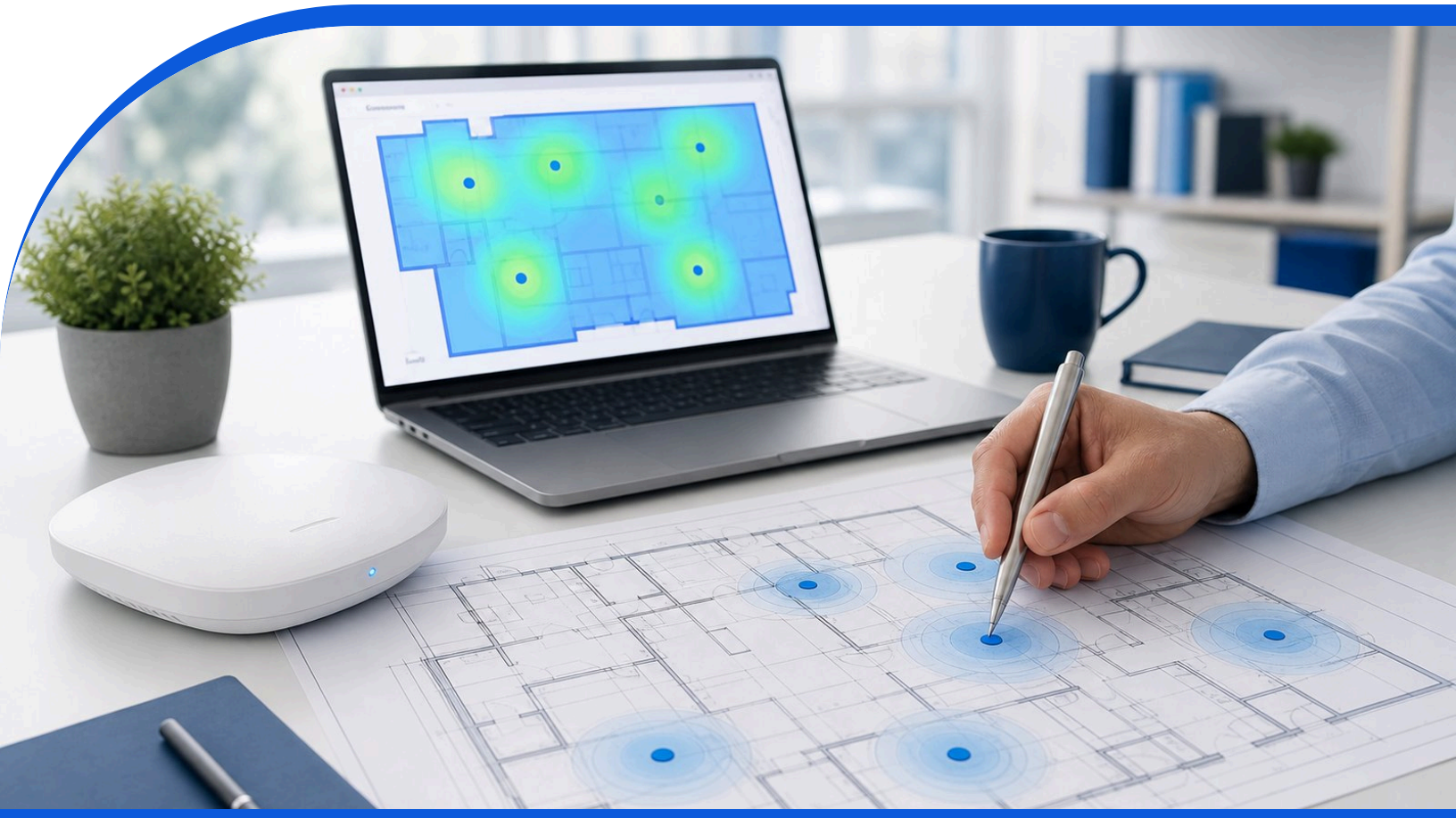
QOS MSP
Managed Services

BUSINESS WI-FI PLANNING:

THE SITE-SURVEY CHECKLIST



+1 (877) 800-7672

www.qosmsp.com

Business Wi-Fi Planning & Site-Survey Checklist

Most bad Wi-Fi wasn't installed badly. It was installed for a smaller office, a lighter device load, and fewer walls — and then the business grew into dead zones, dropped calls, and a network nobody trusts.

Good business Wi-Fi is designed, not guessed. It starts with a site survey: measuring the space, the walls, the interference, and the real device count before a single access point goes up.

Use this checklist to plan wireless that covers every corner, holds a connection as people move, and keeps staff, guests, and devices safely apart. Work through it before you buy hardware — the cheapest fix is the one you make on paper.

1. Start With Requirements, Not Access Points

"We need more Wi-Fi" is not a plan. What you're covering and who's using it decides everything that follows.

