloud e AI.

Non è un invito all'isolamento tecnologico. L'Europa resterà interconnessa con gli ecosistemi tecnologici globali. Le organizzazioni continueranno a usare fornitori, piattaforme, applicazioni e capacità AI specialistiche diverse. Ma per i workload cruciali la dipendenza non può più essere trattata come un sottoprodotto accidentale dell'adozione del cloud.

Va progettata, gestita e, dove necessario, ridotta.

La scelta infrastrutturale è diventata parte della resilienza, della governance e della strategia operativa di lungo periodo. Un'organizzazione può mantenere le stesse applicazioni e gli stessi servizi cloud e trovarsi comunque con un livello di rischio diverso, a seconda della sua capacità di documentare, ripristinare, proteggere e, se necessario, spostare l'ambiente che li sostiene.



L'Europa sta spostando l'attenzione da come i sistemi digitali debbano comportarsi alla domanda se collettivamente disponiamo dell'infrastruttura, della capacità e del controllo operativo necessari per farli funzionare.

CAPITOLO 02

Che cosa porta il CADA

Capacità, assurance e un nuovo dibattito sul cloud

Il CADA è una **proposta** di regolamento europeo destinata a rafforzare l'ecosistema del cloud e dell'AI in tutta l'Unione Europea.

Il CADA resta una proposta. Il testo finale, le modalità attuative, i criteri di assurance e i tempi possono cambiare nel corso dell'iter legislativo. Ma la direzione strategica è chiara.

L'Europa intende aumentare la capacità cloud e AI sviluppando al tempo stesso un modo più coerente di valutare sovranità e rischio.

Quattro elementi sono importanti. I primi due, capacità e quadro di assurance proposto, sono caratteristiche dirette della proposta della Commissione. Le implicazioni organizzative e di procurement descritte di seguito sono l'interpretazione di Aruba della direzione di marcia e non vanno lette come una descrizione dei requisiti giuridici definitivi.

Capacità e infrastruttura

Il CADA riconosce che la capacità cloud e AI dipende dall'infrastruttura fisica. Data center, capacità di calcolo, storage, networking, energia, raffreddamento e connettività non sono elementi secondari.

La Commissione ha dichiarato l'ambizione di almeno triplicare la capacità dei data center europei entro cinque-sette anni, migliorando al tempo stesso le condizioni per uno sviluppo sostenibile, per le autorizzazioni e per l'integrazione con il sistema energetico.

Per le organizzazioni questo significa che l'infrastruttura cloud diventa una questione di **capacità strategica**, non solo una scelta di procurement.

Un quadro comune di sovranità

Il CADA propone quattro Union Assurance Levels, da UAL1 a UAL4, per valutare la sovranità di cloud e AI. Il quadro è pensato per applicarsi ai singoli servizi e non come etichetta generica per un intero fornitore.

UNION ASSURANCE LEVEL	INTERPRETAZIONE IN LINGUAGGIO SEMPLICE
UAL1	I dati sono elaborati e conservati su infrastruttura situata nell'Unione.
UAL2	Il servizio dimostra una maggiore indipendenza dai paesi terzi e una maggiore trasparenza sulla catena di fornitura del software.
UAL3	Il fornitore è posseduto e controllato dall'UE e soddisfa condizioni operative aggiuntive, inclusi requisiti relativi al personale.
UAL4	Il fornitore dimostra piena trasparenza e controllo effettivo sulla propria catena di fornitura software, senza interferenze di paesi terzi.

Il quadro produce una valutazione più granulare delle caratteristiche di controllo di un servizio: dove gira, chi lo controlla, chi lo opera, quali dipendenze contano e come quelle dipendenze possono essere documentate.

Il CADA non rende sovrano un servizio perché porta un'etichetta. Rende le condizioni della sovranità più **visibili** e sempre più fondate su **evidenze**.



Domanda e procurement

Il CADA renderà probabilmente la sovranità sempre più rilevante nella selezione del cloud nel settore pubblico, in particolare per i casi d'uso altamente critici.

La Commissione descrive la proposta come comprensiva di un meccanismo di adozione per il settore pubblico basato sulla valutazione del rischio, mantenendo al contempo un mercato aperto per la grande maggioranza dei casi d'uso.

