
Oltre la Compliance

Lo Strategic Control Stack di Aruba per affrontare eIDAS 2.0, NIS2, DORA e AI Act.

aruba.it

puise

Sommario

01 Il controllo digitale: la nuova priorità europea	4
02 Le difficoltà reali che le organizzazioni stanno affrontando	6
03 Quattro risposte a un unico problema di controllo	7
04 Il posizionamento distintivo di Aruba: CSP + QTSP in Europa	10
05 eIDAS 2.0: l'identità digitale come infrastruttura di fiducia	14
06 NIS2: la cybersecurity come baseline strutturale	16
07 DORA: la resilienza operativa come principio di progettazione	18
08 AI Act: la governance come prerequisito infrastrutturale	20
09 Il framework di acquisto	23
10 Oltre la compliance, verso il controllo	26

PARTE I

L'architettura del controllo

CAPITOLO 01

Il controllo digitale: la nuova priorità europea

Per anni il progresso è stato misurato principalmente in termini di velocità, scala ed efficienza. Oggi non è più sufficiente: l'economia digitale europea sta entrando in una nuova fase. Mentre le organizzazioni operano attraverso ambienti cloud, fornitori esterni, sistemi di identità digitale e processi abilitati dall'intelligenza artificiale, la sfida centrale non riguarda più soltanto la digitalizzazione, è il mantenimento del controllo nel tempo che garantisce che i sistemi restino affidabili, resilienti e governabili.

Chi governa le fondamenta digitali?

In questo contesto eIDAS 2.0, NIS2, DORA e AI Act assumono un ruolo strategico. Non si tratta, infatti, di regolamenti isolati, ma di framework che rientrano in un più ampio sforzo europeo per garantire che i sistemi digitali siano affidabili, che i servizi essenziali restino operativi, che i rischi cyber siano governati e che l'AI venga adottata in modo responsabile.

La regolamentazione è strutturale, non opzionale. La domanda centrale non è quanto velocemente le organizzazioni innovino, ma se rimangono in possesso del controllo dei sistemi che abilitano quell'innovazione.

Il filo conduttore di queste normative non è la compliance fine a sé stessa, infatti, ma il controllo: ogni regolamento affronta un diverso livello dello stesso problema, ma tutti convergono nella stessa direzione.

La compliance deve essere integrata fin dalla progettazione, non aggiunta successivamente come strumento.

eIDAS 2.0 riguarda l'identità digitale fiduciaria. DORA riguarda la resilienza operativa nel settore finanziario. AI Act disciplina la governance dell'Intelligenza Artificiale. NIS2 stabilisce la baseline di cybersecurity.

Considerati nel loro insieme, formano un framework coerente per la realizzazione di sistemi digitali affidabili, resilienti e tracciabili.

Considerati nel loro insieme, i regolamenti stanno ridefinendo anche i processi di acquisto. La conformità sta diventando un criterio sempre più determinante nelle gare e nelle selezioni europee, soprattutto nei contesti in cui identità digitale, resilienza, auditabilità e sovranità infrastrutturale devono essere dimostrate in modo integrato.

Per gli uffici acquisti questa non è più una considerazione di back-office, è la progettazione stessa della decisione di acquisto.



CAPITOLO 02

Le difficoltà reali che le organizzazioni stanno affrontando

La maggior parte delle organizzazioni non ha progettato i propri ambienti digitali come sistemi coerenti. Infrastrutture, identità, cybersecurity e meccanismi di fiducia si sono evoluti separatamente, spesso su fornitori e geografie differenti. Il risultato è una progressiva perdita di visibilità e controllo.

Le sei pressioni strutturali

- **Frammentazione infrastrutturale:** componenti tecnologiche adottate separatamente, senza un disegno architetturale orientato a resilienza e auditabilità.
- **Crescente dipendenza da terze parti:** rischio di concentrazione, esposizione alla supply chain digitale, oneri legati alla verifica della conformità dei fornitori.
- **Proliferazione delle identità:** modelli di identità differenti tra utenti, sistemi, API e agenti AI.

- **Lacune nella tracciabilità:** difficoltà nel dimostrare chi ha fatto cosa, quando e in quale contesto operativo, attraverso gli ecosistemi.
- **Responsabilità a livello di board:** la gestione del rischio richiede oggi evidenze architetturali, non assicurazioni di policy.
- **Ritardo nella governance dell'AI:** amplifica il rischio in assenza di fondamenta digitali affidabili.