Write Down:

- Every area that needs coverage — offices, warehouse, breakrooms, parking, outdoor
- What runs on the wireless — laptops, phones, VoIP calls, scanners, cameras, IoT
- Where people move while connected — and where they can't drop
- Who gets on the network — staff, guests, contractors, personal devices
- The applications that can't stutter — video calls, VoIP, real-time systems

The Goal:

A coverage and capacity target you can design against — not a guess about how many access points "should" do it.

2. Map Every Space You Need to Cover

This is the site survey. A floor plan and a walk-through turn assumptions into measured facts.

Survey the Building:

- Get a scaled floor plan — square footage, ceiling heights, floor count
- Mark construction that blocks signal — concrete, brick, metal, glass, firewalls
- Note every space that must stay connected — and the dead spots today
- Walk multi-floor and multi-building coverage as one system, not separate networks
- Record existing wiring and where new cable can and can't run

The Red Flag:

If nobody has walked the space with a survey tool, access-point placement is a guess — and guesses leave dead zones.

3. Count the Devices, Not the People

Wireless capacity is set by devices and applications, not headcount. A 40-person office can carry 200 connected things.

Estimate Real Load:

- Two to three devices per person is normal — laptop, phone, tablet
- Add the fixed devices — VoIP phones, printers, cameras, sensors, scanners
- Flag high-density rooms — conference rooms, training rooms, event spaces
- Identify bandwidth-heavy use — video meetings, large file transfers, streaming

The Goal:

Access points sized for how many devices actually connect at once — so the network stays fast when the room fills up.

4. Plan for Interference Before It Plans for You

Wireless shares the air with everything around it. Interference is a design problem, not bad luck.

Account For:

- Neighboring networks competing on the same channels
- Microwaves, cordless phones, Bluetooth, and other 2.4 GHz noise
- Dense walls and metal shelving that reflect and absorb signal
- Channel planning across access points so they don't fight each other
- Using 5 GHz and 6 GHz bands to escape crowded 2.4 GHz

The Bottom Line:

Coverage isn't enough. Access points have to be tuned to coexist, or they interfere with themselves.

5. Design Access Point Placement Deliberately

Where the access points go — and how they hand devices off — is what separates engineered Wi-Fi from a box on a shelf.

Place for Coverage and Roaming:

- Overlap cells so a device never loses signal between access points
- Mount for the space — ceiling for open floors, directional for long aisles
- Design roaming so calls and sessions survive the walk from room to room
- Cover the edges — stairwells, corners, loading docks, outdoor areas
- Leave room to add access points as the business grows

The Goal:

Full coverage with clean handoff — no dead zones, and no dropped calls when someone moves.

6. Separate Guests, Staff, and Devices

One flat, open wireless network is a security incident waiting to happen. Segmentation is not optional.

Build In From the Start:

- A separate guest network that can't reach internal systems
- Staff Wi-Fi on its own segmented VLAN
- Cameras, IoT, and building devices isolated from user traffic
- Strong encryption (WPA2/WPA3) on every network
- Access control that ties who's on Wi-Fi to what they're allowed to reach

The Red Flag:

If a guest phone and your accounting server sit on the same flat network, wireless is your weakest door.

7. Power and Cable Every Access Point Properly

Wireless is only wireless at the last few feet. Every access point rides on a wired connection behind the ceiling.

Get the Physical Layer Right:

- Run structured cabling to every access-point location before you mount them
- Plan Power over Ethernet so access points don't need local power
- Size the switches to feed every access point at full capacity
- Confirm the wired network and internet circuit can carry the wireless load

The Bottom Line:

Great access points on undersized cabling and switching still deliver bad Wi-Fi. The wireless design and the wired design have to match.

8. Validate After Install — Survey Again

A design on paper is a prediction. A post-install survey is proof.

Verify the Real Network:

- Re-survey coverage and signal strength across every space
- Test roaming by walking calls and sessions through the building
- Load-test high-density rooms at real device counts
- Confirm guest, staff, and device networks are truly separated
- Document channels, placement, and settings for the next change

The Goal:

Proof that the wireless performs the way it was designed to — measured, not assumed.

9. Wireless Must Support the Business

Wi-Fi succeeds when work gets easier — not when the access points are mounted.

Keep Wireless Aligned With:

- How and where your people actually work
- The applications the business runs on
- Security and compliance obligations
- Growth — new space, more devices, another site

The Goal:

A wireless network people stop thinking about, because it simply works everywhere they go.

The Final Word

Reliable business Wi-Fi isn't a product you buy. It's a design you commit to — survey the space, size for real load, place access points deliberately, segment the traffic, and prove it after install.

Businesses that plan wireless this way get coverage they forget about. The rest keep buying more access points to fix a problem that was never measured.

Next Step:

Walk your worst dead zone and ask three questions: what's it built of, how many devices need it, and has anyone ever surveyed it? If the answer to the last one is no, that's where good Wi-Fi starts. QOS MSP runs the site survey, designs the coverage, and secures the network — for businesses across Indianapolis and Indiana.