Nel tempo le stesse domande diventeranno rilevanti per le organizzazioni private nei settori critici, nelle industrie regolamentate e negli ambienti enterprise complessi:

- **esiste un rischio eccessivo di concentrazione?**
- **il fornitore può essere sottoposto ad audit?**
- **esiste un percorso di uscita credibile?**
- **qual è l'esposizione operativa e giurisdizionale?**
- **il servizio può sostenere i processi critici durante un'interruzione?**

Ecosistema e innovazione

Il CADA collega la politica sul cloud all'innovazione europea, all'interoperabilità e alle capacità open source, rafforzando l'ecosistema che sviluppa, opera e governa i servizi cloud e AI. Questo conta perché la capacità senza competenza crea un'altra forma di dipendenza. All'Europa serve infrastruttura, ma servono anche competenze operative, pratiche di sicurezza, controllo del software, servizi di piattaforma ed ecosistemi affidabili che rendano utile quell'infrastruttura.

CAPITOLO 03

Oltre la residenza del dato

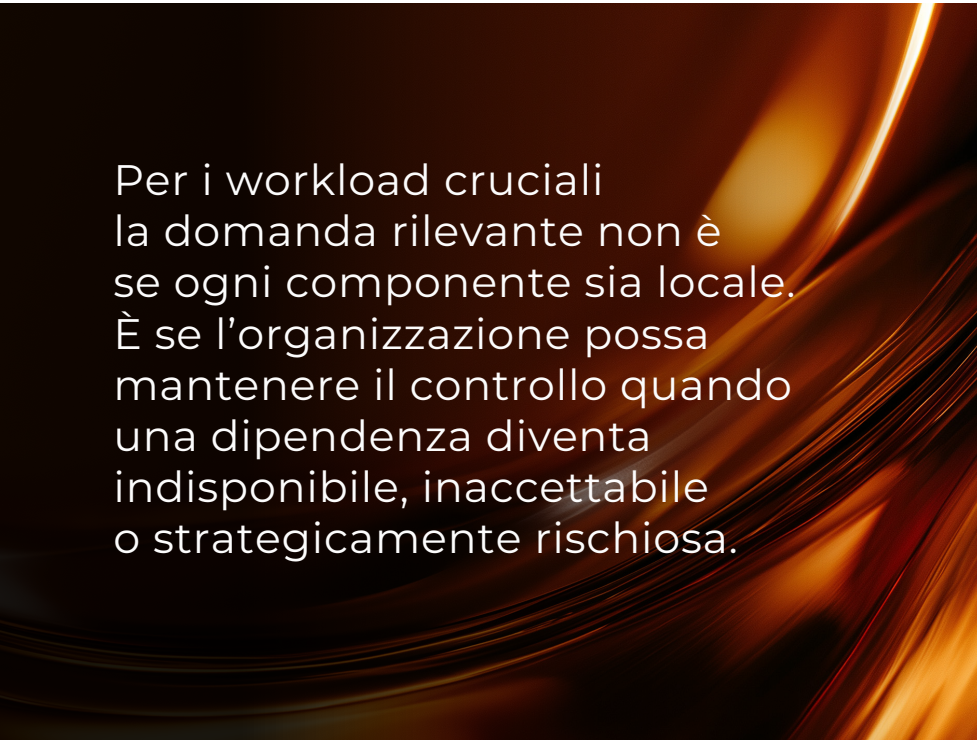
Il significato reale della sovranità

La residenza del dato è spesso la prima domanda della strategia cloud. Le organizzazioni devono sapere dove i loro dati sono conservati, elaborati, salvati e ripristinati. Ma la sola residenza del dato non stabilisce la sovranità.

Un workload può trovarsi in Europa e dipendere comunque da un fornitore controllato altrove. Il suo management plane può essere operato da un'altra giurisdizione. Gli accessi privilegiati possono essere esercitati da amministratori fuori dall'UE. Componenti software critici possono essere aggiornati o mantenuti attraverso canali esterni. La risposta agli incidenti può dipendere da team fuori dal controllo operativo europeo. Il workload può essere difficile da ripristinare in autonomia o da migrare verso un altro ambiente.

La sovranità in senso sostanziale è la capacità dimostrata di **governare, operare, proteggere, ripristinare** e far **evolvere** un servizio senza dipendenze esterne inaccettabili.

