

AI Readiness for Construction Firms: Governance, Data, Security, and Operations for Responsible AI from Preconstruction to the Field

How contractors can find AI already in use, protect bid, owner, subcontractor, and employee data, and adopt AI with rules, evidence, and a person in the loop

Last updated: October 23, 2026 | Prepared by AdvancedBITS

About this guide

This is a framework guide, not a client case study. It describes no client outcomes, and every statistic comes from independent third-party research. It is general information and not legal advice. The legal and contract points summarize published commentary and public sources, and the right answer for your firm depends on your contracts, your states, and your projects, so confirm them with your attorney. AdvancedBITS does not replace your attorney, insurance broker, or compliance advisors. It strengthens the technology foundation beneath your AI use.

Executive takeaway

Construction firms are adopting AI where the paperwork piles up: estimating, bid management, requests for information (RFIs), meeting minutes, daily reports, and pay applications. The risk is not the tools themselves. It is that bid pricing, owner-restricted drawings, subcontractor banking details, and employee records can end up in tools nobody reviewed, under contracts that never contemplated AI.

AI readiness for a contractor means five things: knowing what is in use, knowing which data may go where, setting rules people can follow, keeping a human reviewer on anything that leaves the company, and keeping the evidence to prove it. This guide gives you a seven-domain model, a one-page data rule list, a legal and contract map, four working checklists, and a 90-day roadmap.

The contractors who benefit most from AI will not be the ones who adopt it fastest. They will be the ones who can say, with dates, which tools they use, what data each may touch, who approves new ones, and who checked the output. That is the kind of evidence insurers and owners increasingly ask for.

Nothing here argues against using AI. The research below shows that AI is paying off for contractors that use it. The question is whether your governance has kept pace with your adoption, and the research suggests many have not yet.

On this page: [Where construction stands on AI and governance](#) | [Where AI shows up in a construction company](#) | [The seven-domain AI readiness model](#) | [What never goes into an AI tool: the one-page data rule list](#) | [The legal, contract, and standards map for contractors](#) | [Microsoft 365 readiness for AI](#) | [Vendor and platform review: AI inside the software you already use](#) | [AI note-takers and recorded meetings](#) | [The AI acceptable use policy outline](#) | [Match the review to the risk](#) | [Controls for AI agents](#),

[plug-ins, and automation](#) | [Working checklists for AI governance in construction](#) | [A 90-day AI readiness roadmap](#) | [Score your readiness: ten questions](#) | [How AdvancedBITS supports AI readiness for construction firms](#) | [AI readiness for construction firms: frequently asked questions](#)

Where construction stands on AI and governance

Adoption is moving faster than governance, and people are not waiting for approval.

Table 1 summarizes the independent findings behind this guide. The cybersecurity and incident statistics for construction are covered on our construction technology and AI page, so they are not repeated here.

Table 1. AI adoption and governance in construction, by the numbers

Finding	Source	What it means for a contractor
79% of boards have approved AI investments, and 40% have established AI governance policies.	Grant Thornton, 2026 AI Impact Survey, construction and real estate	The gap between approving AI and governing it is wide. Money is moving faster than rules.
27% of architecture, engineering, and construction (AEC) firms use AI for automation, problem-solving, or decision-making. 42% cite data sharing security as a top integration challenge, and 65% invest less than 10% of technology budgets on training.	Bluebeam, 2026 AEC Technology Outlook (1,000+ AEC professionals)	Data security is a top barrier, and training is thin.
38% of commercial specialty contractors report measurable AI results, up from 17%. 24% use AI for cost estimating and 22% for bid management.	ServiceTitan, 2026 Commercial Specialty Contractor Industry Report (1,000+ industry leaders)	AI pays off where bids and cost data live, which is exactly the most sensitive data.
78% of AI users bring their own AI tools to work.	Microsoft and LinkedIn, 2024 Work Trend Index	Informal use is the starting point, not the exception.
Employee use of unapproved shadow AI tripled to 45% in one year.	Verizon, 2026 Data Breach Investigations Report (DBIR) news release	Unapproved use is growing across industries.
63% of breached organizations lacked an AI governance policy. Among those with a policy, fewer than half had an approval process for AI deployments.	IBM, Cost of a Data Breach Report 2025	A policy without an approval path does not control anything.
More than 20% of organizations reported a breach targeting AI models or applications, most often through compromised APIs, apps, or plug-ins (27%) and cloud misconfigurations (27%).	IBM, Cost of a Data Breach Report 2026	Connected tools and plug-ins are part of the risk, not only the chat window.
One in four malicious breaches was AI-enabled, at an average cost of \$6 million versus \$4.99 million overall, mostly deepfake impersonation and AI-enabled malware.	IBM, Cost of a Data Breach Report 2026 (newsroom release)	Convincing fake requests make payment and banking verification more important.

