CISILION

PILLAR 03 • CONNECT

Network Infrastructure

Build a resilient, secure network that keeps people, applications and operations connected.

An end-to-end modernised network infrastructure built for performance, security and growth.

WHY THIS MATTERS

AI, cloud and hybrid work are reshaping network demand.

97% of IT leaders see modernised networks as critical to deploying AI, IoT, and cloud

71% of organisations say their data centres can't yet meet today's AI demands

Source: Cisco, 2025 Global Networking Trends survey of 8,065 IT and business leaders

WHERE THINGS GO WRONG

Services rely on ageing foundations

Capacity, resilience or supportability constraints surface when demand or the business changes.

Fragmented vendors and visibility

Separate network, internet, cloud, SaaS and security views slow fault isolation and obscure user impact.

Lifecycle debt increases exposure

Unsupported assets, inconsistent standards, drift and patch dependencies increase operational effort and exposure.

Secure access is inconsistent

Users, devices, applications and connected environments are governed through different controls and operating processes.

WHAT WE DELIVER

Evidence before investment

Assess experience, performance, resilience, secure access, lifecycle exposure and operational maturity before recommending change.

A unified operating model

Campus, wireless, WAN, data centre, edge and observability joined up by design.

Modernisation targeted by risk and value

Protect viable investments, address material constraints and phase change around business priorities.

Assured and self healing operations

Combine 24×7 monitoring, incident and problem management, lifecycle governance, AI assisted insight and approved automation.

WHAT GOOD LOOKS LIKE

- ✓ Resilient connectivity for business-critical services
- ✓ End-to-end visibility from user to application
- ✓ Faster diagnosis and evidence led remediation
- ✓ Identity and context aware access with consistent policy
- ✓ A Lifecycle managed infrastructure with predictable investment
- ✓ Capacity and flexibility for cloud, IoT and relevant AI-enabled demand

WHY CISILION

Evidence before investment
Decisions are based on critical-service dependencies, experience, resilience, risk and lifecycle evidence.

Optimise before replacing
Viable assets are protected; refresh is prioritised by risk, business value, energy use and lifecycle.

Assurance across the full service path
Connectivity is considered from the user and site through internet, cloud, SaaS and applications—not only the assets the customer owns.

One lifecycle owner, with accountable automation
One governance model links assessment, design, delivery, adoption & improvement - automation applied where appropriate.

Secure access designed with connectivity
Identity, device context, segmentation and policy are integrated into operating model rather than added after deployment.

CLIENT PROOF

LOCKTON · WARBURG PINCUS · British Land

Our 5–step approach

We modernise data centre, campus and edge into one connected architecture- performance, security and visibility built in from day one.

STEP 01 **ASSESS** Understand your infrastructure, risks and AI-readiness before investing	Map critical services and dependencies · Baseline user/application experience · Review capacity, resilience, lifecycle and supportability · Assess secure access, segmentation and operational maturity · Validate readiness for planned cloud, workplace, IoT and AI use cases	**Outcome:** A decision-ready view of material risks, experience gaps, viable assets and investment priorities.
STEP 02 **DESIGN** Target architecture, roadmap and investment plan agreed before procurement	Define the target connectivity and operating model · Design resilience, secure access and assurance into the architecture · Select management approach by customer requirement · Develop migration, lifecycle, sustainability and investment options	**Outcome:** An Agreed target state and phased business case balancing resilience, risk, experience and cost.
STEP 03 **DELIVER** Modernise infrastructure with minimal disruption to users and services	Pilot and validate · Modernise campus, wireless, WAN, data-centre and edge capabilities as required · Integrate observability and service management · Migrate through controlled change, testing and rollback planning	**Outcome**: Modernised capability introduced with controlled risk, validated performance and minimal avoidable disruption.
STEP 04 **ADOPT** Enable operational readiness and maximise value from the platform	Establish runbooks, standards, ownership and escalation · Enable network, service-desk and security teams · Complete operational acceptance · Baseline service and experience measures · Embed change and lifecycle governance	**Outcome:** Teams, processes and evidence are in place to operate the environment safely and realise the intended value.
STEP 05 **MANAGE** AI-assisted, human led operational insight, lifecycle governance and continuous optimisation	24×7 monitoring and incident management within agreed scope · Experience and service assurance · Problem, change, configuration and lifecycle management · AI-assisted investigation and governed automation · Capacity, risk and continual-improvement reviews	**Outcome:** More predictable service performance, faster evidence-led response and an estate that evolves through controlled, prioritised improvement.

CLIENT PROOF

[Cisilion's] structured delivery, technical expertise and proactive guidance helped us reduce programme risk, maintain compliance and ensure the building was ready for seamless operational go-live."

Charles Horne, Project Director

British Land

Start with a network assessment

identify performance, resilience and security gaps, design the right network platform before you scale it

Book now