DIMENSIONE DI CONTROLLO	LA DOMANDA CHE LE ORGANIZZAZIONI DOVREBBERO PORSI
Proprietà	Chi possiede e controlla in ultima istanza il fornitore?
Giurisdizione	Quali autorità giuridiche possono incidere sul servizio o sul suo operatore?
Infrastruttura	Dove sono operate le risorse di calcolo, storage, rete, backup e ripristino?
Operations	Chi amministra il servizio, fornisce supporto e risponde agli incidenti?
Software	Chi controlla aggiornamenti, accessi remoti, roadmap e dipendenze critiche?
Sicurezza	Il fornitore è in grado di rilevare, contenere, investigare e documentare gli eventi cyber?
Continuità	Il servizio può restare operativo durante un'interruzione o il venir meno di un fornitore?
Portabilità	Workload e dati possono essere ripristinati, spostati o portati fuori nella pratica?
Evidenze	Il fornitore può dimostrare queste affermazioni con evidenze verificabili?



Per i workload cruciali
la domanda rilevante non è
se ogni componente sia locale.
È se l'organizzazione possa
mantenere il controllo quando
una dipendenza diventa
indisponibile, inaccettabile
o strategicamente rischiosa.

Per i consigli di amministrazione e i team esecutivi queste domande si traducono direttamente in **continuità** e **responsabilità**. Se un servizio cruciale non può essere operato, ripristinato o spostato in autonomia, l'organizzazione porta una dipendenza che non è in grado di governare adeguatamente.

Gli ambienti cloud moderni dipendono da hardware, software, componenti open source, servizi specialistici e filiere internazionali complesse. La sovranità non richiede un patrimonio tecnologico isolato. Le organizzazioni devono distinguere tra dipendenze controllabili, dipendenze esterne governate e dipendenze critiche che non possono essere sottoposte ad audit, sostituite o operate in autonomia.

Aruba raggruppa questa capacità in cinque dimensioni del **Controllo Strategico**:

- **controllo giurisdizionale** - dove opera l'infrastruttura, chi la possiede e la governa e quali autorità giuridiche possono incidere su di essa;
- **controllo operativo** - chi amministra il servizio, esercita gli accessi privilegiati e risponde quando le condizioni si deteriorano;
- **controllo su dati e AI** - dove girano dati, modelli e workflow, come sono autorizzati gli accessi e come sono tracciate le azioni;
- **resilienza e reversibilità** - se i servizi possono essere ripristinati, spostati o operati attraverso un percorso indipendente;
- **controllo su tecnologia ed ecosistema** - se le dipendenze rilevanti di software, standard, interfacce e filiera restano visibili e governabili.

I livelli di assurance proposti dal CADA e l'architettura normativa europea non richiedono che ogni componente sia europeo: richiedono che le dipendenze rilevanti siano **comprese, documentate e proporzionate** al rischio del workload.

CAPITOLO 04

L'AI rende strategica l'infrastruttura

Il modello di AI non è l'intero sistema

La parte visibile dell'AI è il modello: l'assistente, l'applicazione, l'agente o l'interfaccia con cui gli utenti interagiscono. Ma **ogni sistema di AI dipende da uno stack più profondo di infrastruttura, software, dati, identità, sicurezza e operations**. Quello stack comprende:

- capacità di calcolo per training e inferenza;
- risorse CPU e GPU;
- storage e pipeline di dati;
- accesso ai modelli e orchestrazione;
- identità, permessi e autenticazione;

- logging, monitoraggio e tracciabilità;
- controlli di cybersecurity;
- backup, resilienza e ripristino;
- capacità energetica e di rete;
- amministrazione e supporto umani.

L'AI Act introduce un approccio basato sul rischio, con obblighi via via più stringenti per i sistemi a rischio più elevato. I suoi requisiti comprendono gestione del rischio, qualità dei dati, registrazione delle attività, documentazione, supervisione umana, robustezza, cybersecurity e accuratezza.

Ma questi requisiti presuppongono che l'infrastruttura sottostante al sistema di AI possa essere a sua volta **controllata e documentata**.

Un'organizzazione non può stabilire una tracciabilità affidabile se i flussi di dati non sono chiari. Non può dimostrare una cybersecurity robusta se i pesi dei modelli, i dati di training e le pipeline di inferenza non sono protetti. Non può garantire la supervisione umana se identità e modelli di autorizzazione sono deboli. Non può mantenere la continuità se il workload AI dipende da un'infrastruttura che non può essere ripristinata o spostata.

La Commissione ha presentato la proposta come un sostegno a soluzioni di AI europee più sovrane, resilienti e competitive, creando al tempo stesso condizioni migliori perché imprese, ricercatori e pubbliche amministrazioni investano in tecnologie AI e cloud.

