The Construction IT Readiness Checklist

15 questions every construction firm in Western Pennsylvania and Northeast Ohio should be able to answer about its technology. Each has a Green, Yellow, and Red answer and one next step. Allow about 15 minutes.

HOW TO USE THIS SHEET

Every question has three answers. Tick the box beside the one that matches your business today: Green means you are in good shape, Yellow is worth fixing soon, and Red should be addressed first.

When you have answered all 15 questions, count the ticks of each color, write the totals on the Score yourself page, and fill in the action plan on the last page.

1. Project files: drawings, models, and submittals

These four questions cover where the latest drawings live, who can open them, and how you recover a file that was overwritten.

Q1. Is there a single spot everyone goes to for the latest drawings, models, and submittals?

- ☐ GREEN — One platform is the system of record (Procore, Autodesk Construction Cloud, Newforma, Trimble Connect, or even a tightly run SharePoint). Field and office both open files from there, never from email or a personal folder.
- ☐ YELLOW — A shared folder is the official location, but PDFs and CAD files still get emailed between the PM and the foreman.
- ☐ RED — Drawings travel by email. Two foremen are looking at different revisions on Tuesday morning.

Next step: Pick one platform that fits how you work and stop sharing project files by email within 90 days. Most of the work is the migration.

Q2. Are the big project files (drawings, models, photos, drone footage) backed up in a way that does not slow the office down?

- [ ] GREEN — Backups run in the background and only ship the files that changed, so a nightly run is a few gigabytes, not the whole project.
- [ ] YELLOW — Full backup of every file every night. Sometimes the backup is still running when staff arrive.
- [ ] RED — No off-site backup of the project server, or the backup is on the same NAS as the source.

Next step: A modern backup tool (Veeam, Datto, MSP360) only sends the changed parts of a file, so the office connection is not saturated. Add an off-site or cloud copy with a quarterly restore test.

Q3. Do subcontractors and consultants get scoped access instead of full project access?

- [ ] GREEN — Per-discipline roles. The MEP sub can read structural but not edit it; the architect can publish but cannot delete history.
- [ ] YELLOW — Everyone is a project admin because permission tickets pile up.
- [ ] RED — You hand over a shared link to the entire project to anyone who asks.

Next step: Spend an afternoon defining roles by discipline, archive old subs the day they finish, and audit the access list quarterly.

Q4. When a project file is corrupted or overwritten, do you have version history that lets you roll back at least a week?

- [ ] GREEN — Whatever platform holds your drawings or models keeps publish history for the project lifetime, plus a separate local backup of the working files every few hours.
- [ ] YELLOW — Last night's backup exists. Anything older is gone.
- [ ] RED — You restore from whatever someone last emailed.

Next step: Confirm the publish-history retention on the platform you use. Pair it with local hourly snapshots so you have two recovery paths.

2. Mobile workforce and field devices

Your team works from trucks, trailers, and active sites. These three questions cover the devices that leave the office and the data on them.

Q5. Is every laptop, tablet, and phone enrolled in MDM (Intune, Jamf, Kandji)?

- [ ] GREEN — Auto-enroll on first boot via Apple Business Manager or Windows Autopilot. Lost devices wipe with one click.
- [ ] YELLOW — Most laptops are enrolled, foreman tablets are not. Personal phones with the Procore app have no policy at all.
- [ ] RED — You discover an ex-employee still has a company laptop two weeks after termination.

Next step: Buy MDM seats for every device that touches company data. Budget roughly $4 to $10 per device per month.

Q6. Is full-disk encryption turned on for every laptop, with a recovery key saved somewhere central?

- [ ] GREEN — BitLocker (Windows) or FileVault (Mac) is on for every laptop. Recovery keys are in your MDM, not on a sticky note.
- [ ] YELLOW — On most laptops, but no central record of recovery keys. A lost laptop is unrecoverable, but probably also unreadable.
- [ ] RED — Off, or unknown. Anyone who finds a laptop left in a truck can read what is on it.

Next step: A single MDM policy turns this on and saves the recovery key automatically.

Q7. Do field crews have offline-capable apps for spotty cellular zones (parking garages, rural sites, basements)?

- ☐ GREEN — Procore, PlanGrid, Bluebeam, and Microsoft 365 are configured for offline use. Crews keep working through dead zones.
- ☐ YELLOW — Apps work but require a connection to load drawings. The foreman has to drive a quarter mile to download.
- ☐ RED — Web-only tools. No connection equals no work.

Next step: Verify offline mode is enabled per app. Train crews to sync before they drive into a known dead zone.

3. Project management and AP/AR

These four questions cover the systems that run the job and move the money.

Q8. Is there one platform that runs the project (Procore, ACC, Buildertrend, Sage 300, Foundation), or three spreadsheets?

- ☐ GREEN — A single PM platform integrated to accounting. Field-to-office data flows without copy-paste.
- ☐ YELLOW — A platform exists but spreadsheets are still the source of truth for half the team.
- ☐ RED — Spreadsheets, email threads, and a whiteboard.

Next step: Pick the platform, then retire the spreadsheets within 90 days. Expect the rollout to take more effort than the purchase.

