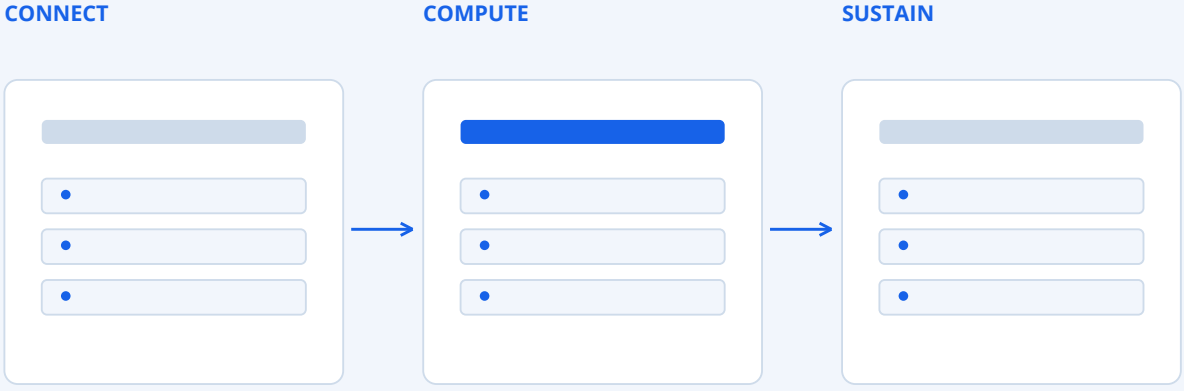
CONNECTED THINKING / PUBLIC WHITE PAPER

Connected Infrastructure

An engineering perspective on networks, intelligent compute, data centres, security, resilience and the operating environments they support.

Powering Intelligent Infrastructure.



Conceptual illustration / infrastructure dependencies

An engineering perspective for technical and commercial decision-makers.

Design revision 1.1 / 27 October 2026

EXECUTIVE PERSPECTIVE

Infrastructure works as a system.

Technology estates are systems of dependent capabilities. Connectivity influences application experience; power and cooling constrain compute; identity and security shape data access; logistics and lifecycle decisions determine whether a design can be commissioned and maintained. Isolated product choices create avoidable operational friction.

> This paper outlines an integrated approach for technical decision-makers. It is a methodology and capability overview, not a claim that a particular architecture is deployed at a named customer.

A CONNECTED VIEW

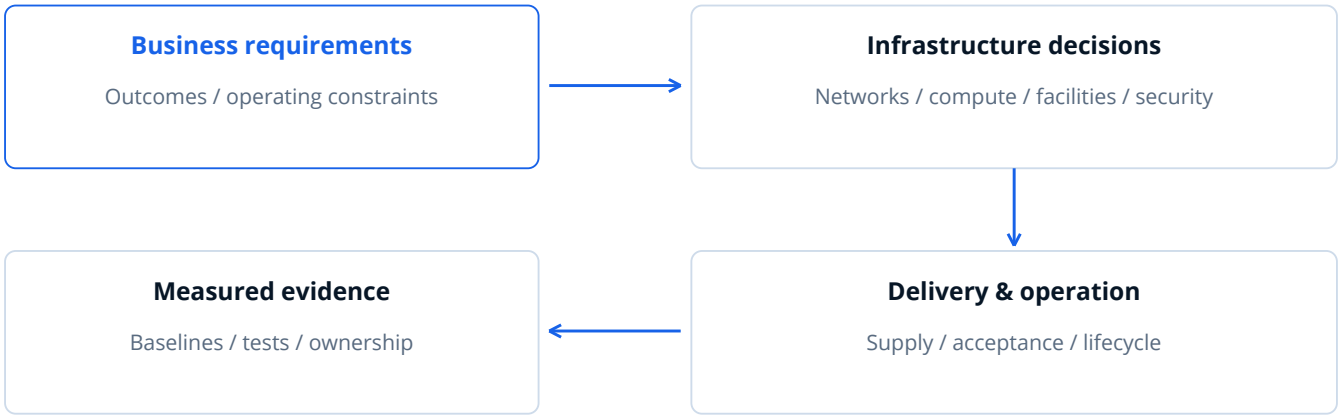


FIG 01 / Dependencies connect technical choices with delivery and operation · Conceptual illustration.