Molti processi critici dipendono oggi da sistemi che le organizzazioni non possiedono interamente, non governano completamente e spesso non sono in grado di verificare in modo esaustivo. Dimostrare accountability, di conseguenza, diventa sempre più complesso, soprattutto all'interno di ambienti ibridi, supply chain digitali articolate e workflow automatizzati. Emerge una sfida fondamentale per le organizzazioni: **come mantenere la governance in sistemi che non controllano interamente?**

Autorità regolatorie, clienti e consigli di amministrazione non si accontentano più di sistemi che semplicemente funzionano, richiedono alle organizzazioni la capacità di dimostrare chi ha operato, con quale autorizzazione, su quali infrastrutture e con quali misure di protezione. Recuperare questo livello di controllo, la capacità di operare, adattarsi ed evolvere senza dipendenze, sta diventando una necessità strategica.

In Aruba, chiamiamo questo approccio “controllo strategico”: la capacità di governare, adattare ed evolvere l'intero stack digitale, mantenendo il controllo e l'autonomia su infrastrutture, dati e processi decisionali.

Un simile risultato non si ottiene introducendo nuovi strumenti o policy, ma richiede un approccio architetturale che parte dai sistemi progettati per integrare nativamente fiducia, resilienza, tracciabilità e accountability.

CAPITOLO 03

Quattro risposte a un unico problema di controllo

Considerati nel loro insieme, eIDAS 2.0, NIS2, DORA e AI Act possono essere letti come quattro risposte coordinate alla stessa sfida strutturale: garantire che i sistemi digitali restino governabili anche in un contesto sempre più complesso, distribuito e automatizzato.

In questo contesto, **l'identità digitale non è più soltanto un meccanismo di accesso. È un'infrastruttura della fiducia**, che consente alle organizzazioni di dimostrare chi ha agito, con quale livello di autorizzazione e con quali garanzie legali e operative.

Rappresenta inoltre il livello di connessione che rende interoperabili i processi, permettendo che identità, firme e attestazioni siano riconosciute e utilizzate tra organizzazioni, settori e Paesi diversi, senza la necessità di effettuare nuove integrazioni a ogni passaggio.

Ogni regolamento agisce su un diverso livello, ma tutti orientano le organizzazioni nella stessa direzione: **identità più forte, accountability più chiara, maggiore resilienza, operazioni più verificabili.**

I QUATTRO, UNO PER UNO

1 eIDAS 2.0

Definisce le regole per l'identificazione elettronica e i servizi fiduciari, consentendo alle organizzazioni di verificare l'identità e validare le transazioni digitali a livello transfrontaliero. In termini operativi: **consente di dimostrare chi sta agendo e se un'interazione digitale può essere considerata affidabile.**

3 AI ACT

Introduce un approccio basato sul rischio per l'intelligenza artificiale, con obblighi crescenti all'aumentare del rischio. In termini operativi: **garantisce che i sistemi di AI siano trasparenti, tracciabili e sicuri.**

2 DORA

Definisce come le organizzazioni finanziarie debbano garantire la continuità operativa sotto stress, imponendo la capacità di prevenire, resistere e recuperare da interruzioni dei sistemi ICT. In termini operativi: **assicura che i servizi critici continuino a funzionare anche in caso di guasti sistemici o attacchi informatici.**

4 NIS2

Eleva il livello minimo di cybersecurity nei settori essenziali e importanti. In termini operativi: **impone alle organizzazioni di gestire in modo strutturato il rischio cyber e di dimostrarlo concretamente.**

COME SI INTEGRANO

Questi strumenti normativi devono essere interpretati come componenti di un'unica architettura, non come iniziative separate:

- **eIDAS 2.0** stabilisce l'identità digitale fiduciaria;
- **NIS2** mette in sicurezza l'ambiente digitale;
- **DORA** garantisce la continuità operativa;
- **l'AI Act** disciplina i sistemi intelligenti costruiti sopra queste fondamenta.

Fiducia e sicurezza non sono più funzionalità aggiuntive: sono elementi strutturali che permettono alle organizzazioni di operare ed evolvere senza perdere il controllo.

PERCHÉ SONO STATI INTRODOTTI

L'obiettivo dell'Europa non è soltanto la crescita digitale, ma una **crescita digitale governata**, in cui l'innovazione non comporti dipendenze, fragilità o perdita di visibilità.

Esiste ora un corrispettivo sul lato dell'offerta rispetto a questa architettura normativa. Se eIDAS 2.0, NIS2, DORA e l'AI Act definiscono le regole che le organizzazioni devono rispettare, il proposto Cloud and AI Development Act (CADA) affronta una questione precedente: se l'Europa disponga effettivamente delle infrastrutture necessarie per poterle applicare. Le quattro normative definiscono l'esigenza di capacità di calcolo affidabile, controllabile e gestita in ambito europeo. Il CADA rappresenta il tentativo dell'Europa di costruire l'offerta necessaria a soddisfare questa esigenza.

