



FREE GUIDE · 2026 EDITION

The Complete Guide to Technology for Construction Companies in Scotland

A practical guide for construction directors: site connectivity, cyber security, Cyber Essentials, Microsoft 365, AI and choosing an IT partner.

By Kenny Stevenson, Operations Director · Indigo Unified Communications
Updated September 2026 · indigocomms.co.uk/guides/construction-technology/

Contents

1. Overview

The Complete Guide to Technology for Construction Companies in Scotland

2. **What are the biggest technology challenges for construction companies?**
3. **What does a good IT strategy look like for a construction company?**
4. **How should construction companies protect themselves from cyber attacks?**
5. **What's the best internet for a construction site?**
6. **How can construction companies improve communication between office and site?**
7. **How can construction companies get more from Microsoft 365 and AI?**
8. **How do you choose an IT provider for a construction company?**
9. **Construction technology readiness checklist**

Every chapter is also on our website, where links and sources are kept up to date:
indigocomms.co.uk/guides/construction-technology/

The Complete Guide to Technology for Construction Companies in Scotland

Construction companies in Scotland need technology that works across head office, live sites and mobile teams. Get five things right: one secure place for project documents, reliable connectivity at every site, cyber security that meets tender requirements such as Cyber Essentials, managed devices, and a roadmap that plans investment instead of reacting to failures. This guide explains each one in practical terms for firms with 15 to 100 staff.

Who this guide is for

It's written for owners, managing directors, operations, contracts, commercial and project managers, office managers and finance directors of Scottish construction businesses. That includes housebuilders, commercial contractors, civil engineering firms and specialist subcontractors, typically with 15 to 100 staff.

Why technology matters more than ever in construction

Construction has changed a lot over the last decade. Drawings are shared digitally, health and safety records are completed on tablets, and clients expect real-time updates. Procurement, scheduling and reporting all run on cloud systems. At the same time, cyber attacks have become more targeted. The NCSC says construction firms are targeted because of the sensitive data they hold and the high-value payments they handle, and clients now ask about cyber security before awarding work.

For a construction business, better technology doesn't just mean fewer IT problems. It means fewer project delays, stronger tender submissions, less risk and more productive teams on site and in the office.

What's in this guide

1. **What are the biggest technology challenges for construction companies?** The eight problems we see most often, from site connectivity to AI.
2. **What does a good construction IT strategy look like?** Six pillars, a recommended technology stack and a three-phase roadmap.
3. **How should construction companies protect themselves from cyber attacks?** Why construction is targeted, Cyber Essentials for tenders, and the layers of protection.
4. **What's the best internet for a construction site?** FTTP, leased lines, 5G, failover and site WiFi compared.

5. **How can construction companies improve communication between office and site?** Cloud telephony, Teams and business mobiles.
6. **How can construction companies get more from Microsoft 365 and AI?** Teams, SharePoint, Intune and Copilot in practice.
7. **How do you choose an IT provider for a construction company?** Questions to ask, and signs you've outgrown your provider.
8. **Construction technology readiness checklist** 20 questions to test where you stand.

The guide at a glance

A modern construction technology strategy focuses on:

- Secure collaboration between office and site
- Reliable connectivity wherever projects are delivered
- Cyber security that satisfies clients and tenders
- Efficient communication across teams
- Centrally managed devices
- Practical use of AI and automation
- A long-term roadmap tied to business goals

The biggest misconception we come across

How Indigo does this. Most construction businesses don't need to spend heavily on new technology. Many already have powerful tools in Microsoft 365 that they don't use consistently across office, site and mobile teams. In our experience supporting more than 15 construction businesses, the biggest gains usually come from simplifying systems, connecting the tools you already have and getting people to use them.

Frequently asked questions

How much should IT support cost for a construction company?

Managed IT support is usually priced per user per month. The cost depends on the number of users, the level of support and security, and whether connectivity, phones and mobiles are included. Compare providers on what's included and the outcomes they deliver, not just the monthly figure.

Is Microsoft 365 suitable for construction companies?

