1 Architecture Design Principles for AI

These principles are to be applied in conjunction with the core enterprise architecture principles detailed in Architecture Design Principles.

1.1 Modular and Composable Design

1.1.1 Statement

AI systems must be architected as modular, composable components to enable flexible integration, scaling, and replacement.

1.1.2 Rational

Modularity supports rapid innovation, easier upgrades, and the ability to swap or extend AI capabilities as technology evolves.

1.1.3 Implications

- Prefer microservices, containerisation, and API-first approaches for AI workloads.
- Enable event-driven or change-driven architectures for dynamic AI orchestration.
- Support plug-and-play integration with existing enterprise platforms.

1.1.4 Improvement Actions

- Adopt modular design patterns for all new AI solutions.
- Document interfaces and dependencies for AI components.
- Establish guidelines for composability and integration.

1.1.5 Control Linkage

This principle is supported by the Responsible AI Policy, which requires that AI systems are reliable, maintainable, and support beneficial outcomes for people and planet. Modular design enables flexibility and adaptability, aligning with the policy's commitment to responsible and sustainable AI development (Responsible AI Policy, "Reliability" and "Inclusivity and sustainability" principles).

1.1.6 Architectural Check

Check

Is the AI system modular and composable, supporting integration and future extensibility?

Action

Prioritise solutions with clear interfaces, microservice architecture, and support for plug-in models.

1.2 Lifecycle Traceability

1.2.1 Statement

AI architectures must provide end-to-end traceability across the data, model, and operational lifecycle.

1.2.2 Rationale

Traceability ensures accountability, auditability, and the ability to diagnose issues or explain outcomes.

1.2.3 Implications

- Implement data lineage, model versioning, and audit trails for all AI systems.
- Maintain logs for training, inference, and decision-making processes.
- Support regulatory and internal audit requirements.

1.2.4 Improvement Actions

- Integrate traceability tools and frameworks (e.g., ML metadata stores).
- Define standards for logging and audit across AI lifecycle stages.

1.2.5 Control Linkage

This principle is supported by the Responsible AI Policy ("Transparency" and "Accountability" principles), which requires that AI systems are transparent, understandable, and can be challenged and validated by humans. It is also supported by the AI Risk Assessment Requirement, which mandates auditability and documentation throughout the AI system lifecycle (Requirement – IT – Assess AI risk, Section 5).

1.2.6 Architectural Check

Check

Does the AI system provide traceability for data, models, and decisions?

Action

Require evidence of lineage, versioning, and audit capabilities.

1.3 Secure-by-Design

1.3.1 Statement

AI systems must be secure by design, with robust controls for data, models, and operational environments.

1.3.2 Rationale

AI introduces new attack surfaces (e.g., model inversion, data poisoning) and must be protected from emerging threats.

1.3.3 Implications

- Enforce role-based access and encryption for AI artefacts.
- Isolate training and inference environments.
- Monitor for adversarial attacks and vulnerabilities.

1.3.4 Improvement Actions

- Conduct security assessments specific to AI risks.
- Implement automated monitoring and alerting for AI security events.

1.3.5 Control Linkage

This principle is supported by the Responsible AI Policy (“Security and safety” and “Reliability” principles), which require robust security controls and dependable operation of AI systems. The AI Risk Assessment Requirement further mandates that security risks are identified and mitigated as part of the AI use case assessment and periodic review (Requirement – IT – Assess AI risk, Section 5).

1.3.6 Architectural Check

Check

Is the AI system designed with security controls for data, models, and operations?

Action

Review security architecture, access controls, and monitoring provisions.

1.4 Interoperability and Standards Alignment

1.4.1 Statement

AI systems must align with open standards and support secure, interoperable integration with enterprise platforms.

1.4.2 Rationale

Interoperability enables data sharing, composability, and future-proofing as AI technologies evolve.

1.4.3 Implications

- Use open APIs, standard data formats (e.g., JSON), and shared vocabularies.
- Ensure compatibility with ISO/IEC 42001, NIST AI RMF, and other relevant frameworks.

1.4.4 Improvement Actions

- Mandate interoperability checks for all AI procurements.
- Maintain a register of supported standards and frameworks.

1.4.5 Control Linkage

This principle is supported by the Responsible AI Policy (“Transparency” and “Inclusivity and sustainability” principles), which encourage the use of open standards and accessible systems. The AI System Definition Guidance also supports this by defining the types of AI systems and techniques that must comply with group policies and standards (Guidance – IT – AI system definition, Section 1–2).

1.4.6 Architectural Check

Check

Does the AI system support open standards and secure integration?

Action

Validate API support, data format compatibility, and standards alignment.

1.5 Scalable Infrastructure

1.5.1 Statement

AI architectures must support elastic scaling for both training and inference workloads.

1.5.2 Rationale

AI workloads can be highly variable; scalable infrastructure ensures performance and cost-effectiveness.

1.5.3 Implications

- Design for process orchestration, load balancing and autoscaling.
- Monitor resource utilisation and optimise for cost.