L'AI rende **strategica** l'infrastruttura perché amplifica ogni dipendenza sottostante.

Nasce così il **Paradosso Compute-Compliance**. Le organizzazioni hanno bisogno di accedere a capacità di calcolo sempre più potenti e specializzate, ma gli usi a maggiore impatto aumentano anche la necessità di chiarezza giurisdizionale, conformità, protezione dei dati, tracciabilità, cybersecurity e responsabilità operativa. Trattare questi obiettivi come opposti impone una scelta non necessaria tra capacità e controllo.

Il compito architetturale è risolvere il paradosso: combinare l'innovazione globale sui modelli con condizioni infrastrutturali e operative proporzionate al rischio del caso d'uso.

Questo richiede più della sola infrastruttura privata. Richiede la capacità di scegliere e orchestrare i modelli in base a sensibilità, prestazioni ed economics di ciascun caso d'uso. Un ambiente AI controllato può combinare modelli privati e open-weight, modelli proprietari scelti dal cliente e, dove opportuno, l'accesso a modelli di frontiera esterni senza rinunciare al governo dei dati, delle identità e dei workflow sottostanti.

L'obiettivo è una scelta controllata, per singolo workload: modelli privati e open-weight dove sovranità o sensibilità

lo richiedono, e modelli di frontiera esterni quando offrono funzionalità o prestazioni superiori, collegati attraverso routing governato, identità, logging e controlli di policy.

La scelta dei modelli è quindi essa stessa un elemento del Controllo Strategico. Le organizzazioni devono poter determinare quali modelli operino all'interno di un ambiente europeo controllato, a quali si acceda dall'esterno e come le richieste vengano instradate tra gli uni e gli altri. Questo preserva l'accesso all'innovazione riducendo la dipendenza non necessaria da un singolo modello o fornitore.

Quanto più significativo è il caso d'uso AI, tanto più contano le domande:

- dove gira il modello?
- dove sono elaborati i dati?
- chi può accedere all'ambiente?
- quali terze parti controllano i componenti critici?
- come sono registrate e attribuite le azioni?
- il workload può essere ripristinato?
- l'organizzazione può spostarsi su un altro ambiente se necessario?
- il servizio AI è distribuito su un'infrastruttura proporzionata al suo rischio?



Aruba fornisce fondamenta europee sicure e conformi su cui le organizzazioni possono distribuire l'AI con maggiore controllo: compute, cloud, sicurezza, identità, trust, connettività e verificabilità. La AI Platform di Aruba è in sviluppo come ambiente multi-modello costruito su Aruba Cloud e operato all'interno dell'infrastruttura europea di data center di Aruba. La sua architettura è progettata per supportare modelli privati e open-weight, deployment bring-your-own-model, training dei modelli e accesso controllato a modelli di frontiera esterni, consentendo alle organizzazioni di unire capacità di AI e controllo su infrastruttura, dati e operations.

L'AI Platform di Aruba è strutturata su **tre livelli connessi**: fondamenta europee di infrastruttura, cloud e calcolo; un livello di abilitazione che combina modelli privati, open ed esterni con strumenti, agenti e funzionalità di orchestrazione modulari; e un livello applicativo che espone queste capacità attraverso API, soluzioni verticali, widget e assistenti aziendali controllati.

Sopra questa base, capacità di orchestrazione e strumenti AI modulari possono supportare funzioni come accesso a knowledge base, elaborazione documentale, OCR, gestione del testo, confronto tra modelli e routing automatico. Questo consente alle organizzazioni di usare capacità specializzate dove opportuno, invece di indirizzare ogni attività a un modello generalista.

Il livello di abilitazione della piattaforma va oltre l'accesso ai modelli. Strumenti e agenti modulari possono fornire capacità specializzate, collegare i modelli alla conoscenza e ai processi aziendali, instradare le attività verso il modello più appropriato, confrontare gli output e interagire con servizi digitali fiduciari. Si crea così un percorso dall'infrastruttura di modelli generica a un'AI governata e specifica per dominio.

CAPITOLO 05

Che cosa cambia il CADA per le organizzazioni

Dalla selezione del cloud alla progettazione del controllo

Il CADA trasforma la decisione sul cloud da esercizio di sourcing a **esercizio di progettazione del controllo**.

Prezzo, prestazioni, scalabilità, funzionalità ed esperienza per gli sviluppatori resteranno centrali nella selezione del cloud. Ma per i workload cruciali le organizzazioni valutano sempre più se potranno mantenere il controllo dell'ambiente digitale nel tempo.