Yes. Microsoft 365 Business Premium gives construction firms email, Teams, SharePoint document management with version control, and Intune device management in one subscription. When it's set up properly, office and site teams work from the same up-to-date drawings and records, and lost devices can be wiped remotely.

Should our construction business get Cyber Essentials?

For most construction businesses, yes. Cyber Essentials is required for central government contracts that handle personal data or OFFICIAL information (PPN 09/23), and it's increasingly asked for by local authorities, housing associations and principal contractors. The NCSC reports that organisations with Cyber Essentials are 92% less likely to claim on their cyber insurance.

What's the best internet connection for a construction site?

It depends on the site's location, how long the project runs and how many people work there. Most sites start with a 5G or 4G router, which can be live within days, and long projects add a fixed line with the mobile router kept as automatic backup. Head offices usually suit full fibre or a leased line.

Should we have one supplier for all our technology?

Many construction companies benefit from one partner covering IT support, Microsoft 365, cyber security, connectivity, telephony and mobiles. It removes the finger-pointing between suppliers when something fails and keeps every decision aligned to one roadmap. Check that the partner has real expertise in each area, not just a price list.

Where to start

Start with a structured review of your current setup. It shows immediate risks, quick wins and longer-term improvements before you commit to new systems or suppliers. [Book a free Construction Technology Assessment](#) →

What are the biggest technology challenges for construction companies?

The eight technology challenges we see most in Scottish construction companies are: communication between site and office, poor site connectivity, cyber security risk, unmanaged mobile devices, document version control, rising technology costs, technology that can't keep up with growth, and uncertainty about AI. They usually share one cause: technology that's been added piece by piece over the years instead of planned.

1. Communication between site and office

When site managers, engineers, quantity surveyors and office teams aren't working from the same information, mistakes happen. Drawings and revisions are shared late, people use different messaging apps, and important decisions sit in someone's personal inbox. The result is rework, delay and cost.

Best practice: one collaboration platform (usually Microsoft Teams and SharePoint) where project documents, conversations and meetings are available to the right people, on site or in the office.

2. Poor connectivity on construction sites

Temporary compounds often have no fixed line, so teams fall back on phone hotspots. When that happens, cloud apps become unusable, video calls fail, drawings don't sync and health and safety paperwork is delayed.

Best practice: every site gets a connectivity plan covering the main connection, automatic failover, secure WiFi, secure remote access and room to grow. See Chapter 4.

3. Cyber security is now a business risk

Construction firms hold tender documents, contracts, drawings, staff records and supplier bank details, and they make large payments. That makes them attractive to criminals, particularly for invoice fraud. An attack can mean project delays, financial loss, contract disputes and lost tenders, and clients increasingly ask for proof of cyber security before awarding work.

Best practice: treat cyber security as part of operational risk management, not only as an IT issue. See Chapter 3.

4. Managing mobile devices

Smartphones, tablets, rugged devices, laptops and shared site devices get lost, fall behind on updates and hold sensitive data. Without central management, security is inconsistent and support is always reactive.

Best practice: every business device is centrally managed, kept up to date, secured and able to be wiped remotely if lost.

5. Document control and version management

Drawings, specifications, RAMS, inspection reports, variations, contracts and certificates all need to be current. When an out-of-date drawing reaches site, the consequences can be serious.

Best practice: structured document management with version control, permissions and secure sharing.

6. Rising technology costs

Over the years, many firms end up with several suppliers, overlapping software subscriptions, separate phone and broadband contracts, and licences nobody uses.

Best practice: review your technology regularly and make full use of what you already pay for before buying more.

7. Supporting business growth

Technology that worked with 20 employees often breaks at 80. Growth exposes weak user management, limited security, ageing hardware and the lack of a roadmap.

Best practice: a three-to-five-year technology roadmap tied to your business plan. See Chapter 2.

8. Artificial intelligence: opportunity or confusion?

We often hear the same questions. Can AI reduce admin? Is Microsoft Copilot worth it? Is it secure? The opportunity is real, but only when AI has clear objectives and sensible rules around it.

Best practice: start with practical uses that save time on repetitive tasks. See Chapter 6.