1.5.4 Improvement Actions

- Implement autoscaling and serverless options for AI services.
- Track and report on infrastructure usage and efficiency.

1.5.5 Control Linkage

This principle is supported by the Responsible AI Policy (“Reliability” and “Inclusivity and sustainability” principles), which require that AI systems consistently perform as intended and deliver beneficial outcomes at scale.

1.5.6 Architectural Check

Check

Can the AI system scale elastically for training and inference?

Action

Assess infrastructure design and scaling capabilities.

1.6 Model Portability and Reusability

1.6.1 Statement

AI models should be portable across environments and reusable for multiple use cases.

1.6.2 Rationale

Portability and reusability reduce duplication, accelerate innovation, and support strategic alignment.

1.6.3 Implications

- Prefer standard model formats.
- Support transfer learning and fine-tuning.
- Separate model, data, and business logic layers.

1.6.4 Improvement Actions

- Document model formats and portability requirements.
- Encourage reuse through internal model registries.

1.6.5 Control Linkage

This principle is supported by the AI System Definition Guidance, which encourages the use of adaptable and reusable AI models and techniques to support a wide range of use cases and evolving requirements (Guidance – IT – AI system definition, Section 2–3).

1.6.6 Architectural Check

Check

Is the AI model portable and reusable across environments?

Action

Require documentation of model format and reuse strategy.

1.7 Observability and Monitoring

1.7.1 Statement

AI systems must include observability and monitoring for performance, drift, and operational health.

1.7.2 Rationale

Continuous monitoring ensures reliability, compliance, and rapid response to issues.

1.7.3 Implications

- Integrate real-time monitoring and alerting for AI metrics.
- Track model drift, anomalies, and degradation.

1.7.4 Improvement Actions

- Deploy observability platforms for AI workloads.
- Define KPIs and thresholds for AI system health.

1.7.5 Control Linkage

This principle is supported by the Responsible AI Policy (“Reliability” and “Accountability” principles), which require that AI systems are dependable and their functioning can be demonstrated throughout their lifecycle. The AI Risk Assessment Requirement also mandates ongoing monitoring and periodic review of AI systems (Requirement – IT – Assess AI risk, Section 5).

1.7.6 Architectural Check

Check

Is the AI system observable and monitored for key metrics?

Action

Review monitoring tools and reporting processes.

1.8 Service Landing and Operational Readiness

1.8.1 Statement

AI systems must pass a structured service landing process before production deployment.

1.8.2 Rationale

Operational readiness ensures supportability, maintainability, and compliance.

1.8.3 Implications

- Complete architecture checks, operational controls, and documentation.
- Define service boundaries and dependencies.

1.8.4 Improvement Actions

- Formalise service landing requirements for AI.
- Maintain operational runbooks and support plans.

1.8.5 Control Linkage

This principle is supported by the AI Risk Assessment Requirement, which requires that all AI systems are assessed, recorded in the AI inventory, and reviewed before deployment to live environments (Requirement – IT – Assess AI risk, Section 5).

1.8.6 Architectural Check

Check

Has the AI system passed operational readiness checks?

Action

Verify completion of service landing and support documentation.

1.9 Governance Hooks

1.9.1 Statement

AI architectures must expose hooks for governance, compliance, and policy enforcement.

1.9.2 Rationale

Governance integration enables automated risk assessment, policy checks, and lifecycle management.

1.9.3 Implications

- Tag AI artefacts with metadata for governance.
- Provide interfaces for risk and compliance tools.

1.9.4 Improvement Actions

- Integrate governance hooks into AI platforms.
- Automate policy enforcement where possible.

1.9.5 Control Linkage

This principle is supported by the Responsible AI Policy (“Accountability” principle), which requires that AI systems are governed throughout their lifecycle and that their functioning can be demonstrated through actions and decision-making processes. The AI Risk Assessment Requirement also supports this by requiring integration with governance and risk assessment tools (Requirement – IT – Assess AI risk, Section 5).

1.9.6 Architectural Check

Check

Does the AI system support governance integration?

Action

Validate metadata tagging and policy interface capabilities.

1.10 Strategic Alignment with Organisational Vision

1.10.1 Statement

AI systems must align with core architecture principles and support integration with digital workspace tools.

1.10.2 Rationale

Alignment ensures consistency, supportability, and strategic fit.

1.10.3 Implications

- Ensure compatibility with authentication, automation, and operational delivery standards.
- Support digital workspace integration.

1.10.4 Improvement Actions

- Map AI system architecture to core architectural standards.
- Document integration points and dependencies.

1.10.5 Control Linkage

This principle is supported by the Responsible AI Policy (“Inclusivity and sustainability” principle), which requires that AI systems are developed and used in a way that supports beneficial outcomes for people and planet, and are aligned with group policies and standards.

1.10.6 Architectural Check

Check

Is the AI system aligned with platform architecture and delivery standards?

Action

Review integration and compatibility documentation.