Non tutti i workload richiedono il massimo livello di assurance. Applicare a ogni applicazione lo standard di sovranità più elevato sarebbe costoso, inutile e potenzialmente controproducente.

CATEGORIA DI WORKLOAD	PRIORITÀ PRINCIPALE	RISPOSTA CLOUD APPROPRIATA
Workload di produzione standard	Prestazioni, agilità, affidabilità e prevedibilità dei costi	Una piattaforma cloud di produzione robusta, con forte automazione e qualità operativa
Processi di business core	Continuità, controllo operative ed evidenze	Un ambiente operativo europeo con governance e resilienza rafforzate
Dati sensibili o regolamentati	Giurisdizione, verificabilità, identità e sicurezza	Un profilo di servizio a maggiore assurance, con operations trasparenti
Ambienti di ripristino critici	Indipendenza, resilienza e uscita	Un ambiente cloud indipendente per backup, disaster recovery e cyber recovery
Workload AI sensibili	Compute controllato, governo del dato e tracciabilità	Infrastruttura AI sicura, con identità, logging e controllo operativo solidi

Per i workload AI sensibili il profilo di controllo richiesto può andare oltre la localizzazione dell'infrastruttura. Può comprendere la selezione dei modelli, le politiche di routing, la protezione di prompt e knowledge base, i permessi sugli strumenti, il comportamento degli agenti e la capacità di documentare quale modello o componente abbia compiuto una determinata azione. Le organizzazioni dovrebbero partire da queste domande:

- quali processi comprometterebbero materialmente il business se indisponibili?
- quali dati richiedono un controllo giurisdizionale, legale o di sicurezza più forte?
- quali sistemi sostengono obblighi regolamentari, finanziari, sanitari, di settore pubblico o di infrastruttura critica?
- quali applicazioni non possono essere ripristinate efficacemente se il fornitore primario diventa indisponibile?
- quali casi d'uso AI prendono decisioni rilevanti, accedono a informazioni sensibili o si collegano ai sistemi core?
- quali servizi dipendono da componenti tecnologici che l'organizzazione non è in grado di sottoporre ad audit o di sostituire?

La questione quindi non riguarda tanto la sovranità quanto la valutazione di quali workload richiedano quale livello di controllo.

Le organizzazioni possono partire da un **Assessment del Controllo Strategico in sei fasi**:

- 1. classificare** i processi, i dati e i casi d'uso AI il cui guasto, esposizione o perdita di controllo genererebbe conseguenze rilevanti;
- 2. mappare** le dipendenze infrastrutturali, software, di identità, operative, contrattuali e giurisdizionali;
- 3. definire il profilo di controllo** richiesto per ciascun workload, invece di applicare un'unica etichetta di sovranità al fornitore o all'intero parco applicativo;
- 4. progettare l'architettura target**, indicando dove siano giustificati un ambiente primario europeo, un deployment ibrido, un ambiente AI controllato o una piattaforma di ripristino indipendente;
- 5. testare resilienza e reversibilità** con esercitazioni di ripristino, artefatti portabili, ambienti target compatibili e runbook di uscita eseguibili;
- 6. mantenere le evidenze** perché luoghi di operatività, accessi, dipendenze, eventi di sicurezza e prontezza al ripristino possano essere dimostrati nel tempo.

In questo contesto il controllo strategico diventa prezioso perché riduce l'incertezza.

Rende i sistemi critici più resilienti, il procurement più informato, gli audit più efficienti e l'adozione dell'AI più governabile.

CAPITOLO 06

Il nuovo valore del cloud indipendente

Il CADA europeo, l'AI e il controllo strategico / Il quadro europeo di controllo strategico per Cloud e AI.

Resilienza, ripristino e uscita credibile

Il CADA rafforza un cambiamento importante nella strategia cloud: la resilienza richiede sempre più **indipendenza**.

Per molte organizzazioni la domanda non è se sostituire un hyperscaler. Le piattaforme cloud globali resteranno importanti per applicazioni specialistiche, servizi di piattaforma, ecosistemi di sviluppo e innovazione su larga scala. La domanda più rilevante è se l'organizzazione sia troppo dipendente da un solo fornitore, una sola geografia, un solo control plane o un solo ecosistema tecnologico.