La regolamentazione stabilisce le regole. Il CADA costruisce la capacità infrastrutturale. Il **Controllo Strategico** è ciò che mette in relazione questi due elementi. **La sovranità è architetturale, non contrattuale, non riguarda la velocità ma il controllo.**

L'AI Act segna il passaggio dell'AI dalla fase sperimentale a una dimensione di governance verificabile. Le organizzazioni devono dimostrare come i sistemi di AI vengono progettati, addestrati, distribuiti e monitorati, incluso come le decisioni vengono prese e come i rischi vengono gestiti. **L'AI non può essere governata se l'infrastruttura sottostante, l'identità e i livelli di controllo non sono già affidabili.**

In assenza di queste fondamenta, l'AI non riduce la complessità. La amplifica.



CAPITOLO 04

Il posizionamento distintivo di Aruba: CSP + QTSP in Europa

La sfida per le organizzazioni non è soddisfare quattro requisiti normativi separati. È costruire un sistema che ripristini il controllo, su identità, cybersecurity, operatività e AI, all'interno di un framework europeo coerente. È esattamente questo che Aruba abilita. E il modo in cui lo abilita è strutturalmente distintivo.

LO STACK EUROPEO INTEGRATO

Aruba è l'unico operatore europeo che combina capacità di **Cloud Service Provider (CSP)** e di **Qualified Trust Service Provider (QTSP)** all'interno di un unico modello operativo europeo. A questa combinazione, Aruba aggiunge infrastrutture data center proprietarie, operations di cybersecurity integrate, servizi di identità digitale e connettività, tutto all'interno di un'unica giurisdizione europea.

Questa combinazione conta perché risponde ai quattro regolamenti con una sola architettura, anziché quattro:

- **come CSP**, Aruba offre capacità cloud europeo sovrano e data center proprietari che rispondono ai requisiti di infrastruttura, hosting e resilienza operativa di NIS2 e DORA.
- **come QTSP**, Aruba opera nel settore dei servizi fiduciari qualificati attraverso due provider qualificati, Actalis (la prima Certification Authority italiana) e ArubaPEC, offrendo servizi che includono firme digitali, posta elettronica certificata (PEC), marcature temporali, recapito elettronico qualificato e identità digitale. Su scala continentale, i servizi fiduciari di Aruba gestiscono oltre 1,6 miliardi di firme elettroniche all'anno, 9 milioni di caselle PEC, oltre 2 milioni di identità digitali emesse (SPID) e 2,7 milioni di domini sotto gestione.
- **come operatore integrato**, Aruba opera la cybersecurity dal proprio SOC, gestisce capacità di managed detection and response e allinea la propria postura di sicurezza a framework riconosciuti come il NIST CSF.
- **come European builder & maker**, Aruba progetta, costruisce e gestisce direttamente le proprie infrastrutture e le proprie soluzioni, anziché rivendere capacità di terzi. È questo che rende la fiducia verificabile: l'architettura non è assemblata, è di proprietà.

Questa è anche la direzione che la politica industriale europea sta oggi promuovendo attivamente. L'obiettivo del proposto Cloud and AI Development Act (CADA), ovvero l'espansione della capacità di calcolo gestita in Europa per carichi di lavoro sensibili e critici, descrive ciò che Aruba già rappresenta: un operatore che realizza e gestisce infrastrutture proprie, anziché rivendere servizi di terzi.

Aruba non deve trasformarsi in ciò che il CADA mira a costruire. Aruba è già un operatore che opera in questo ambito.

Nessun concorrente diretto nel mercato europeo del cloud sovrano è in grado di offrire questa combinazione di competenze e asset. I provider di cloud sovrano non offrono servizi fiduciari qualificati. I fornitori di servizi di identità e fiducia digitale non dispongono di un'offerta di cloud sovrano europeo né di data center proprietari.

Questa combinazione distintiva continua a rappresentare un unicum nel mercato europeo.

Considerate nel loro insieme, queste quattro normative delineano una sfida comune di governance. Favorire il controllo strategico rappresenta la nostra risposta a questa sfida.

COSA ABILITA

L'infrastruttura non è più una commodity. È un asset strategico, la base su cui poggiano controllo, resilienza e capacità di evoluzione nel lungo periodo.

Aruba affronta questa sfida come un problema architetturale, non come una proposta di prodotto. Integrando infrastrutture europee, servizi fiduciari qualificati, cybersecurity, identità digitale e connettività all'interno di una sola giurisdizione europea, Aruba offre un modello operativo unificato in cui il controllo è integrato by design, non ricostruito a posteriori.

Questo permette alle organizzazioni di:

- **mantenere** piena visibilità sui propri ambienti digitali;
- **ridurre** la dipendenza da provider frammentati;
- **dimostrare** la conformità come conseguenza naturale dell'architettura;
- **evolvere** in modo continuo senza perdere il controllo.

