Network Readiness Checklist

Most coworking operators don't think much about their network until it starts to demand attention. That's understandable. When you're opening and running a space, the priority is simply getting things to work.

This checklist draws on our experience working alongside coworking operators at every stage, from opening a first space to managing multi-location portfolios. It is designed to give first-time and scaling operators a clearer view of what matters as they plan ahead.

The goal is not to add complexity or push change. It is to help operators look ahead thoughtfully because small, early decisions around connectivity often shape member experience, support load, and how easy it is to scale later.

How to use this checklist

- Answer honestly based on today, not your ideal future state
- Highlight any questions that feel unclear or uncomfortable
- Pay special attention to anything marked ⚠️ A note from experience

1. Internet Circuits

Before Wi-Fi, before access points, and before any hardware decisions, there is the internet circuit itself. This is the connection that feeds everything in your space, from member laptops and video calls to printers, phones, and security systems. When this connection is undersized, unreliable, or poorly understood, issues tend to surface elsewhere and are often misdiagnosed as Wi-Fi problems.

- ☐ Do you know what type of internet circuit you have (coax vs dedicated fiber/DIA)?
- ☐ Is your upload speed sufficient for video calls, not just downloads?
- ☐ Do you have an SLA (uptime guarantees) from your ISP? If so, do you understand it?
- ☐ Do you have any backup connection in place?

⚠️ A note from experience:
Fast download speeds can hide slow upload performance. Video calls fail on upload, not download. We recommend a baseline of 100 Mbps upload for a typical single-site coworking space, though spaces with larger teams or frequent video use may require 200+ Mbps.

2. Redundancy & Downtime Risk

Internet outages are not a question of if, but when. They may come from an ISP issue, nearby construction, a weather event, or something as simple as a failed piece of equipment. Planning for downtime is less about preventing every outage and more about understanding how your space behaves when one occurs.

- ☐ If your primary internet went down, do you know what would stop working immediately?
- ☐ Do you know how much one hour of downtime would realistically cost you?
- ☐ Do staff know what happens automatically during an outage (failover vs manual)?
- ☐ Do you have a backup circuit?
- ☐ Is your backup connection tested—not just installed?
- ☐ Are each of your circuits under active monitoring so you know if they are down?

⚠ A note from experience:
Think of a backup like an insurance policy. A backup circuit that no one has tested is just expensive peace of mind.

3. Local Network Infrastructure (The "IT Closet Stuff")

Most coworking operators inherit their network infrastructure rather than intentionally designing it. It often comes bundled with a build-out, installed by a vendor, or carried over from an earlier phase when the priority was simply getting online. Because it sits out of sight, this layer can feel abstract or easy to ignore, even though it plays a central role in performance, security, and reliability.

- ☐ Do you have a dedicated firewall (not just a router)?
- ☐ Are switches and access points designed for commercial use?
- ☐ Do you know how many devices your network can handle concurrently?
- ☐ Could you confidently explain, at a high level, how traffic flows through your network?
- ☐ Something about hardware age?

⚠ A note from experience:
Adding more access points rarely fixes underlying design issues. When the core network is undersized or poorly segmented, extra hardware often just spreads the same problems around. The result is more complexity, not better performance.

4. Wi-Fi Access & Authentication

How people get onto your Wi-Fi has an outsized impact on both security and the day-to-day experience in your space. When access is simple and well-defined, members connect quickly, staff don't have to intervene, and issues are easy to resolve. When it is not, small frictions show up repeatedly and often land on community teams to sort out.

- [ ] Are members using a shared password or individual credentials?
- [ ] Do you know how quickly you can revoke access when someone leaves?
- [ ] Is guest access separated from member access in a meaningful way?
- [ ] Does onboarding/offboarding require staff involvement every time?

⚠ A note from experience:
Many spaces start with shared passwords because they are simple and quick to set up. As members change and teams grow, controlling who has access and when becomes more important.

5. Network Segmentation & Privacy

As teams grow and become more sophisticated, expectations around privacy and security tend to rise quietly. What feels acceptable in a small, early-stage environment can start to feel insufficient once larger teams, regulated industries, or more sensitive work enter the space. This is often the point where "good enough" connectivity begins to show its limits.

- [ ] Can one member's devices see another member's devices on the network?
- [ ] Do teams have isolated, private network environments by default or by request?
- [ ] Are communal resources (printers, AV) accessible without breaking isolation?
- [ ] Would an enterprise prospect feel confident asking about your network security?
- [ ] Something about compliance to support enterprise clients?

⚠ A note from experience:
Network segmentation is less about complexity and more about boundaries. It determines whether one company's devices can see another's, how private work is protected, and how confidently you can answer security-related questions from prospective members. When done thoughtfully, it allows privacy and shared resources to coexist without forcing tradeoffs that create friction for staff or members.

6. Member Experience & Support Load

This is where network decisions show up day to day. When connectivity works quietly, members stay productive and staff stay focused on hospitality. When it does not, even small issues can become recurring distractions that pull attention away from higher-value work.

- [ ] Do community staff regularly troubleshoot Wi-Fi issues?
- [ ] Are support issues predictable or ad-hoc and stressful?
- [ ] Do you have simple "Plan B" options for common failures (dongles, adaptors, wired internet, etc.)?
- [ ] Can staff help without escalating everything to a vendor?

