



# Give Your Network a Redesign: Network Readiness Guidebook.

Give Your Network a Redesign. We are The Redesign Group, your global IT solutions partner delivering value with velocity across data center, networking, security, and managed services. As a consultative Cisco partner, we combine boutique-level attention with national-scale expertise to help you design, secure, and manage modern networks that perform.

This guidebook gives IT leaders a practical, expert-led path to self-assess their networks, prioritize quick wins, and see exactly what a Redesign Network Assessment delivers.

## How to Use This Guide

- Pick 3–5 KPIs that matter most to your business and use our 90-day plan to prove progress.
- Align stakeholders on why networks struggle today, then baseline with the Readiness Checklist.
- Follow the 30/60/90-day Quick-Wins Plan with brief how-to steps under each action.
- Build your business case using the ROI framework, examples, and the included calculator table.
- Validate findings and accelerate outcomes with a Redesign Network Assessment.

# Table of Contents:

Outcomes You Can Prove in 90 Days	3
Why Networks Struggle Now	3
Tear-Out Readiness Checklist	4
Quick-Wins Plan: 30/60/90 Days	5
Business Case & ROI	6
What a Redesign Network Assessment Delivers	9
Citations & Further Resources	9
Next Step	10

# Outcomes You Can Prove in 90 Days.

Start with measurable improvements across performance, security, and cost. We will help you define, track, and report progress clearly.

- ✓ **Performance:** Lower critical-path latency; stabilize WAN under load; reduce mean time to repair (MTTR) via better telemetry and incident runbooks.
- ✓ **Security:** Accelerate vulnerability remediation; expand segmentation coverage; harden control-plane and admin access; reduce alert noise to sharpen signal.
- ✓ **Cost:** Eliminate overlapping tools; optimize licenses you already own (especially Cisco); right-size circuits and cloud egress; cut manual rework through standardization.

How to track it: Choose 3–5 KPIs with a clear before/after, such as branch uptime, segmentation coverage, critical CVE closure time, duplicated licenses removed, and change failure rate. Capture weekly snapshots and summarize progress in an executive one-pager.

## Why Networks Struggle Now.

Modern IT moves faster than legacy designs and processes can handle. If this looks familiar, you're not alone, and you're not stuck.

### Hybrid Sprawl

Apps, users, and data live everywhere; older patterns weren't built for distributed edges and cloud.

### Fragmented Tools

Too many consoles create blind spots, alert fatigue, and slow response.

### Evolving Threats

Identity, lateral movement, and aaS misconfigurations outpace manual controls.

### Scaling Demands

New sites and apps ship faster than standards and automation can keep up.

### Process Gaps

Inconsistent changes and config drift undermine stability and trust.

What you need is a lifecycle partner that can assess → design → implement → manage, aligning technology to outcomes your business cares about. That's our wheelhouse.

# Tear-Out Readiness Checklist.

Score each item: 0 = not in place, 1 = in progress, 2 = operational. Total per category to reveal strengths and gaps. Aim for 8–10 per category as a healthy baseline.

## 1) Architecture

- ☐ Documented end-to-end network map with data flows
- ☐ Standardized designs for campus, WAN/SD-WAN, and data center
- ☐ Identity-based access and least privilege enforced on network edges
- ☐ Cloud and SaaS connectivity patterns defined and secured
- ☐ Configuration standards versioned and reviewed quarterly

## 2) Performance

- ☐ Critical applications have documented SLOs and path preferences
- ☐ Proactive telemetry (NetFlow, synthetic tests) for key sites/apps
- ☐ QoS policies aligned to business priorities and validated
- ☐ Change success rate and MTTR tracked and trended
- ☐ Capacity plans for circuits, controllers, and wireless density