What these challenges have in common

These problems look different, but they usually have one cause: technology has grown piece by piece, with each system brought in to fix one problem, and nothing ties them together. The most successful construction companies don't necessarily spend more. They invest in technology that's integrated, secure, easy to use and matched to how their teams actually work.

How Indigo does this. We've worked with construction firms that already had Microsoft 365, business mobiles, cloud telephony and modern internet, yet staff still used personal messaging apps and emailed drawing versions back and forth. The fix wasn't new software. We simplified what they had, set up Teams and SharePoint per project, and trained people to use them.

Sources: NCSC, *Cyber Security for Construction Businesses* (2022, now archived) · DSIT, *Cyber Security Breaches Survey 2025/2026* (April 2026).

What does a good IT strategy look like for a construction company?

A good construction IT strategy treats technology as business infrastructure, not a collection of products. It rests on six pillars: secure collaboration, reliable connectivity everywhere, cyber security as standard, standardised devices, communication without barriers, and strategic planning. It's delivered in three phases, stabilise, modernise and optimise, so disruption stays low and every investment shows a result.

What makes a construction IT strategy "modern"?

The strongest strategies are secure by design, easy for staff to use, reliable on every site, able to scale as the business grows, built around collaboration, backed by clear policies and reviewed regularly. You wouldn't build a project without proper foundations, and the same goes for your technology.

The six pillars of a construction technology strategy

1. Secure collaboration

Drawings, contracts, RAMS, health and safety records, reports, variations and certificates must reach the right people while staying secure. That means version control, permission-based access, mobile access, Teams integration and automatic cloud backup. The aim isn't just storing files. It's making sure everyone works from the latest version.

2. Reliable connectivity everywhere

Office resilience, temporary site connectivity, remote access, guest WiFi, secure VPN or zero-trust access, automatic failover and mobile data. Construction rarely happens in one place, so your connectivity can't be built for one place either.

3. Cyber security as standard

Multi-factor authentication, endpoint protection, email security, managed detection and response, regular updates, backup and disaster recovery, awareness training, device encryption and conditional access. Done well, it also strengthens tender submissions.

4. Standardised devices

A standard set of laptops and phones means faster deployment, easier support, better security and simpler buying. With cloud device management, new devices are configured before they reach the employee.

5. Communication without barriers

Business telephony, Teams, mobiles, video, messaging, presence, call recording where needed, and shared directories, all on one consistent platform.

6. Strategic IT planning

A roadmap covering growth, security improvements, device replacement cycles, Microsoft 365 adoption, AI, connectivity upgrades, compliance, disaster recovery and budget forecasting.

What technology stack do we recommend for construction companies?

Business need	Recommended approach
Productivity	Microsoft 365 Business Premium
Collaboration	Microsoft Teams and SharePoint
File storage	SharePoint and OneDrive
Device management	Microsoft Intune
Cyber security	Microsoft Defender or equivalent endpoint protection, with managed detection and response
Connectivity	Business FTTP, leased line, or 5G for temporary sites
Communication	Cloud telephony and business mobiles
Backup	Microsoft 365 backup and a business continuity plan
AI	Microsoft Copilot where there's a clear use case
Planning	Regular technology reviews and virtual-CIO guidance

The specific products matter less than making every decision part of one integrated strategy.

Signs your IT strategy needs reviewing

- Staff regularly complain about slow systems
- Several versions of the same drawing are in circulation
- Site teams struggle to access information
- Different departments use different tools
- Internet outages regularly affect work
- Cyber security only gets discussed after an incident
- There's no documented disaster recovery plan
- Nobody has reviewed your technology in the last two years
- Several suppliers, and nobody owns the whole picture
- Technology decisions are reactive, not planned

How to build a technology roadmap in three phases

1. **Stabilise.** Fix recurring issues, improve reliability, standardise devices and strengthen security.
2. **Modernise.** Move to cloud collaboration, improve communication, roll out central device management and upgrade connectivity.
3. **Optimise.** Introduce automation, improve reporting, explore AI, increase adoption and refine processes.

How Indigo does this. One of the most common mistakes we see is solving one problem without looking at the whole picture. A new phone system won't improve communication if documents are still hard to find, and faster internet won't help if staff are working from old file versions. We start every engagement by understanding how your people work and where delays happen, then build the roadmap around that.