⚠ **A note from experience:**
Every "small" issue compounds over time. What feels minor in isolation adds up to lost staff time, increased stress, and a steadily more frustrating experience for members.

7. Visibility & Network Insight

Your network is constantly generating signals about how your space is actually being used. Unlike surveys or support tickets, this information reflects real behavior, not just what members choose to report. When you have access to that insight, patterns become easier to spot and decisions feel less like guesswork.

- ☐ Can you see peak usage times and high-traffic areas?
- ☐ Do you know how many devices are active at any given time?
- ☐ Can you spot abnormal usage patterns or potential abuse?
- ☐ Are network insights used for staffing, layout, or planning decisions?
- ☐ Something about data holes with access control data only

⚠ **A note from experience:**
Without visibility, decisions are based on anecdotes, not patterns. A single complaint or comment can feel urgent, even when it does not reflect how the space is actually being used.

8. Scalability: Expand or Adding a Another Location

Expansion is often when earlier network decisions become visible. What works in one space can be harder to manage across multiple locations, especially without clear documentation. The key question is not whether your setup works today, but how easily it can be repeated tomorrow.

- ☐ Could you replicate your current setup without reinventing everything?
- ☐ Are configurations documented or locked in someone's head?
- ☐ Would adding a second site double your complexity—or mostly copy/paste?
- ☐ Could staff manage double the locations without needing twice the expertise?
- ☐ Something about brand consistency & roaming

⚠ **A note from experience:**
What works once doesn't always scale cleanly. Growth has a way of exposing shortcuts that were invisible at the start.

9. Total Cost of Ownership (Beyond the Hardware)

The upfront cost of networking equipment is usually the easiest part to understand. The longer-term costs are more subtle and tend to show up over time in the form of staff hours, outside support, and ongoing maintenance. As setups grow more complex, even small changes can require coordination, troubleshooting, or paid assistance.

- [ ] Do you factor your own time into “DIY” decisions?
- [ ] Are updates handled as part of a regular process, or only when something breaks?
- [ ] Do small changes require outside help and extra invoices?
- [ ] Have earlier decisions created ongoing maintenance or cleanup work?

⚠ A note from experience:
The lowest upfront cost often costs the most over time. What looks simple at the start can quietly add up in staff hours, support calls, and one-off fixes. The real cost shows up in how often you have to think about it.

10. Strategic Optionality (Your Future Self Will Thank You)
Not every capability needs to be in place from day one. What matters is whether your current setup keeps options open as your space evolves. Strategic optionality is about preserving the ability to respond to new member needs, pricing models, or growth plans without being forced into disruptive changes.

- [ ] Could you offer private networks or bandwidth tiers if demand arose?
- [ ] Would monetizing connectivity feel natural—or impossible with your setup?
- [ ] Are you locked into a single vendor or architecture?
- [ ] Can your network adapt without a full rip-and-replace?

⚠ A note from experience:
Flexibility is easiest to preserve before you need it. When systems are designed with change in mind, future adjustments feel manageable instead of disruptive.

Network Readiness Summary

Use this page to step back and make sense of your answers. The goal isn't to score yourself, it's simply to identify where attention now will save you time, stress, or rework later.

Review each section and count how many items you checked. Based on that total, select the confidence level that best fits:

3–4 – Confident
2 – Mixed
1 – Not Confident
Unclear – if you could not confidently answer several items.

Section	Score	Confident	Mixed	Not Confident	Unclear
Internet Circuits	____	☐	☐	☐	☐
Redundancy & Downtime	____	☐	☐	☐	☐
Network Infrastructure	____	☐	☐	☐	☐
Wi-Fi Access & Authentication	____	☐	☐	☐	☐
Network Privacy & Segmentation	____	☐	☐	☐	☐
Member Experience & Support	____	☐	☐	☐	☐
Visibility & Insights	____	☐	☐	☐	☐
Scalability (Next Location)	____	☐	☐	☐	☐
Total Cost of Ownership	____	☐	☐	☐	☐
Strategic Flexibility	____	☐	☐	☐	☐

How to interpret your results

Mostly Confident
You are likely in a solid position. Focus on documenting what is working and making sure that knowledge is easy to repeat and share.

Mixed
This is common, especially for early or growing operators. Prioritize a few high-impact areas and address them deliberately rather than trying to fix everything at once.

Not Confident
This is a signal to slow down before making changes or scaling further. Gaining clarity now can prevent unnecessary rework and stress later.

Unclear
Uncertainty usually means key information is missing or hard to access. Pausing to understand what you have and how it works often brings the most immediate value.

Priority Areas (Top 3)
List the three areas that felt most fragile, unclear, or operationally heavy.

1. _____

2. _____

3. _____

Warning Signs to Watch For
If you notice any of the following, it's usually time to take action:

- ☐ Community staff spending more time on connectivity than hospitality
- ☐ Larger teams asking detailed security or privacy questions
- ☐ "Quick fixes" becoming permanent
- ☐ Anxiety around adding a second location
- ☐ Fear of touching the network because it might break something

A second look from someone who understands coworking networks can bring focus and confidence to your next step, helping you prioritize what matters now without overthinking everything else.

Review Your Results with an isofy Network Engineer

Schedule Your Free Review Now

Exclusively for Coworking Convos Participants