READ THE DISCIPLINES

01 Connected networks 03
02 AI-ready compute 04
03 Data-centre systems 04
04 Security 05
05 Document & workspace 05
06 Resilient operations 06
07 Delivery & supply chain 07
08 Implementation framework 08

01 / CONNECTED NETWORKS

Start with the path the application takes.

Begin with physical topology, structured cabling, distribution and access switching, Wi-Fi design, fibre and site constraints. Build the IP underlay and routing model around traffic, latency, availability and change operations. For multiple sites, assess WAN link diversity, SD-WAN policy, route failover, segmented access and observable application paths.

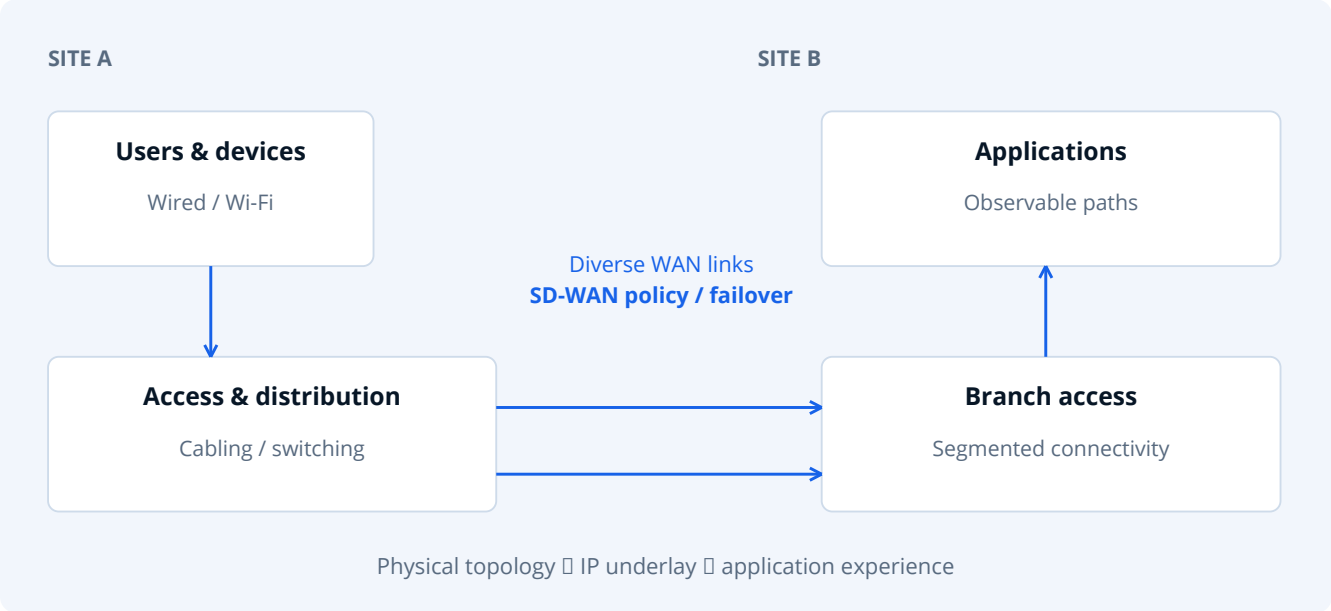


FIG 02 / A multi-site network connects physical access, WAN policy and applications · Conceptual illustration.

ACCEPTANCE & OWNERSHIP

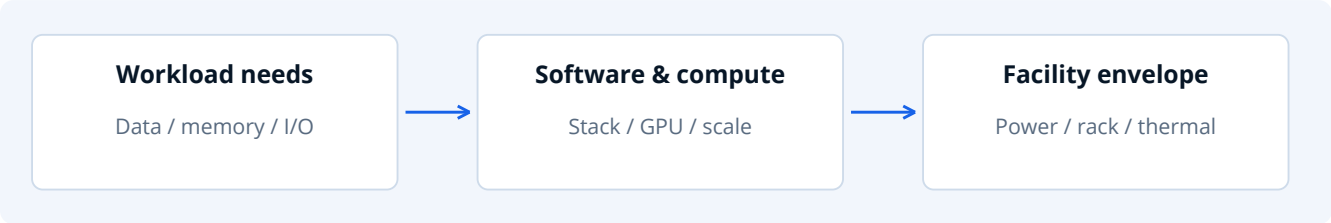
Acceptance requires documented performance baselines, coverage testing, failover evidence, configuration ownership and realistic support paths.