Sources: Microsoft, *Microsoft 365 Business Premium* service description · NCSC, *Cyber Essentials: Requirements for IT infrastructure*.

How should construction companies protect themselves from cyber attacks?

Construction companies should protect themselves with layers: multi-factor authentication on every account, centrally managed and encrypted devices, email filtering against phishing and invoice fraud, tested backups, 24/7 monitoring and regular staff training. They should also get Cyber Essentials, which is required for some government contracts and increasingly requested in construction tenders. Getting the basics right consistently removes most of the risk.

Why are construction companies targeted?

The NCSC says construction businesses of all sizes are targeted because of the sensitive data they hold and the high-value payments they handle. That data includes tender submissions, contracts, financial records, drawings, health and safety documents, staff data and supplier bank details. Mobile working, temporary sites and subcontractor access add further gaps. Across all UK businesses, 43% reported a breach or attack in the last 12 months, and phishing was by far the most common (38%) (Cyber Security Breaches Survey 2026).

What does a cyber attack actually cost a construction business?

The ransom is rarely the biggest cost. Inaccessible drawings, lost project records, payroll and invoicing stopped, customer data stolen, payment fraud, contract disputes and reputational damage can hit several live projects at once. A few hours of downtime can cost far more than recovering the systems.

Is Cyber Essentials a tender requirement?

Increasingly, yes. Under PPN 09/23, suppliers to central government must hold Cyber Essentials where a contract involves citizens' personal data, government staff data or OFFICIAL information. Local authorities, housing associations, healthcare bodies, utilities and large principal contractors now ask about cyber security in PQs and supplier assessments too.

Cyber Essentials covers five controls: firewalls, secure configuration, user access control, malware protection and software updates. Beyond tenders, it helps with cyber insurance: the NCSC reports certified organisations are 92% less likely to make a claim. Uptake is growing, with 61,430 certificates issued in the year to June 2026, but only 5% of UK businesses hold it (Cyber Security Breaches Survey 2026). Holding it still helps a firm stand out.

The layers of protection every construction company needs

Identity protection

Multi-factor authentication, strong password policies, conditional access and identity monitoring. Only 47% of UK businesses use two-factor authentication (Cyber Security Breaches Survey 2026), so this is the single biggest quick win.

Device security

Every laptop, desktop and phone should be encrypted, updated, centrally managed, running endpoint protection and monitored.

Email security

Filtering against phishing, business email compromise, malicious attachments and links, and impersonation. Finance teams should confirm any change to bank details by phone.

Data protection

Project information stored securely, with access controls, automatic backup, tested recovery and protection against accidental deletion.

Monitoring and response

Continuous monitoring, ideally a 24/7 security operations centre, spots unusual activity and stops it before it becomes an incident.

People

Regular awareness training helps staff recognise suspicious emails, fraud attempts, password risks, social engineering and unsafe file sharing.

What does good look like?

A well-protected construction company can answer "yes" to all of these:

- Are all business devices centrally managed?
- Is multi-factor authentication enabled for every user?
- Are backups tested?
- Can lost laptops be remotely secured?
- Are updates applied automatically?
- Do staff get security training at least yearly?
- Is there a documented incident response plan?
- Have security controls been reviewed in the last 12 months?
- Are you working towards or maintaining Cyber Essentials?

Cyber security isn't a one-off project. Threats change, staff come and go, and projects start and finish, so it needs regular review.

How Indigo does this. Indigo holds Cyber Essentials Plus and ISO 27001:2022 ourselves, and every client gets endpoint detection and response, email filtering, Microsoft 365 security settings and backup as standard, and our Platinum package adds a 24/7 security operations centre watching for threats. We take construction clients through Cyber Essentials certification, usually starting with multi-factor authentication, device management and access reviews. Those fundamentals remove most of the risk before any advanced tools are needed.

Sources: DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026 · Cabinet Office, *PPN 09/23: Updates to the Cyber Essentials Scheme* · NCSC, *Cyber Security for Construction Businesses* (2022) · Infosecurity Magazine, *Cyber Essentials Has Record Year*, 17 September 2026.

