When evaluating a network architecture to fuel your digital transformation, use the following requirements checklist to guide your network vendor and technology architecture assessment.

Requirements Checklist for Vendor Evaluation

Ask your vendors:

- ☑ Can you demonstrate the business benefits of your architecture?
- ☑ Can you help us migrate our installed base seamlessly to a software-centric architecture?
- ☑ Do you offer investment protection?
- ☑ Is your architecture networkwide (access, core, WAN, branch)?
- ☑ Is your architecture open and standards-based?
- ☑ Do you have broad partner or services ecosystem support?
- ☑ Does your architecture simplify sustainable network compliance and support security certifications?
- ☑ Can you help us develop our network team's skill set to support a programmable network?
- ☑ Do you have a proven track record to be a trusted partner for the long-term, to support IT through the journey to digital?
- ☑ Do you or your partners offer a full portfolio of professional and technical architecture services?

Requirements for Technology Architecture Assessment

Architecture

- ☑ Can you offer on-premises and cloud-managed network consumption models?
- ☑ Does your architecture enable end-to-end service automation?
- ☑ Is your architecture designed for provisioning of services from the cloud?
- ☑ Is your architecture designed to support a controller-based programmable network?
- ☑ Is your architecture built to support virtualization that enables network services and hosted third-party apps to be deployed consistently across network devices, appliances, and virtual platforms?

Management

- ☑ Can your management system create and apply networkwide policy and services through standard APIs and traditional interfaces?
- ☑ To what extent does the architecture support consistent northbound APIs for third-party management or control applications?

Security

- ☑ Can your network act as a networkwide security sensor and intelligence dashboard?
- ☑ Can your network enforce contextual security policies and respond to contain threats?

For more information, visit:
www.cisco.com/go/dna