Survey figures are self-reported. The Grant Thornton results cover construction and real estate firms together. The IBM figures describe breached organizations across industries and sizes and are not construction-specific. None of these is an AdvancedBITS client result.

Where AI shows up in a construction company

AI is rarely one tool. It is a set of small habits spread across departments, plus features arriving inside software you already license. Table 2 maps the most common places, what is typically at stake, and the first control to put in place. Use it to guide the discovery work in Table 13.

Table 2. Where AI shows up, and what is at stake

Function	Typical AI use	Data at stake	First control
Estimating and preconstruction	Summarizing bid documents, checking takeoffs, drafting proposals and cost narratives	Unit costs, labor productivity, margins, subcontractor quotes, owner plans and specifications	Approved tools only, and no upload of owner-restricted or licensed design documents without checking the contract
Project management	Drafting RFIs, submittals, change-order narratives, and meeting minutes, and AI note-takers on calls	Owner and subcontractor correspondence, contract terms, project schedules, recorded conversations	Human review of every outgoing document, and consent rules for recorded calls (Table 9)
Field operations and safety	Daily reports and safety talks drafted from a phone, photo and video analysis, site cameras	Site photos, crew names, incident details, worker location or biometric data	Company-approved apps on managed devices, and a written policy for worker monitoring
Accounting and finance	Invoice and pay application processing, cash forecasting, vendor communications	Banking details, lien waivers, bonding and financial statements, pay applications	No AI authority over payments or bank-detail changes, and call-back verification
HR and safety administration	Job posts, resume screening, policy drafting, onboarding	Payroll, I-9s, background checks, injury and medical records	Never in public tools, and human decisions on hiring and discipline
Executives and business development	Email, owner updates, proposals, research on prospects and competitors	Strategy, pricing approach, owner relationships, financial position	Approved tools, and no pooled competitor pricing in shared tools
Software you already own	AI features inside project management, estimating, building information modeling (BIM), accounting, CRM, and meeting platforms	Whatever the software already holds	An inventory of AI features, settings reviewed, and admin controls on

The seven-domain AI readiness model

Readiness is measured across seven domains, and leadership is accountable for all of them. A firm can be strong in one and exposed to another, so score each separately. Table 3 gives the question to ask, the evidence you should be able to show, and the risk if the domain is ignored.

Table 3. The seven readiness domains

Domain	Question to ask	Evidence you can show	Risk if ignored
1. Leadership and accountability	Who owns AI risk, approvals, and the policy?	A named owner, a dated policy, and a regular review	Nobody asks for approval, because nobody owns it
2. Data and information	Do we know which data may go into which tools?	A data rule list (Table 5) that people have seen	Bids, owner files, and employee records end up in unreviewed tools
3. Microsoft 365 and project platforms	Are permissions and sharing ready for AI search?	Site owners, access reviews, and external-sharing rules (Table 7)	AI search surfaces files people should not see
4. Security and identity	Are accounts, devices, email, and payments protected?	Multi-factor authentication (MFA) coverage, endpoint protection, and a funds-transfer verification procedure	A stolen account or fake request reaches the same data AI can reach
5. Vendors and embedded AI	Which vendors and software features use our data with AI?	A vendor review record with AI terms (Table 8)	Data is used for training or shared in ways nobody approved
6. People, training, and human review	Do employees know the rules, and who checks the output?	Training records and named reviewers by use case	Wrong answers reach owners, subcontractors, or the field
7. Contracts and compliance	Do our contracts, licenses, and obligations allow our AI use?	A contract and compliance review (Table 6), with counsel	A breach of a nondisclosure agreement (NDA), license, or federal requirement

