



FREE RESOURCE · VERSION 1.0

# The Construction IT Readiness Checklist

17 questions every Pittsburgh, Cleveland, and Tri-State construction firm should be able to answer about their technology, with a red, yellow, and green rubric and the single next step to take for each one.

**~20 minutes**  
to complete

**17 questions**  
across 4 domains

**Scored**  
so you know what to fix first

## HOW THE RUBRIC WORKS

For every question you will see three answer bands. Mark the one that matches your business today.

**Green: you are in good shape**

**Yellow: worth fixing soon**

**Red: address this first**

KawaConnect is an IT consulting firm serving Pittsburgh, Cleveland, and the Tri-State area. Questions? Call **(412) 556-7007** or email [support@kawaconnect.com](mailto:support@kawaconnect.com). No sales pitch inside.

# 1. Project files: drawings, models, and submittals

---

Where do the latest drawings actually live, and who can roll back when something gets clobbered? These four questions separate firms that lose a day to "which version are we on" from firms that don't.

## 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 "official" but PDFs and CAD files still get emailed around 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 commit to retiring email-as-a-file-share within 90 days. The migration is the hard part; the daily flow becomes obvious.

## 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 actually 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 isn't saturated. Add an off-site or cloud copy with a quarterly restore test.

## Q3. Do subcontractors and consultants get scoped access (their own model space or document set) 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 OneDrive 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, 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

---

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

**Green** Auto-enroll on first boot via Apple Business Manager / 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. Costs \$4-\$10 per device per month; saves you from one breach.

#### 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. A lost laptop in the truck is a data breach.

---

**Next step:** A single MDM policy turns this on and saves the recovery key automatically. No excuse for not having this in 2026.

### 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. 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 you drive in" when entering a known dead zone.

## 3. Project management and AP/AR

---

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

**Green** 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 commit to retiring the spreadsheets within 90 days. The cost is sunk; the friction is the rollout.

### 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, no payment-detail changes accepted via email alone.

**Yellow** Single approver. Vendor emails saying "our bank changed" sometimes get acted on without a callback.

**Red** AP processes wires from emailed PDFs. Has happened, will happen again.

---

**Next step:** Construction is in the top three industries targeted by BEC. Document the callback rule and put it next to every AP keyboard.

#### 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. Cash flow surprises monthly.

---

**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 and multi-state compliance

---

#### 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:** MFA is the single highest-ROI security control. Construction is in CISA's ransomware top-three. Turn it on everywhere this month.

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

- Green** Managed EDR (Huntress, SentinelOne, CrowdStrike, Defender for Business + SOC) on 100% of endpoints including jobsite trailers.
- Yellow** Defender is on but no one reviews 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. Trailer PCs are often the forgotten ones.

### 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 quarterly simulated phish. Click rate trends down.
- Yellow** One-time training at hire.
- Red** No training. AP gets a phishing email a week, opens 10% of them.

---

**Next step:** Phishing-awareness is the cheapest security control with measurable ROI. Five minutes a month per employee.

**Q16. Are you maintaining OSHA recordkeeping correctly, including state-specific filings (Pennsylvania, Ohio)?**

**Green** OSHA 300/300A/301 logs current; electronic submission in March on schedule; state-specific fields tracked.

**Yellow** Logs exist but submission is "I think we filed it."

**Red** No logs, or logs maintained on a paper clipboard nobody finds.

---

**Next step:** Most accounting/HR platforms can export OSHA forms automatically. Confirm yours does, then put the March submission on the controller's recurring calendar.

**Q17. For Ohio non-residential work, are you running E-Verify on every new hire and keeping the records for IT-discoverable audits?**

**Green** E-Verify integrated with onboarding software. Records archived in HRIS with retention policy.

**Yellow** E-Verify run manually, paper records in HR.

**Red** Not running E-Verify on Ohio commercial sites.

---

**Next step:** Ohio's 2025+ E-Verify mandate has teeth. Talk to your HR provider about automating it through onboarding.

## Score yourself

---

Count how many of each color you marked across the 17 questions. Rough interpretation below. It is a starting point, not a verdict.

 Green answers

 Yellow answers

 Red answers

**17**  
Total questions

**14+ Green:** you are running a tight operation. The risk now is drift: enforce the cadence (quarterly restore tests, monthly patching, monthly state-of-IT report).

**9-13 Green:** the basics are mostly there. Your three biggest Yellows are likely your three biggest risks. Close them in 90 days.

**Under 9 Green, or any Red on Q1, Q9, Q12, or Q14:** you have an exposure that turns a routine day into a company-ending event. Treat these as priority one.

### Want a second pair of eyes?

KawaConnect runs construction-IT readiness calls free, no pitch. We currently support firms across Pittsburgh, Cleveland, and the Tri-State (TRE Construction is a long-standing client). Walk us through your answers, we point out what we would fix first and roughly what it costs. No slides, no contract, no follow-up unless you ask.

**Call** (412) 556-7007 · **Email** [support@kawaconnect.com](mailto:support@kawaconnect.com) · **Web** [kawaconnect.kawalink.us](http://kawaconnect.kawalink.us)

---

This checklist is provided as-is for self-assessment. It is not a substitute for a formal risk assessment, legal advice, or cyber-insurance underwriting. Product names belong to their respective owners; their mention does not imply endorsement. © 2026 KawaConnect.