## 3) Security

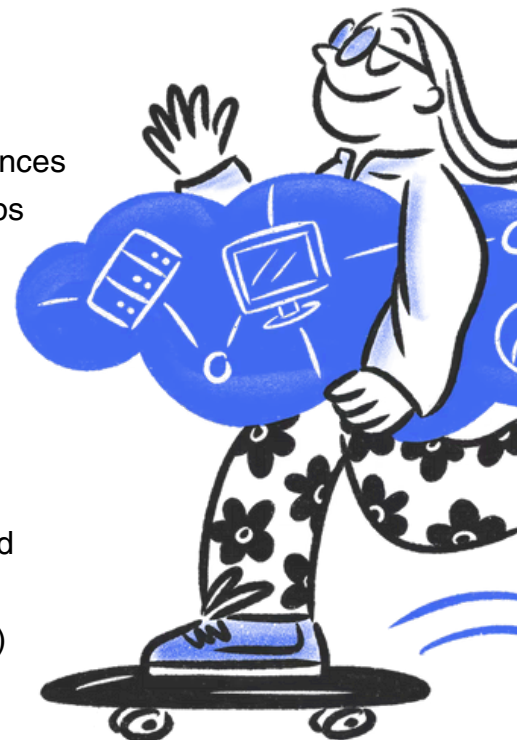
- ☐ Admin access hardened (MFA, RBAC, break-glass controls)
- ☐ North-south and east-west segmentation defined and enforced
- ☐ Timely patching for network OS and critical CVEs with SLAs
- ☐ Encrypted traffic inspection strategy (policy + privacy controls)
- ☐ Backups and golden configs tested for rapid restore

## 4) Visibility & Resilience

- ☐ Unified observability across on-prem, WAN, and cloud edges
- ☐ Health dashboards for executives and operators
- ☐ Automated alerts with runbooks to reduce noise
- ☐ HA patterns tested (failover, brownout, circuit impairment)
- ☐ Tabletop exercises for incident response and DR

## 5) Cost

- ☐ License utilization reviewed; shelfware identified
- ☐ Overlapping tools rationalized with an owner and timeline
- ☐ Cloud egress and backhaul costs monitored and optimized
- ☐ Circuit inventory reconciled to actual need
- ☐ Managed services vs. in-house mix evaluated for value



### Interpreting Results

Broad 0–1 scores indicate high risk and strong ROI potential from standardization and visibility.

1–2 scores suggest optimization and automation will unlock value quickly.

# Quick-Wins Plan: 30 / 60 / 90 Days.

## Days 0–30: Stabilize

- **Baseline health and risks; document the top five issues**
  - How to: Pull last 30 days of incidents from your ticketing system; tag by category (perf, security, change). Create a one-page heatmap of affected sites/apps.
- **Enable core telemetry and standard alerting for critical paths**
  - How to: Turn on NetFlow/sFlow and syslog from edge, WAN, and data center devices to a central collector (e.g., Cisco DNA Center or Secure Network Analytics). Define baseline alerts for link down, high interface errors, and loss/latency thresholds.
- **Harden admin access and close critical CVEs**
  - How to: Enforce MFA and role-based access on network controllers; rotate shared credentials; run a software advisory check against Cisco PSIRT and patch devices with critical CVEs first.
- **Apply quick policy fixes (DNS security, basic segmentation, QoS for critical apps)**
  - How to: Enable DNS filtering on egress; group high-risk assets into separate VLANs/VRFs; mark EF/AF for real-time apps and validate with synthetic tests.
- **Freeze non-urgent changes; introduce a lightweight CAB for high-risk changes**
  - How to: Require a peer review and rollback plan for any change touching routing, security, or WAN policies until baseline stabilizes.

## Days 61–90: Prove and Scale

- **Publish a KPI scorecard showing before/after impacts**
  - How to: Snapshot baseline metrics from Day 0 and compare to Day 60; show trend lines for uptime, MTTR, segmentation coverage, and tool count reduction.
- **Prioritize a 6-month roadmap with quick wins and strategic bets**
  - How to: Use an impact/effort matrix; schedule quarterly releases bundling related network, security, and automation initiatives.
- **Outline an automation backlog (backups, golden configs, policy as code)**
  - How to: Start with high-frequency, low-complexity tasks; define playbooks for config backups, compliance checks, and intent-based policies in your controller.
- **Brief executives on risk reduction, performance gains, and cost takeout**
  - How to: Create a one-page executive summary with KPIs, risk burndown, and financial updates; ask for sponsorship on two strategic initiatives.

# Business Case & ROI.

Strong networks pay for themselves through avoided incidents, faster recovery, and simpler operations. This section helps you quantify value, build internal alignment, and communicate payback clearly to finance and leadership.

## How to Build Your Case

- 1) Set scope and baseline:** Choose 3–5 KPIs (uptime, MTTR, CVE closure time, tool count, change failure rate) and collect 60–90 days of data.
- 2) Map initiatives to value drivers:** Stabilization reduces downtime; segmentation reduces breach impact; consolidation reduces software spend; automation reduces labor hours.
- 3) Quantify each driver:** Apply the formulas below and validate assumptions with historical data and benchmarks.
- 4) Model scenarios:** Best case, expected case, conservative case. Highlight payback period and 12–24 month ROI.
- 5) Assign owners and milestones:** Tie each value stream to an accountable owner with verified checkpoints.