What's the best internet for a construction site?

For most construction sites, the best internet is a 5G or 4G router that can be live within days, upgraded to a fixed line for long projects, with the mobile connection kept as automatic backup. Head offices usually suit full fibre (FTTP) or a leased line. The right choice depends on location, project length, number of users and how much downtime you can accept, so check coverage before committing.

Every construction site is different

A construction business may have a head office, several live sites, temporary compounds, home workers, engineers on the road and subcontractors needing guest access. The aim is the same experience everywhere: the same systems, the same security, wherever someone is working.

Which connection should you choose?

Connection	Best for	Why
Full fibre (FTTP)	Head office, permanent and regional offices	High speed at low cost. Full fibre now reaches 71% of Scottish premises (Ofcom, 2025)
Leased line	Head offices, multi-site firms, heavy cloud use	Dedicated bandwidth, the same upload and download speeds, and a guaranteed fix time
5G / 4G	Temporary site offices, short projects, backup	Live in days, with no wait for fixed-line installation
Resilient failover	Anywhere downtime is unacceptable	Dual lines, multiple carriers, mobile backup and SD-WAN, so one connection takes over when another fails

Check mobile coverage at the exact site before relying on 4G or 5G. Scotland has the lowest 4G coverage by area of any UK nation, although 5G is available outside 77% of premises (Ofcom, 2025). External antennas and choosing the right network make a big difference.

How to set up site WiFi properly

Poor wireless coverage affects tablets, laptops, phones, CCTV, printers, meeting rooms and visitors. A well-designed site network has reliable coverage, secure sign-in, separate guest access, seamless roaming between access points, performance monitoring and room to grow. WiFi should be designed, not just installed.

How do you connect every site together?

SD-WAN and modern secure networking connect offices and compounds as one network, apply the same security policies everywhere, prioritise critical applications and let you monitor performance from one place.

Plan for the unexpected

Ask yourself:

- What happens if the office internet fails?
- How quickly can a new site be brought online?
- Can staff keep working remotely?
- Is failover automatic?
- Can critical systems be reached from another location?

Business continuity belongs in every connectivity plan. Future site technology, such as smart CCTV, IoT sensors, connected plant, digital inspections and real-time reporting, all depends on reliable connectivity.

How Indigo does this. The most common mistake we see is choosing connectivity on price alone. We ask clients to work out what losing connectivity for an hour costs, not just the monthly line rental. For new compounds, we usually deploy a managed 5G router within 2-3 working days, order a fixed line if the project is long enough, and keep the 5G unit as automatic failover. Every connection we manage is monitored 24/7.

Sources: Ofcom, *Connected Nations: Nations report 2025* (Scotland), 19 November 2025.

How can construction companies improve communication between office and site?

Construction companies improve office-to-site communication by bringing voice, video, messaging and mobiles onto one platform, usually a cloud phone system integrated with Microsoft Teams, so calls reach site managers wherever they are. Business mobiles should be bought centrally, on the network with the best coverage at your sites, and managed through mobile device management so lost phones can be wiped.

What modern business communication looks like

Your workforce expects to use voice, video, instant messaging, mobiles, Teams, presence and screen sharing. Running these as separate systems causes missed calls and slow decisions. Bringing them together means faster decisions, fewer missed calls, better collaboration, better customer service and simpler management.

Choosing a phone system for a construction company

Cloud phone systems let the office number ring on a desk phone, in Teams or on a site manager's mobile. They support call queues and out-of-hours routing, plus call recording where it's needed. Common platforms include 8x8, 3CX and Microsoft Teams Phone. The UK's copper phone network is being switched off by 31 January 2027, so any firm still on analogue lines or ISDN needs to plan a move.

Managing business mobiles in construction

A modern mobile strategy includes central buying, device lifecycle management, security policies, mobile device management (MDM), usage monitoring, cost control and lost-device protection. For site teams, rugged phones and tablets survive dust, water and drops. Treat mobiles as business-critical equipment, not just company phones.