Topology / Coverage / Failover / Configuration ownership

02 / WORKLOAD PLACEMENT

AI-ready compute and workload placement

Determine workload characteristics before selecting servers or accelerators: data locality, memory, network throughput, GPU resource needs, storage I/O, virtualisation compatibility, physical rack density and thermal capacity. AI infrastructure also depends on data governance, model lifecycle, access controls and monitoring.



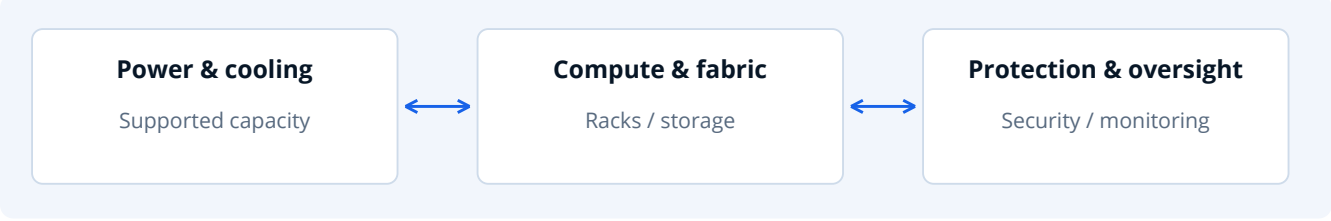
Decision gates include software stack validation, scaling profile, facility feasibility, vendor support, power budget and recoverability.

FIG 03 / Validate the workload, software stack and physical envelope together · Conceptual illustration.

03 / DATA-CENTRE & FACILITY SYSTEMS

Data-centre and facility systems

A data centre is an integrated system of racks, compute, storage, fabric, electrical distribution, uninterruptible power supply, cooling, environmental monitoring and physical security. Resilience targets and maintenance procedures must be engineered together.



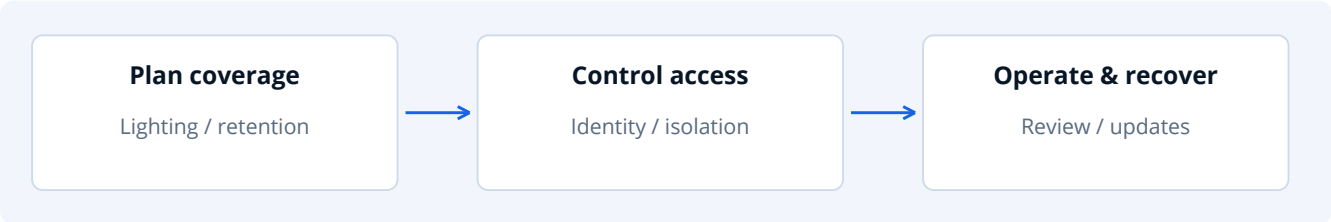
Capacity planning should use supported equipment envelopes and account for growth, redundancy, network interconnects, storage protection and lifecycle replacement.

FIG 04 / Resilience and maintenance span the facility and the technology estate · Conceptual illustration.

04 / ELECTRONIC & CYBER-PHYSICAL SECURITY

Electronic and cyber-physical security

IP surveillance and access-control systems require coverage planning, lighting, recorder/storage sizing, identity management, network isolation and retention policy. Security designs should include privacy requirements and operational ownership, not just camera placement.



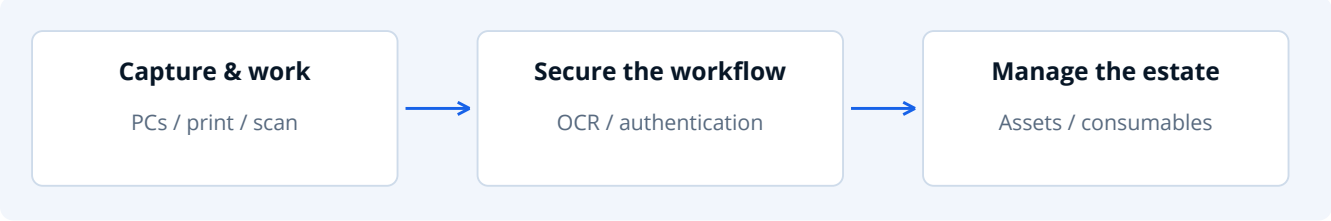
Control planes, devices and users must be managed with least privilege, supported updates, event review, tested recovery and appropriate monitoring.