## Value Drivers, Formulas, and Examples

- **Risk reduction:** Expected loss = incident probability × business impact.
  - Example: If your annual probability of a major lateral-movement incident is 25% and impact is \$800,000, expected loss is \$200,000. If segmentation and faster detection cut probability to 10% and impact to \$500,000, new expected loss is \$50,000. Annual risk reduction value: \$150,000.
- **Downtime cost:** Cost/hour × impact × hours avoided.
  - Example: Revenue at risk of \$75,000/hour × 30% service impact × 20 hours saved via improved resilience/MTTR = \$450,000 annual benefit.
- **Tool consolidation:** (Tool count eliminated × annual cost per tool) + support/training savings.
  - Example: Retire 3 overlapping tools at \$40,000 each and reduce support/training by \$15,000 → \$135,000 annual savings.
- **License optimization:** Activated features value vs. new spend avoided.
  - Example: Enabling Cisco DNA Center Assurance and SecureX replaces \$50,000 of point tools and avoids \$25,000 of new subscriptions → \$75,000 benefit.
- **Operational efficiency:** Change failure rate × rework hours × labor rate.
  - Example: 20 failed changes/year × 6 hours rework × \$120/hour = \$14,400. Cutting failures by 70% saves \$10,080 annually and reduces incident risk.







## Simple ROI Calculator (Example)

Value Stream	Annual Benefit
Risk Reduction	\$150,000
Downtime Avoided	\$450,000
Tool Consolidation	\$135,000
License Optimization	\$75,000
Operational Efficiency	\$10,080
<b>Total Annual Benefit</b>	<b>\$820,080</b>
Estimated One-Time Investment	\$250,000
Estimated Annual Operating Cost	\$120,000
<b>Net Annual Benefit</b> (Benefit – Operating)	<b>\$700,080</b>
<b>Payback Period</b> (One-Time / Net Annual Benefit)	<b>~4.3 months</b>
<b>Year-1 ROI</b> ((Benefit – Costs) / Costs)	<b>~174%</b>

Tip: Replace the example numbers with your actuals. Keep assumptions conservative and include sensitivity ranges.

### Visual Summary

Use a simple bar visualization in your executive deck to make the case intuitive:

- Annual Benefits  \$820k
- Operating Cost  \$120k
- One-Time Cost  \$250k
- Net Benefit  \$700k

Prefer a spreadsheet? Export the calculator above and chart the values in your format of choice.



# What a Redesign Network Assessment Delivers.

Our assessment is a fast, low-friction engagement designed to create momentum while setting the stage for long-term transformation. With deep Cisco expertise, we meet you where you are and accelerate what's next.



**Architecture blueprint** with current-state map and future-state design.



**TCO/ROI model** covering tool rationalization and operational savings



**Configuration and security baseline** with a prioritized gap list



**Practical roadmap** aligned to 30/60/90 and 6-month outcomes



**Performance and reliability scorecard** tied to business SLOs



**Executive readout** to align IT and business stakeholders



**Risk register** with likelihood/impact and mitigation plan

## Citations & Further Resources.

Explore these references to deepen your plan and validate best practices:

- The Redesign Group: <https://redesign-group.com>
- Cisco SD-WAN Overview: [Cisco SD-WAN](#)
- Cisco Security Portfolio: [Cisco Secure](#)
- Cisco DNA Center (Operations & Assurance): [Cisco DNA Center](#)
- Cisco Meraki Cloud-Managed Networking: [Cisco Meraki](#)
- Cisco Design Zone (Best Practices & Reference Architectures): [Cisco Design Zone](#)
- NIST Cybersecurity Framework: [NIST CSF](#)
- CISA Zero Trust Maturity Model: [CISA ZTMM](#)
- Center for Internet Security (CIS) Controls: [CIS Controls](#)
- Service Level Objectives (SLOs): [SRE: SLOs](#)
- SANS Incident Response Resources: [SANS White Papers](#)

# Next Step

Ready to validate your checklist, prioritize quick wins, and build a pragmatic roadmap?  
Give Your Network a Redesign by requesting a Complimentary [Redesign Network Assessment](#).

We combine the agility and personal attention of a boutique firm with the scale and expertise of a national integrator to deliver outcomes that last.

[re]DESIGN