IL MODELLO PROGRESSIVO

Aruba concretizza questo approccio attraverso quattro fasi progressive:

- **Enable** - Fondamenta native europee su infrastruttura, cloud, connettività, fiducia e sicurezza;
- **Enhance** - Servizi gestiti e orchestrati che integrano competenze e tecnologie diverse in soluzioni coerenti, riducendo la frammentazione e garantendo un unico punto di responsabilità;
- **Empower** - Co-progettazione di soluzioni su misura che combinano il giusto mix di infrastrutture, cloud, cybersecurity, servizi trust, AI e servizi gestiti per supportare gli obiettivi strategici dell'organizzazione;
- **Evolve** - Partecipazione attiva agli ecosistemi europei, contribuendo agli standard di interoperabilità e ai futuri framework di fiducia.

Questo approccio va oltre il supporto alla compliance. È il ripristino del controllo organizzativo sull'infrastruttura digitale.

PARTE II

Regolamento per regolamento

CAPITOLO 05

eIDAS 2.0: l'identità digitale come infrastruttura di fiducia

La domanda strutturale

La vostra organizzazione è in grado di dimostrare, su scala e attraverso le frontiere, chi sta operando in una transazione digitale e se quell'azione è giuridicamente vincolante?

eIDAS 2.0 è il framework europeo per l'identificazione elettronica e i servizi fiduciari qualificati. La sua riforma, che culmina nello European Digital Identity Wallet, sposta l'identità da credenziale detenuta dall'utente a infrastruttura interoperabile operata in tutto il Mercato Unico.

Implicazioni architetturali

Il passaggio da eIDAS 1.0 a 2.0 ridefinisce l'identità in quattro modi. Primo, l'identità diventa wallet-centric: cittadini e imprese controllano credenziali che presentano a servizi pubblici e privati. Secondo, l'identità diventa interoperabile: lo stesso wallet funziona attraverso Stati membri, settori e casi d'uso. Terzo, l'identità diventa ricca di attributi: oltre all'autenticazione, il wallet contiene attestazioni elettroniche qualificate di attributi (QEAA) e informazioni di business

verificate. Quarto, l'identità diventa operativa su scala: dal KYC all'onboarding all'esecuzione contrattuale, l'identità non è più un punto di ingresso ma un livello continuo di fiducia.

Per le organizzazioni, ciò si traduce in requisiti architetturali specifici:

- la capacità di emettere, presentare e verificare credenziali di identità basate su wallet;
- la capacità di integrarsi con servizi fiduciari qualificati per firme elettroniche, sigilli, marcature temporali ed e-delivery;
- la capacità di gestire flussi di identità transfrontalieri senza ri-integrazione in ogni giurisdizione;
- la capacità di validare l'identità in modo continuo, non solo al primo accesso.

Intersezioni

eIDAS 2.0 è il livello di identità che rende operativi gli altri tre regolamenti. Sotto DORA, l'identità è il modo in cui gli operatori finanziari dimostrano chi ha avviato quale azione sotto stress. Sotto NIS2, la governance dell'identità è uno dei requisiti baseline di cybersecurity. Sotto l'AI Act, l'identità è il modo in cui le organizzazioni distinguono l'azione umana da quella automatizzata e auditano le decisioni mediate dall'AI.

Cosa offre Aruba

Attraverso i Quality Trust Service Provider, Actalis (la prima Certification Authority italiana e tra i primi QTSP fondatori in Europa) e ArubaPEC, Aruba opera nel settore dei servizi fiduciari qualificati su scala continentale, offrendo firme digitali, posta elettronica certificata (PEC), marcature temporali, servizi di recapito elettronico qualificato (QeRDS), identità digitale (incluso SPID), verifica dell'identità e attestazioni elettroniche.

Il Wallet Gateway di Aruba fornisce il livello di integrazione attraverso cui le organizzazioni consumano le capacità dell'EUDI Wallet senza ricostruire l'infrastruttura di identità per ogni paese o caso d'uso. Aruba ha un ruolo di primo piano nei progetti POTENTIAL e WeBuild LSP (Large Scale Pilot) all'interno del European Digital Identity Framework, dove opera all'intersezione tra servizi fiduciari qualificati, integrazione wallet e interoperabilità transfrontaliera.

Si veda il **paper Wallet di Aruba** per il toolkit operativo su integrazione EUDI Wallet, QES/QEAA/QeRDS e flussi di identità transfrontalieri.

CAPITOLO 06

NIS2: la cybersecurity come baseline strutturale

La domanda strutturale

La vostra organizzazione è in grado di dimostrare, con evidenze, che la cybersecurity è governata come capacità strutturale e non come stratificazione di strumenti e policy?