FIG 05 / Coverage, access and operational controls belong in the same design · Conceptual illustration.

05 / DOCUMENT INTELLIGENCE & CONNECTED WORKSPACE

Document intelligence and connected workspace

Printers, MFPs, scanners, document capture and OCR workflows connect physical records to business processes. Selection criteria include throughput, media format, consumables, authentication, secure release, retention and line-of-business integration.



The workplace stack covers PCs, mobile endpoints, collaboration, connectivity and specific industry peripherals such as POS devices, with deployment, asset control and service management considered from the outset.

FIG 06 / Documents and endpoints remain connected to lifecycle and service management · Conceptual illustration.

06 / RESILIENT OPERATIONS

Design for recovery. Prove it in operation.

Define acceptable service interruption and data loss before choosing backup or disaster recovery technologies. Recovery time objectives and recovery point objectives inform replication, retention, restore testing, off-site separation, networking and escalation procedures.

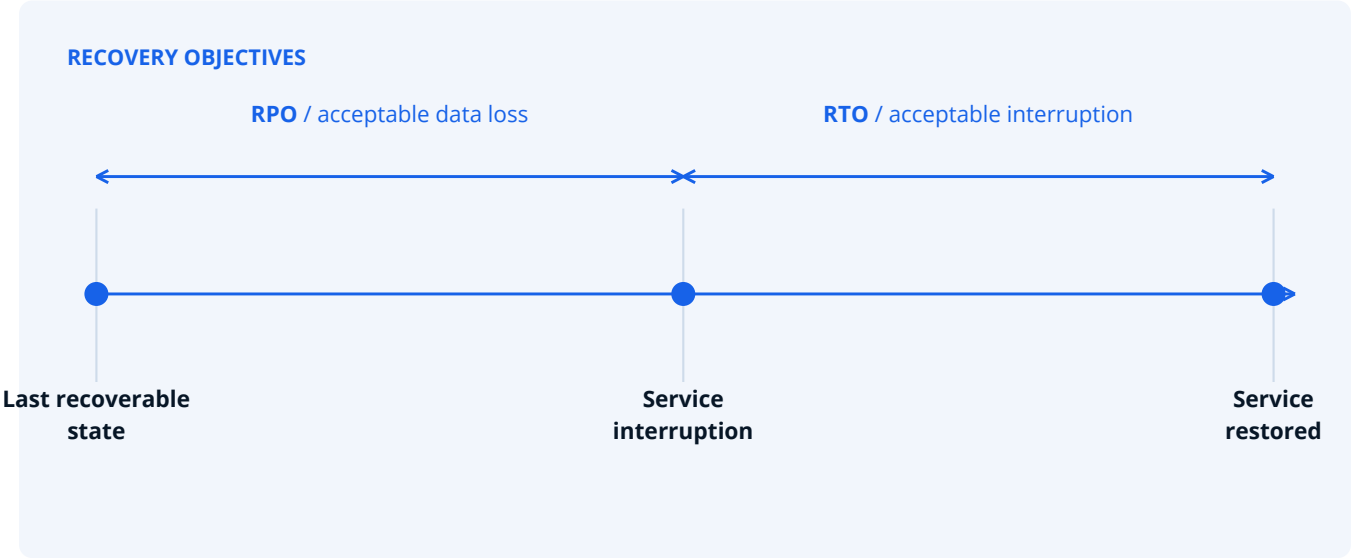


FIG 07 / Recovery objectives describe different parts of a service interruption · Conceptual illustration.

Monitoring, patching, inventory, power protection, spare equipment and runbooks transform a commissioned system into an operable service.

OPERATING DISCIPLINE

Monitor & patch	Inventory & spares	Power & runbooks

07 / DELIVERY & NATIONAL SUPPLY CHAIN

A sound design must be deliverable.