Q9. Are wire transfers and large vendor payments protected against business email compromise (BEC)?

- ☐ GREEN — Dual approval on every wire over a defined threshold, callback verification to a known-good number for any new bank-info request, and no payment-detail changes accepted via email alone.
- ☐ YELLOW — Single approver. An emailed request to change a vendor's bank details sometimes gets acted on without a callback.
- ☐ RED — AP processes wires from emailed PDFs with no second check.

Next step: Write down the callback rule and post it at every AP desk.

Q10. Are change orders and AR aging tracked automatically, instead of living in one person's head?

- ☐ GREEN — Change orders flow from the PM platform straight into the AR aging report. The CFO sees overdue receivables Monday morning without asking.
- ☐ YELLOW — Tracked, but reconciliation is manual and happens once a month.
- ☐ RED — Change orders get billed when someone remembers them, and cash flow is a surprise most months.

Next step: Configure your accounting integration so change orders cannot leave the PM platform without a billing record.

Q11. When a new sub or vendor comes on, is there a short checklist for setting up their access (and shutting it off later)?

- ☐ GREEN — A one-page packet creates the right portal accounts on day one, and revokes them automatically when the project closes.
- ☐ YELLOW — Onboarding is informal. Subs from a project two years ago still have a login somewhere.
- ☐ RED — No process. Anybody who asked has access.

Next step: Write the one-page checklist this week: portal accounts, document access, project close-out revocation. Use it for every sub.

4. Cybersecurity

These four questions cover sign-in, endpoint protection, backups, and staff training.

Q12. Is multi-factor authentication enforced on email, ERP, banking, and every cloud service?

- [ ] GREEN — MFA enforced everywhere, phishing-resistant where possible (passkeys, FIDO2, number-matching). No SMS-only on admin accounts.
- [ ] YELLOW — MFA on email but not on Procore, banking, or the GPS tracking platform.
- [ ] RED — Password-only login on critical systems.

Next step: Turn MFA on everywhere this month, starting with email, banking, and admin accounts.

Q13. Is EDR (not just legacy AV) on every endpoint with someone watching alerts?

- [ ] GREEN — Managed EDR (Huntress, SentinelOne, CrowdStrike, Defender for Business plus a SOC) on 100% of endpoints, including jobsite trailers.
- [ ] YELLOW — Defender is on but no one reviews the alerts.
- [ ] RED — Built-in AV only, or some machines have nothing.

Next step: Inventory every endpoint and confirm modern EDR plus a human on the alerts. Check the PCs in jobsite trailers, which are easy to miss.

Q14. Do you have backups that follow 3-2-1 (three copies, two media, one off-site or immutable)?

- [ ] GREEN — Production data, file servers, model server, and accounting all backed up to a second medium and an immutable off-site target. Quarterly restore test.
- [ ] YELLOW — Backups exist on a second NAS in the same office.
- [ ] RED — No off-site backup, or backups have not been restored in over a year.

Next step: Add an immutable cloud destination with object lock. Schedule a quarterly restore drill and put it on the calendar like a safety meeting.

Q15. Has your team had phishing-awareness training in the last 12 months, with simulated phishes?

- [ ] GREEN — KnowBe4, Hoxhunt, Wizer, or Curricula. Monthly five-minute lessons plus a quarterly simulated phish. Click rate trends down.
- [ ] YELLOW — One-time training at hire.
- [ ] RED — No training. AP receives phishing emails and nobody has shown them what to look for.

Next step: Start a training program that takes each employee about five minutes a month, and track the click rate on the simulated phishes.

Score yourself

Count how many of each color you ticked across the 15 questions and write the totals in the boxes. Then tick the band that matches your result.

GREEN	YELLOW	RED
_____	_____	_____
out of 15	out of 15	out of 15

- [ ] **13 or more Green:** you are in good shape. Keep it that way with quarterly restore tests, monthly patching, and a monthly state-of-IT report.

- [ ] **8 to 12 Green:** the basics are mostly there. Pick your three most serious Yellows and close them within 90 days.

- [ ] **Under 8 Green, or any Red on Q1, Q9, Q12, or Q14:** fix any Red on those four questions first, then the rest of your Reds, then the Yellows.

A Red on Q1, Q9, Q12, or Q14 puts the whole result in the Red band, however many Greens you have.

Action plan

Write down the five things you will fix first. Start with any Red on a critical question (Q1, Q9, Q12, or Q14), then your other Reds, then your Yellows. Use the next step printed under each question as the starting point.

PRIORITY	WHAT TO FIX	WHO OWNS IT	TARGET DATE	DONE
1				☐
2				☐
3				☐
4				☐
5				☐

Get a second opinion

KawaConnect offers a free IT readiness call to construction firms in Western Pennsylvania and Northeast Ohio. Walk us through your answers and we will tell you what we would fix first and roughly what it costs. For ongoing help, see our managed IT service (kawaconnect.com/managed-it/) and networking and firewall work (kawaconnect.com/networking-firewalls/).

Book a free readiness call: kawaconnect.com/contact/ | sales@kawaconnect.com | (412) 556-7007