NIS2 eleva il livello minimo di cybersecurity nei settori essenziali e importanti, formalizzando come obbligo di legge ciò che prima era buona pratica.

Sposta la cybersecurity da funzione IT che riporta verso l'alto a responsabilità a livello di board, che richiede evidenze architetturali.

Implicazioni architetturali

NIS2 si traduce in requisiti architetturali specifici che vanno oltre i tradizionali controlli di sicurezza:

- le misure di gestione del rischio devono essere proporzionate a dimensione, settore ed esposizione dell'entità e dimostrabili;
- l'incident reporting deve essere tempestivo, strutturato e coerente lungo la supply chain;
- la sicurezza della supply chain deve essere governata, non presunta, incluse le terze parti ICT;
- gli organi di governance (board, management) hanno responsabilità personale sulla postura di cybersecurity;
- test di sicurezza, formazione e miglioramento continuo devono essere documentati, non dichiarati;
- le capacità chiave di cybersecurity, SOC, vulnerability management, incident response, business continuity, devono essere operate in-house con adeguata maturità o approvvigionate da fornitori qualificati.

Intersezioni

NIS2 è la baseline di sicurezza su cui si costruiscono i requisiti di resilienza di DORA, il livello di governance dell'identità che eIDAS 2.0 rende operativo e la fondazione di fiducia che

l'AI Act presuppone quando richiede che i sistemi di AI operino su infrastrutture sicure. NIS2 è il regolamento che, se assente, mina gli altri tre.

Cosa offre Aruba

Aruba opera il proprio Security Operations Centre h24, con capacità di managed detection and response (MDR) ed extended detection and response (xMDR).

La postura di sicurezza di Aruba è allineata al NIST Cybersecurity Framework, con vulnerability assessment e penetration testing (VAPT) regolari, Web Application Protection (WAP) e infrastruttura dedicata anti-DDoS.

Aruba è il primo e il più importante cliente delle proprie soluzioni di cybersecurity: lo stesso livello di maturità operativa che protegge l'ecosistema digitale di Aruba e la sua base clienti è quello che Aruba offre come servizio. Per le organizzazioni che vogliono soddisfare gli obblighi NIS2 attraverso un fornitore europeo qualificato, Aruba offre due modelli operativi: cybersecurity managed (SaaS) per chi necessita di capacità integrate, e cybersecurity self-managed (PaaS) per chi mantiene le operazioni in-house ma ha bisogno di infrastrutture sotto giurisdizione europea.

Si veda il **paper Cybersecurity di Aruba** per il modello strutturale, managed vs self-managed, l'allineamento NIST CSF e l'integrazione con i servizi fiduciari.

CAPITOLO 07

DORA: la resilienza operativa come principio di progettazione

La domanda strutturale

La vostra organizzazione è in grado di continuare a erogare servizi critici quando i sistemi ICT di terze parti falliscono, vengono attaccati o non sono disponibili?

DORA, il Digital Operational Resilience Act, si applica alle entità finanziarie e ai fornitori ICT di terze parti che le servono. Sposta la resilienza dall'esercizio del piano di contingenza a una disciplina operativa continua e documentata, coprendo gestione del rischio ICT, incident reporting, digital operational resilience testing, gestione del rischio di terze parti e information sharing.

Implicazioni architetturali

DORA traduce la resilienza in architettura in cinque domini:

- **gestione del rischio ICT** - framework di governance, inventario degli asset, classificazione delle funzioni critiche;
- **gestione degli incidenti ICT** - detection, reporting, response e analisi della causa primaria sotto tempistiche stringenti;
- **digital operational resilience testing** - dal vulnerability assessment al threat-led penetration testing (TLPT) per le entità significative;
- **gestione del rischio di terze parti ICT** - clausole contrattuali, registro delle informazioni, monitoraggio del rischio di concentrazione, strategie d'uscita;
- **information sharing** - flusso di intelligence tra organizzazioni su minacce e vulnerabilità.

La dimensione più rilevante per i buyer è quella del rischio di terze parti. DORA obbliga le entità finanziarie a porre ai propri fornitori ICT domande che prima non venivano poste

a vendor cloud, hosting o SaaS, su sub-outsourcing, localizzazione geografica di dati e operazioni, diritti di audit, fattibilità dell'uscita e rischio di concentrazione.

Intersezioni

DORA è l'operativizzazione della resilienza che NIS2 stabilisce come baseline, applicata con precisione settoriale alla finanza. Dipende da eIDAS 2.0 per la verifica dell'identità in condizioni di stress e si sovrappone all'AI Act quando le entità finanziarie distribuiscono AI in funzioni rivolte al cliente o di decisione sul rischio.

