ARCHITECTURE & TRUST

AI deployment and security brief.

A compact set of design questions for cloud, private, on-premise and edge AI systems. Controls should be proportionate to the use case and verified during architecture and testing.

1. Choose the operating boundary

Public cloud Evaluate data residency, provider services, identity integration, encryption, egress and shared-responsibility controls.	**Private cloud** Define tenant isolation, network boundaries, administrative access, backups and managed-service responsibilities.
On-premise Plan hardware capacity, patching, physical access, local identity, monitoring, backup and disaster recovery.	**Edge** Address device identity, secure boot, update signing, offline behaviour, local storage and tamper resistance.
Hybrid Map every data flow and define which system is authoritative when connectivity or synchronization fails.	**Third-party AI APIs** Review data use, retention, training terms, regional processing, abuse monitoring and exit options.

2. Define the essential controls

01	**Identity and access**	Least privilege, strong authentication, administrative separation and regular access review.	[ ]
02	**Data protection**	Minimization, classification, encryption, retention, deletion and approved transfer paths.	[ ]
03	**Application security**	Threat modelling, secure coding, dependency review, secrets management and testing.	[ ]
04	**Model and agent controls**	Evaluation, output constraints, tool permissions, human approval, prompt-injection defence and audit trails.	[ ]
05	**Observability**	Health, performance, error, drift, access and security logs with clear ownership.	[ ]
06	**Resilience**	Backups, recovery, offline behaviour, fail-safe states and tested incident procedures.	[ ]
07	**Supplier risk**	Contracts, subprocessors, service dependencies, breach terms and continuity plans.	[ ]

08	**Lifecycle**	Patch, retrain, revalidate, retire and securely dispose of systems and data.	[ ]

3. Launch with evidence

Before production, document acceptance tests, known limitations, user training, escalation paths, monitoring thresholds, rollback procedures, data retention, support ownership and the process for reviewing material changes.

This brief is general educational guidance. It does not certify a system or replace a security, privacy, safety, legal or regulatory assessment.