Un ambiente cloud indipendente può supportare:

- backup e replica dei dati
- cyber recovery
- disaster recovery
- ripristino delle applicazioni critiche
- controllo e residenza del dato
- landing zone per ambiti regolamentati
- portabilità e repatriation
- pianificazione dell'uscita
- domini di guasto operativi separati
- workload di produzione selezionati

Non va inteso come un “secondo cloud” in senso subordinato. È piuttosto un ambiente di controllo: una piattaforma separata che offre all’organizzazione più opzioni quando servono resilienza, ripristino o indipendenza strategica.

Una seconda copia dei dati non è necessariamente una capacità di ripristino indipendente. Backup, ripristino, amministrazione e produzione possono restare legati allo stesso fornitore, allo stesso management plane, allo stesso percorso di accesso privilegiato, alla stessa giurisdizione o alla stessa dipendenza tecnologica critica. In quel caso l’organizzazione ha ridondanza ma può conservare un singolo punto di fallimento strategico. L’indipendenza va progettata nell’architettura, nelle operations, nell’identità e nei test di ripristino.

Un ambiente cloud indipendente di controllo va valutato con quattro domande:

DOMANDA DI CONTROLLO	CHE COSA SIGNIFICA NELLA PRATICA
È operativamente separato?	Il ripristino può essere amministrato e attivato senza dipendere dallo stesso control plane o dallo stesso percorso di accesso privilegiato dell’ambiente primario.
È giurisdizionalmente distinto dove serve?	L’ambiente di ripristino ha un modello operativo europeo definito, adeguato alle esigenze legali e di governance del workload.
È tecnicamente ripristinabile?	Dati, configurazioni, identità e dipendenze applicative possono essere ripristinati con runbook testati, non solo con promesse contrattuali.
È commercialmente credibile come percorso di uscita?	L’organizzazione dispone di una destinazione praticabile, di risorse, di un processo e di tempi per spostare o riavviare i workload cruciali se necessario.

Un ambiente cloud indipendente di controllo diventa uno strumento di resilienza per i consigli di amministrazione e i team esecutivi. Contribuisce a ridurre il rischio di concentrazione, sostiene la pianificazione della continuità operativa, rafforza il cyber recovery e trasforma le clausole di uscita da diritti teorici in opzioni operative.

Aruba può svolgere tre ruoli complementari:

- fornitore cloud di produzione primario per i workload adatti alla sua piattaforma
- livello di controllo europeo accanto ai fornitori cloud globali
- ambiente indipendente di ripristino, portabilità e uscita per le organizzazioni che vogliono ridurre il rischio di concentrazione

La stessa piattaforma può essere utilizzata a livelli diversi: come infrastruttura e compute, attraverso API, servizi di accesso ai modelli e capacità model-as-a-service, oppure attraverso assistenti aziendali configurati, widget e applicazioni verticali.

Il multi-cloud non è semplicemente l’uso di più fornitori. È la progettazione deliberata dell’indipendenza dove l’indipendenza ha valore di business.

Per le organizzazioni regolamentate questo è rilevante rispetto ai principi di responsabilità già rafforzati da NIS2 e DORA: affidarsi a terze parti non elimina la responsabilità dell’organizzazione su continuità, sicurezza e supervisione operativa.

Il valore strategico di un cloud indipendente sta nel trasformare quella responsabilità permanente in un modello operativo ripristinabile.

CAPITOLO 07

La Sovereign Core Architecture

Aruba per i workload cruciali

Alla maggior parte delle organizzazioni serve qualcosa di realizzabile e utile: una **Sovereign Core Architecture** per i workload che contano di più. È l'insieme di condizioni infrastrutturali, operative, di sicurezza, di trust e di ripristino che permettono a un workload cruciale di restare governabile in condizioni normali e sotto stress.

Il workload può continuare a collegarsi ad applicazioni, partner, modelli o ecosistemi globali. Ma l'organizzazione deve poter stabilire chi lo opera, dove gira, come è protetto, come sono governate le sue dipendenze e come può essere ripristinato o spostato se le circostanze lo richiedono.

È la capacità di stabilire un livello credibile di controllo su processi cruciali, dati sensibili, servizi regolamentati, transazioni fiduciarie e ambienti AI.

Per questi workload una Sovereign Core Architecture efficace dovrebbe comprendere:

- infrastruttura operata in un quadro europeo;
- responsabilità chiara sulle operations cloud;
- security operations in grado di rilevare, rispondere e fornire evidenze;
- capacità di resilienza, ripristino e continuità operativa;
- controlli di identità e accesso;
- servizi fiduciari per le transazioni digitali;

- visibilità sulle dipendenze software e operative critiche;
- condizioni trasparenti su dati e supporto;
- un percorso credibile di portabilità e uscita;
- capacità cloud e di calcolo adatte a un deployment AI controllato;
- scelta dei modelli, orchestrazione e accesso controllato a capacità AI private, open ed esterne.