Cosa offre Aruba

Il posizionamento di Aruba rispetto a DORA è diretto: come fornitore ICT sotto giurisdizione europea con infrastrutture proprietarie, servizi fiduciari qualificati e cybersecurity integrata, Aruba riduce sia l'area contrattuale sia il profilo di rischio operativo che DORAscrutina.

I contratti di Aruba possono soddisfare le clausole richieste da DORA su limiti al sub-outsourcing, diritti di audit, strategie d'uscita e perimetri geografici operativi. Il profilo operativo di Aruba, data center proprietari, connettività ridondante, resilienza certificata, risponde alla sostanza di ciò che quelle clausole chiedono. Per le entità finanziarie che navigano DORA, la domanda non è solo se un fornitore può firmare le clausole giuste, ma se l'architettura del fornitore può consegnare ciò che le clausole descrivono. L'architettura di Aruba è costruita per consegnare entrambi.

Si veda il **paper DORA Pulse di Aruba** per il toolkit operativo: clausole contrattuali, requisiti del registro delle informazioni, mappatura del rischio di terze parti, roadmap dei test e i sei punti di posizionamento di Aruba.



CAPITOLO 08

AI Act: la governance come prerequisito infrastrutturale

La domanda strutturale

La vostra organizzazione è in grado di distribuire sistemi di AI le cui decisioni, dati di addestramento e ambiente operativo siano auditabili end-to-end?

L'AI Act introduce un framework basato sul rischio per i sistemi di Artificial Intelligence, con obblighi crescenti all'aumentare della classificazione del rischio. Le pratiche proibite sono vietate. I sistemi ad alto rischio sono soggetti a obblighi di documentazione, test, monitoraggio, trasparenza e supervisione umana. I modelli AI di general purpose hanno obblighi specifici su trasparenza, copyright e rischio sistemico. I sistemi a rischio limitato hanno obblighi di disclosure.

Implicazioni architetturali

L'implicazione architetturale più importante dell'AI Act non è ciò che dice sull'AI, è ciò che presuppone sui livelli sottostanti. Per soddisfare gli obblighi dell'AI Act, un'organizzazione deve già avere:

- infrastruttura affidabile per eseguire workload AI con provenienza documentata;
- identità qualificata per distinguere l'azione umana da quella automatizzata e autenticare gli utenti di sistemi AI ad alto rischio;
- baseline di cybersecurity per proteggere dati di addestramento, pesi dei modelli e pipeline di inferenza;
- resilienza operativa per garantire che i servizi mediati dall'AI degradino in modo controllato;
- tracciabilità lungo il ciclo di vita dell'AI: fonti dati, esecuzioni di addestramento, modifiche di deployment, log di monitoraggio.

In altre parole, l'AI Act presuppone il lavoro che eIDAS 2.0, NIS2 e DORA richiedono. Le organizzazioni che non hanno costruito quelle fondamenta troveranno la conformità all'AI Act molto più difficile di quanto l'AI Act stesso suggerisca, perché l'AI Act tratta quelle fondamenta come date per scontate.

Intersezioni

L'AI Act si colloca sopra gli altri tre. Identità (eIDAS 2.0), sicurezza (NIS2) e resilienza (DORA) non sono obblighi paralleli, sono prerequisiti. Un'organizzazione che affronta l'AI Act isolatamente dagli altri tre finirà per ricostruire le fondamenta strada facendo.

Cosa offre Aruba

La proposta AI di Aruba non è deliberatamente una proposta di modelli. Aruba non offre LLM proprietari. Aruba offre le fondamenta europee su cui l'AI può essere distribuita in modo responsabile: infrastruttura sovrana per il calcolo (CPU e GPU), opzioni di Private AI Platform per i settori regolamentati, orchestrazione multi-modello senza lock-in proprietari, servizi fiduciari qualificati che autenticano le transazioni mediate dall'AI, operations di cybersecurity che proteggono dati di addestramento e pipeline di inferenza, ed energia da fonti idroelettriche proprietarie che risponde alle questioni di sostenibilità nelle valutazioni di rischio dell'AI Act. Per le organizzazioni che vogliono distribuire AI sotto l'AI Act, la domanda non è quale modello scegliere, è se le fondamenta sottostanti al modello possano essere documentate. Il ruolo di Aruba è rendere documentabili quelle fondamenta.

Si veda il **paper AI di Aruba per il paradosso compute-compliance**, l'offerta a tre livelli (IaaS, PaaS, SaaS) e l'architettura della piattaforma per i settori regolamentati.

PARTE III

Dalla normativa all'architettura



CAPITOLO 09

Il framework di acquisto

I quattro regolamenti si traducono in requisiti specifici di controllo, che si traducono in risposte architettrurali, che si traducono in capacità del fornitore. La matrice seguente è pensata per essere usata nell'ordine in cui i team acquisti effettivamente lavorano: **regolamento → requisito di controllo → risposta architettrurale → capacità Aruba.**

Non è esaustiva. È la shortlist strutturale di ciò che un comitato d'acquisto dovrebbe essere in grado di documentare e ciò che un fornitore dovrebbe essere in grado di dimostrare.