What better office-to-site communication delivers

- Faster decisions
- Drawings reach site sooner
- Fewer delays
- Queries resolved faster
- Better updates for clients
- Projects kept on schedule

How Indigo does this. We supply business mobiles on EE, O2 and Vodafone and choose the network by checking coverage at your sites. Every device is enrolled in Microsoft Intune, and rugged handsets are available for site teams. On the phone system side we support 8x8, 3CX and Teams Phone, so we recommend the platform that fits rather than the one we sell.

Sources: Ofcom, *Connected Nations: Nations report 2025* · Openreach, *Time for a big switch-up as PSTN switch-off looms*, 5 February 2026.

How can construction companies get more from Microsoft 365 and AI?

Most construction companies already pay for Microsoft 365 but use little beyond email and Office. The biggest gains come from setting up Teams workspaces per project, storing drawings and records in SharePoint with version control, managing devices with Intune and automating approvals. Once that foundation is in place, Microsoft Copilot can cut time spent on meeting notes, site reports and document drafting, with clear usage rules and a person reviewing the output.

Why Microsoft 365 is more than email

For a construction company, Microsoft 365 is a secure workspace where office staff, project managers and site teams work together from anywhere. Rather than replacing every other system, it becomes the platform that ties them together.

How construction companies use each Microsoft 365 tool

Microsoft Teams

A workspace for each project, client, department, health and safety and the board, holding conversations, drawings, meeting notes, documents, tasks, calendars and video calls. Project information stops living in email chains.

SharePoint

Structured document management with version control, permissions, secure sharing, metadata and search, linked to Teams and backed up automatically. It's the answer to "which drawing is current?"

OneDrive

Personal working files with syncing, recovery and secure sharing. Personal work stays in OneDrive, and shared project documents live in SharePoint.

Microsoft Intune

Central management of laptops, tablets, phones, shared devices and home-working kit: security policies, software deployment, encryption, remote wipe and compliance checks. New devices are configured before they arrive.

Automation

Approval workflows, repetitive data entry, paper forms, notifications and document approvals can be automated with Power Automate. Small savings repeated hundreds of times a month add up.

How can construction companies use AI and Microsoft Copilot?

Copilot works inside the Microsoft 365 apps your people already use. Practical uses in construction:

- **Meetings:** summaries, actions and follow-up notes, instead of writing minutes by hand
- **Documents:** first drafts of site reports, project updates, method statements, risk assessments and client letters, always reviewed by a competent person
- **Information:** finding documents, summarising long reports, comparing versions and highlighting actions
- **Decisions:** a quick view of outstanding actions, project status, risks and client requests

How to use AI responsibly

Consider data security, information governance, training, an acceptable use policy, human review of anything AI produces, and client confidentiality. AI should support professional judgement, not replace it.

How to measure success

Less time spent searching for documents, faster onboarding, better office-to-site collaboration, fewer support requests, higher adoption, less manual admin and happier staff.

How Indigo does this. Before anyone buys more software, we review how well a business uses the Microsoft 365 it already has. Many construction firms still rely on email attachments, shared network drives and manual processes because Teams and SharePoint were never set up properly. Indigo is a Microsoft Solutions Partner with more than 100 Microsoft 365 migrations completed, and fixing adoption usually pays back faster than a new standalone application.

Sources: Microsoft, *Microsoft 365 Copilot overview* (learn.microsoft.com) · Microsoft, *Microsoft Intune documentation*.

How do you choose an IT provider for a construction company?

Choose a provider that has construction experience and can show case studies, gives strategic advice as well as support, builds security into everything, can manage IT, connectivity, phones and mobiles together, publishes its response times, can scale with you and explains things clearly. Compare value and outcomes, not just the monthly price, and ask each provider the ten questions below before you sign.

Seven things to look for

1. Construction experience

Temporary compounds, engineers across multiple sites, large drawing sets, commercially sensitive designs and lots of mobile devices are problems office-only providers rarely see. Ask for construction case studies and references from firms your size.

2. Strategic advice, not just a helpdesk

Look for annual roadmaps, budget planning, security reviews, Microsoft 365 optimisation, AI readiness, device lifecycle planning and connectivity reviews.