Aruba mette insieme infrastruttura cloud e data center europei, security operations, connettività, identità digitale e servizi fiduciari qualificati in un modello operativo integrato. Attraverso i suoi trust provider qualificati, Actalis e ArubaPEC, Aruba fornisce anche servizi come firme elettroniche, marche temporali, recapito

elettronico certificato e identità digitale: elementi importanti dove i servizi cloud incontrano processi digitali fiduciari e giuridicamente rilevanti.

REQUISITO DEL WORKLOAD UFFICIALE	FONDAMENTO ARUBA
Infrastruttura cloud europea	Capacità cloud e data center di proprietà, operati in un quadro europeo
Responsabilità operativa	Un modello di fornitore integrato, con responsabilità chiara sui livelli di servizio core
Cybersecurity	Operatività SOC, managed detection and response, servizi di sicurezza e monitoraggio
Resilienza	Capacità di data center, connettività, ripristino e continuità operativa
Identità e trust	Servizi fiduciari qualificati, identità digitale, firme, marche temporali e recapito certificato
Controllo dell'AI	Fondamenta cloud e di calcolo europee, deployment multi-modello, orchestrazione e strumenti AI modulari per un uso controllato dell'AI
Evidenze	Architettura, documentazione operativa, logging e controlli a support degli audit
Portabilità e uscita	Approcci ibridi, multi-cloud, di migrazione, ripristino e ambiente indipendente

Aruba può estendere la piattaforma attraverso un ecosistema di partner di dominio, la cui competenza, i cui dati e la cui conoscenza dei processi possono essere integrati in strumenti e agenti specializzati. Nascono così soluzioni verticali che uniscono l'infrastruttura e i controlli di Aruba a competenze settoriali o funzionali riconosciute.

Aruba può sostenere questa base di controllo con evidenze che derivano da capacità operative e non da sole dichiarazioni di sovranità. Alcuni esempi: i servizi Hosted Private Cloud e Virtual Private Cloud qualificati ACN QC3 per i casi d'uso ammissibili della pubblica amministrazione italiana; il contributo di ArubaKube a Liqo per l'orchestrazione aperta, multi-cluster e multi-provider; la partecipazione a iniziative europee di interoperabilità come SECA e Gaia-X; i servizi fiduciari qualificati attraverso Actalis e ArubaPEC; le operations di cloud, data center, connettività, ripristino e cybersecurity erogate all'interno del gruppo Aruba. L'applicabilità di ciascun proof point dipende dal servizio, dal settore e dal contratto e va validata in fase di progettazione della soluzione. Nessuna capacità attuale va presentata come già conforme a uno specifico livello di assurance CADA prima che il quadro definitivo e le relative modalità di audit siano applicabili.

Il modello operativo integrato di Aruba è pensato per ridurre l'onere di coordinamento tra questi livelli. Consente alle organizzazioni di collocare workload selezionati su una base europea dove controllo operativo, sicurezza, trust e resilienza sono capacità connesse e non categorie di acquisto separate.

La differenziazione di Aruba consiste nel combinare **infrastruttura europea, cloud, compute, sicurezza, identità, servizi fiduciari** e **abilitazione all'AI** in un modello full-stack modulare.

I clienti possono adottare l'architettura completa oppure, in base alle proprie esigenze, utilizzare i singoli livelli: compute, modelli, strumenti, API, applicazioni o capacità di ripristino.

Nell'AI questo modello integrato si estende dalle fondamenta fisiche e cloud al livello di abilitazione che vi si appoggia.

Modelli, strumenti specializzati e capacità agentiche possono essere esposti tramite API o assemblati in applicazioni controllate, assistenti aziendali e servizi verticali, mantenendo una linea di responsabilità più chiara su infrastruttura, dati, identità e operations.