Per la piena profondità operativa su ciascuna riga, il paper Aruba dedicato fornisce il toolkit.

REGOLAMENTO	REQUISITI DI CONTROLLO	RISPOSTA ARCHITETTURALE	CAPACITÀ DI ARUBA
eIDAS 2.0	Verifica dell'identità transfrontaliera su scala	Verifica qualificata integrata wallet operante negli Stati membri	Aruba Wallet Gateway + Actalis QTSP + partecipazione POTENTIAL/WeBuild LSP
eIDAS 2.0	Firma elettronica qualificata, sigillo e marca temporale	Operatività QTSP continua sotto giurisdizione UE	Actalis (prima CA italiana): 1,6 miliardi di firme annue, full QES/QESeal/QTS/QeRDS
eIDAS 2.0	E-delivery fiduciario e notifiche con valore legale	Infrastruttura PEC e QeRDS operata end-to-end in Europa	Aruba PEC (10M caselle) + Aruba Sign + e-delivery qualificato
NIS2	Operatività SOC h24 e incident response	SOC operato con managed ed extended detection and response	SOC Aruba + servizi MDR/xMDR + allineamento NIST CSF
NIS2	Sicurezza della supply chain e governance terze parti ICT	Fornitore sotto giurisdizione europea con infrastruttura proprietaria	Aruba come builder & maker: nessun sub-outsourcing delle capacità core
NIS2	Vulnerability management e security testing	VAPT, web application protection, anti -DDoS come servizi continui	Aruba VAPT + Web Application Protection + infrastruttura anti-DDoS dedicata
NIS2	Evidenze a livello di board sulla postura di cybersecurity	Architettura documentata, certificazioni e audit trail	ISO 27001 + DC Tier IV + ACN QC3 + allineamento NIST CSF + logging audit-grade
DORA	Clausole contrattuali terze parti ICT (sub-outsourcing, audit, uscita)	Fornitore la cui architettura corrisponde a ciò che le clausole descrivono	Contratti DORA-aligned di Aruba + infrastruttura proprietaria sotto giurisdizione UE
DORA	Requisiti del registro delle informazioni	Fornitore in grado di fornire informazioni strutturate su localizzazioni e sub-provider	Information Pack DORA di Aruba + modello operative geografico trasparente
DORA	Rischio di concentrazione e fattibilità dell'uscita	Fornitore europeo alternativo con capacità full-stack	Aruba come fornitore europeo primario o secondario + Multi-Cloud Link per modelli ibridi
DORA	Partecipazione al threat-led penetration testing (TLPT)	Fornitore in grado di partecipare a scenari TLPT con entità finanziarie	SOC Aruba + modello di engagement security dedicato al settore finanziario
AI ACT	Infrastruttura europea per workload AI	Calcolo (CPU e GPU) sotto giurisdizione UE con provenienza documentata	Aruba AI Platform + AI Endpoints + GPU sovrana + Private AI Platform
AI ACT	Autenticazione fiduciaria delle Azioni mediate dall'AI	Livello di identità qualificata integrato con il workflow AI	Actalis QTSP + Wallet Gateway + infrastruttura di identità per agenti AI
AI ACT	Tracciabilità e audit del ciclo di vita AI	Logging infrastrutturale e tracciabilità lungo l'intero stack AI	Aruba Cloud + AI Platform con logging audit-grade + orchestrazione multi-modello

La matrice non è una checklist.

È una mappa strutturale: ogni riga mostra come un requisito normativo si traduce in una scelta architeturale, e ogni scelta architeturale in una capacità che può essere documentata.

La stessa mappa rivela qualcosa che le quattro normative non mostrano prese singolarmente, che le capacità più solide rispondono a obblighi di più regolamenti contemporaneamente. Una singola operazione SOC risponde simultaneamente a NIS2, DORA e AI Act. Un singolo servizio fiduciario qualificato risponde sia a eIDAS 2.0 sia all'AI Act. L'architettura comprime ciò che sembra essere quattro oneri di compliance separati in un modello operativo coerente.

È questo il significato pratico del Controllo Strategico: non l'assenza di regolamentazione, ma l'architettura che rende la regolamentazione operabile come un singolo problema di progettazione anziché quattro.