An achievable architecture must also be commercially and logistically executable. Specifications and alternatives are checked against distribution stock, lead times, licences, warranties and local conditions. Procurement approval precedes transport, receiving and installation.

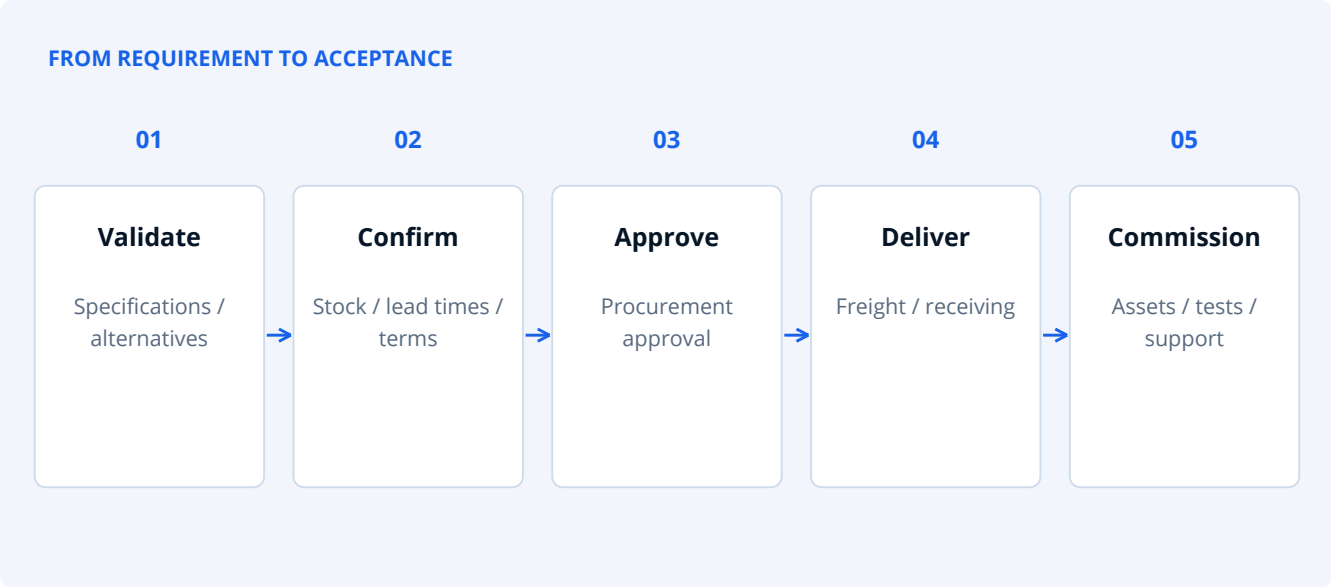


FIG 08 / Commercial and logistical validation precede installation · Conceptual illustration.

A project delivery plan covers manufacturer/distributor channels, freight options, proof of delivery, serialised asset reconciliation, on-site commissioning, testing and after-sales escalation. National reach is coordinated per engagement.

> **National reach is coordinated per engagement.**

08 / IMPLEMENTATION FRAMEWORK

Make acceptance part of the architecture.

Stage 1: discovery, stakeholder interviews, site and application assessment, risk record. Stage 2: architecture options, bill of materials, security and continuity requirements. Stage 3: product and commercial validation with approved supply routes. Stage 4: installation, migration and documented acceptance tests. Stage 5: handover, training, warranties, monitoring and improvement roadmap.



FIG 09 / Five stages connect scope, procurement and measured handover · Conceptual illustration.

Useful evidence includes topology diagrams, site surveys, performance baselines, power and thermal assumptions, test records, exception registers, as-built documents and support responsibility matrices.

CONCLUSION

The highest-value infrastructure investments are those whose components work together under real-world conditions. KABO advocates connected engineering, transparent supply assumptions and measured handover across industries and South African locations.

DISCUSS YOUR REQUIREMENT WITH KABO

Contact: info@kaboitgroup.co.za | www.kaboitgroup.co.za

Note: Specific stock, OEM programme authorisations, delivery times, project capacity, specifications, pricing and contractual commitments are confirmed for each enquiry.

Source copy: public website publication, 25 October 2026. Design revision 1.1, 27 October 2026. All diagrams are explanatory, not depictions of named customer installations.