3. Security built in

Ask how they protect Microsoft 365, what happens if you suffer an attack, whether monitoring is proactive, how backups work, whether they can help you achieve Cyber Essentials and how they manage mobiles. Check whether they hold Cyber Essentials Plus and ISO 27001 themselves.

4. One supplier or several?

Separate companies for IT, internet, phones, mobiles, WiFi and security create complexity, and each blames another when something breaks. One partner who manages the lot, with real expertise in each area, simplifies support and accountability.

5. Responsiveness

Ask for their average first response time and their SLA by priority. Ask who answers the phone, whether you'll have an account manager and how often your technology will be reviewed.

6. Room to grow

They should support new offices, extra sites, more staff, acquisitions, cloud migration, AI and rising security requirements.

7. Value, not just price

Compare experience, response times, security, strategic advice, what's included, customer satisfaction and industry knowledge. The cheapest provider is rarely the best value.

Ten questions to ask an IT provider

1. What experience do you have supporting construction companies?
2. How do you help businesses improve productivity?
3. How do you measure success?
4. How will you support our growth?
5. What cyber security services are included?
6. How do you protect Microsoft 365?
7. What happens if our internet connection fails?
8. Can you manage our mobiles, connectivity and telephony too?
9. How often will you review our technology strategy?
10. What does success look like after 12 months?

Signs you've outgrown your current IT provider

- They only contact you when there's a problem
- Your technology is never reviewed strategically
- Security advice only comes after an incident
- You regularly chase ticket updates
- Suppliers blame each other when things go wrong
- There's no roadmap
- Staff keep hitting the same problems
- They don't understand construction

How Indigo does this. Here are our answers to the questions above. We support more than 15 construction businesses. Our average first response is under 30 minutes (28 minutes in August 2026, with 63% of tickets resolved within two hours). We hold Cyber Essentials Plus and ISO 27001:2022, keep 95% of our clients and score 4.98/5 for satisfaction. We manage IT, connectivity, phones and mobiles from one Glasgow team, and we start with how your business works, not a product list.

Sources: DSIT, *Cyber Security Breaches Survey 2025/2026* · Indigo service desk data, August 2026.

Construction technology readiness checklist

Answer these 20 questions to see how ready your construction company's technology is. They cover strategy, productivity, cyber security, connectivity, communications and AI. If you answer "no" to three or more, there are likely to be quick wins in productivity and security. If you answer "no" to any cyber security question, that area should come first.

Strategy

- Do we have a documented technology roadmap?
- Is our technology reviewed at least yearly?
- Does our technology support our growth plans?

Productivity

- Can office and site teams collaborate easily?
- Are project documents managed centrally with version control?
- Are staff making full use of Microsoft 365?

Cyber security

- Is multi-factor authentication enabled for every user?
- Are all devices centrally managed?
- Are backups tested?
- Do staff receive cyber awareness training?
- Have we achieved, or planned for, Cyber Essentials?
- Do we have a documented incident response plan?

Connectivity

- Is internet reliable at every location?
- Do we have failover if the main connection fails?
- Is WiFi fit for purpose?
- Can we get a new site online within days?

Communications

- Are business mobiles centrally managed?
- Do our phone, Teams and mobile systems work together?

Artificial intelligence

- Have we identified where AI could save time?
- Do we have an AI acceptable use policy?

What next?

If you answered "no" to several questions, a structured review will show the risks, quick wins and longer-term improvements before you commit to new systems or suppliers. [Book a free Construction Technology Assessment](#) →

Back to: [The Complete Guide to Technology for Construction Companies in Scotland](#)

Talk to Indigo

Indigo Unified Communications provides managed IT support, cyber security, connectivity, phone systems and business mobiles to organisations across Scotland, from offices in Glasgow and Livingston. We hold Cyber Essentials Plus, ISO 27001:2022 and ISO 9001:2015.

Book a free technology assessment: 0141 442 0202 ·
gethelp@indigocomms.co.uk · indigocomms.co.uk/contact/

Indigo Unified Communications is a trading name of Indigo E-Commerce Digital Limited, registered in Scotland, company number SC599200. Information correct at September 2026; this guide is general guidance, not professional advice for your specific situation.