CAPITOLO 10

Oltre la compliance, verso il controllo

L'Europa si trova a un punto di svolta. Partecipare agli ecosistemi digitali globali mantenendo il controllo completo e la conformità al quadro normativo europeo, oppure rischiare l'esclusione da entrambi.

eIDAS 2.0, NIS2, DORA e AI Act affrontano ciascuno aspetti diversi della fiducia: identità, sicurezza, resilienza e governance dell'AI. Ma considerati nel loro insieme stabiliscono un principio chiaro:

I sistemi digitali devono essere sicuri, resilienti, tracciabili e controllabili by design.

L'Europa sta passando da un'era definita dall'adozione della tecnologia a un'era definita da governance, resilienza e controllo strategico.

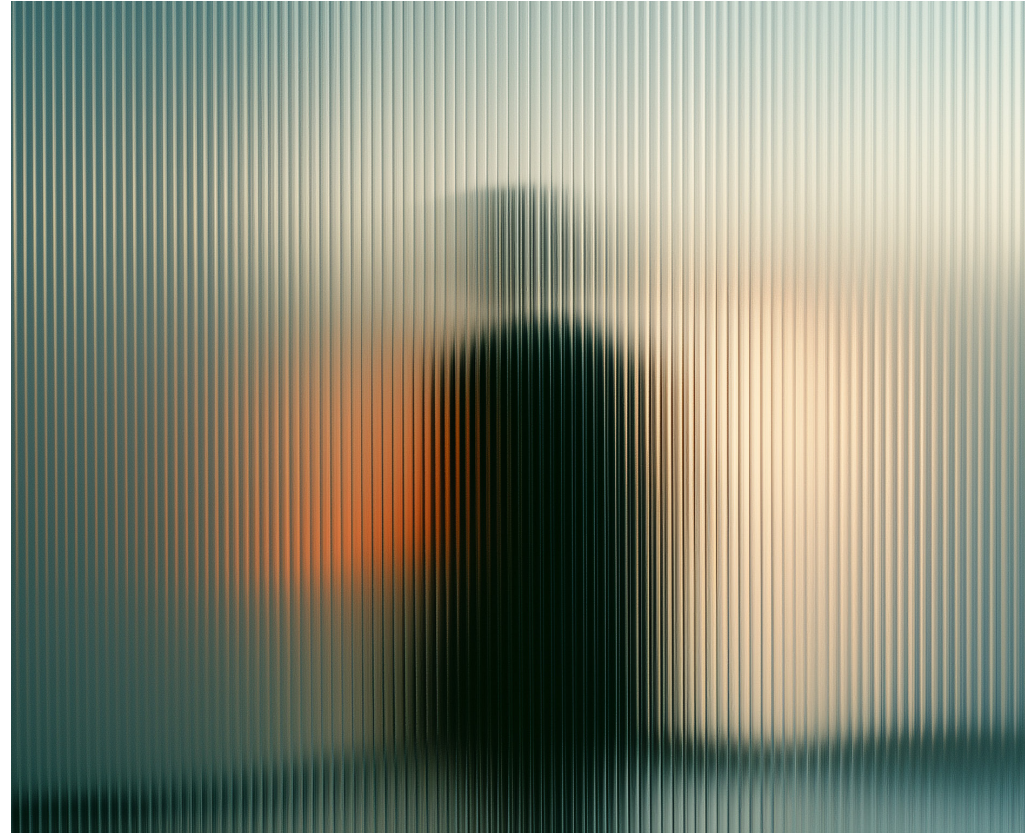
Per le organizzazioni, non si tratta solo di compliance. È un'opportunità per riaffermare la governance di sistemi frammentati, ridurre il rischio sistemico e costruire fondamenta solide per l'evoluzione di lungo periodo, affidandosi a partner che rendono la sovranità praticabile, non un onere. Le organizzazioni che ci riusciranno evolveranno in modo continuo senza perdere il controllo di infrastrutture, dati e processi decisionali.

Aruba rende questo possibile realizzando uno stack europeo unificato, dall'infrastruttura sovrana ai servizi fiduciari qualificati, dalle operations di cybersecurity all'identità digitale, come un sistema coerente.

La posizione dell'Europa sta evolvendo: dal definire regole alla costruzione di capacità concrete. Le quattro normative hanno definito i principi e i requisiti che devono caratterizzare sistemi digitali affidabili; strumenti come il proposto Cloud and AI Development Act pongono ora una domanda ulteriore: se l'Europa sia in grado di realizzarli.

Aruba si colloca proprio in questo punto di convergenza: non è in attesa che l'infrastruttura venga costruita, ma è già oggi un soggetto che la gestisce e la rende disponibile. **Non si tratta più solamente di scegliere quale o più tecnologia. È il momento in cui decidere chi governa le fondamenta digitali.**

Questa decisione spetta alle organizzazioni che l'Europa sta chiedendo di guidare la prossima fase della sua economia digitale. Il ruolo di Aruba è realizzare l'architettura che rende possibile la decisione.



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