ENABLE

Costruire fondamenta europee native su infrastruttura, cloud, connettività, trust e sicurezza

ENHANCE

Combinare servizi gestiti e orchestrati per ridurre la frammentazione e chiarire le responsabilità

EMPOWER

Progettare insieme il profilo di controllo e l'architettura per specifici workload cruciali, requisiti di ripristino e casi d'uso AI

EVOLVE

Usare standard aperti, portabilità e partecipazione agli ecosistemi europei per preservare la libertà di scelta futura mentre normativa e tecnologia cambiano

Per i workload cruciali, **Aruba fornisce fondamenta operative europee e abilita il controllo strategico e la libertà di scelta futura.**



CAPITOLO 08

Dalla conformità al controllo strategico

Un'unica architettura europea di controllo

Il CADA non è isolato. Si collega all'architettura normativa europea che già plasma il modo in cui le organizzazioni progettano i sistemi digitali.

L'**identità** rende le azioni attribuibili. La **sicurezza** protegge l'ambiente. La **resilienza** mantiene operativi i servizi. La **governance** dell'AI presidia le decisioni automatiche.

Il **CADA** aggiunge sotto tutto questo il livello di capacità e sovranità.

QUADRO NORMATIVO	DOMANDA CENTRALE	REQUISITO DI CONTROLLO STRATEGICO
eIDAS 2.0	L'organizzazione può dimostrare chi ha agito e se una transazione digitale è affidabile?	Identità digitale, servizi fiduciari qualificati e transazioni verificabili
NIS2	L'organizzazione può gestire e dimostrare il rischio cyber?	Security operations, risposta agli incidenti ed evidenze
DORA	I servizi finanziari critici possono continuare durante un'interruzione?	Resilienza, governo delle terze parti, ripristino e capacità di uscita
AI Act	I sistemi di AI possono essere operati in modo sicuro, trasparente e responsabile?	Tracciabilità, sicurezza, supervisione umana e infrastruttura controllata
CADA	L'Europa ha la capacità cloud e AI per sostenere i workload critici con un'adeguata sovranità?	Infrastruttura europea, controllo operative e assurance sui livelli di servizio

Infrastruttura, cloud, cybersecurity, identità, trust e connettività non sono conversazioni separate. Per i workload cruciali sono parti dello stesso modello operativo.

Le stesse capacità di identità, sicurezza, resilienza ed evidenza possono contribuire a più requisiti regolamentari e operativi, a seconda del ruolo dell'organizzazione, del settore, dell'implementazione e della valutazione legale.

Un livello di identità qualificata può sostenere transazioni fiduciarie e workflow AI attribuibili. Le security operations possono fornire evidenze rilevanti per NIS2, DORA e la protezione dell'AI. Un'infrastruttura europea resiliente può sostenere continuità, autonomia digitale e assurance del cloud. Il Controllo Strategico non garantisce la conformità: rende gli obblighi sovrapposti più governabili come unico problema architetturale.

Il CADA dà nuova rilevanza a questa proposta. Sposta la conversazione europea dalla conformità alle singole regole alla capacità di far funzionare nella pratica un'economia digitale **affidabile**.



CONCLUSIONI

Il futuro cloud dell'Europa: collaborazione globale, preservando il controllo strategico.

Le tendenze cloud europee non riguardano il ritiro dalla tecnologia globale, ma il riconoscimento che alcuni processi, dati e servizi abilitati dall'AI sono troppo importanti per essere operati su fondamenta che le organizzazioni non riescono a comprendere, governare, ripristinare o sostituire a sufficienza.

Il CADA segnala un passaggio dalle regole alla capacità: dal definire come devono essere i sistemi digitali affidabili al garantire che l'Europa sappia costruire e operare l'infrastruttura da cui quei sistemi dipendono. Per le organizzazioni la risposta deve essere pratica:

- identificare i workload cruciali e i dati sensibili;
- mappare le dipendenze cloud, software e operative;
- valutare il rischio di concentrazione e quello giurisdizionale;
- allineare i livelli di assurance alla criticità dei workload;
- costruire capacità credibili di ripristino e uscita;
- pretendere evidenze operative, non solo garanzie contrattuali;
- usare infrastruttura europea indipendente dove il controllo conta di più.

Il ruolo di Aruba è rendere pratico questo passaggio. Non promettendo sovranità per ogni workload e non trattando la sovranità come un'etichetta, ma abilitando nel tempo il controllo strategico e fornendo una Sovereign Core Architecture per i workload dove il controllo è strategico: infrastruttura europea, operations responsabili, cybersecurity, trust, resilienza ed evidenze in un unico modello integrato.

Il valore futuro del cloud dipenderà non solo da ciò che il cloud sa fare, ma dalla capacità delle organizzazioni di restare in **controllo** di ciò che fa.

About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce una infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.



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