A maturity scale to place yourself

Table 4. AI readiness maturity model

Level	What it looks like	First move
1. Unaware	AI use is not tracked, and there is no policy or owner.	Find out what is in use, without blame.
2. Reactive	A policy exists, but it is not enforced or checked, and approvals are informal.	Name an owner, publish the data rules, and start the inventory.
3. Defined	An inventory, an approved list, and role-based rules exist, with training.	Fix Microsoft 365 permissions, review vendors, and add human review rules.
4. Managed	Controls are tested, evidence is current, and reviews happen on a schedule.	Measure pilots and review contracts and vendor terms regularly.
5. Optimized	AI use is measured, improved, and reported to leadership, owners, and insurers with dates.	Expand uses that prove value and retire those that do not.

What never goes into an AI tool: the one-page data rule list

People follow short rules. Print Table 5, review it with each department, and keep it with your AI policy. It sorts construction data into three tiers. The first tier is off limits unless a tool has been approved for that data and your contracts allow it. Counsel and your owner contracts decide the edge cases.

Table 5. What never goes into an AI tool (one page)

Tier	Data	Rule
Never in public or unapproved tools	Owner-restricted plans, specifications, geotechnical reports, and BIM files	Uploading owner-provided files can breach confidentiality terms even if nothing becomes public. Check the contract first.
Never in public or unapproved tools	Architect and engineering design documents	These are usually licensed for use on one specific project. Uploading them to a tool that generates derivative outputs may exceed that license.
Never in public or unapproved tools	Bid numbers, unit costs, labor productivity models, margins, and subcontractor quotes	Uploaded pricing may be stored or used to train a model and may reach competitors who use the same platform.
Never in public or unapproved tools	Federal contract information, Controlled Unclassified Information (CUI), and export-controlled data	Handle only in systems built for it, under your contract. See Table 6.
Never in public or unapproved tools	Employee data: payroll, SSNs, I-9s, background checks, injury and medical records	Human decisions only. No AI screening or discipline decisions without HR and counsel.
Never in public or unapproved tools	Banking and payment data: subcontractor banking forms, wire instructions, credit applications, bonding and financial statements	AI never changes or approves a payment or banking details. Verify by call-back.
Never in public or unapproved tools	Credentials, security settings, claims and dispute files, and privileged legal communications	Keep within systems and people already authorized to hold them.
Approved tools only	Internal meeting recaps, RFI and correspondence drafts, daily report drafts, schedule summaries, and cost narratives built from non-restricted data	Use approved tools, review before anything leaves the company, and follow the recording rules in Table 9.
Fine with review	Public information: published bid results, building code text, product literature, and general research	Verify facts against the source, especially anything that affects safety, code, or cost.

The legal, contract, and standards map for contractors

Most of the risk in contractor AI use comes from contracts and licenses, not from new AI laws. Table 6 summarizes the main areas, what the published commentary says, and the practical action. It is a starting point for a conversation with your attorney, not legal advice, and several points are unsettled.

Table 6. Legal, contract, and standards map

Area	What to know	Practical action
Owner NDAs and confidentiality	Uploading owner-provided geotechnical reports, BIM files, or pricing into an AI tool may breach confidentiality obligations or NDAs and may expose trade secrets if the platform stores or trains on inputs (Bernstein Shur).	Check NDAs and contracts before uploading. Use tools with no-training terms, logging, and project-level data isolation.
Design document licenses and copyright	Architects and engineers typically keep copyright, and standard agreements license the documents for a specific project. Uploading plans or models into an AI tool that generates derivative outputs likely exceeds that license (Bernstein Shur).	Do not upload licensed design documents to general AI tools. Ask the design team and owner before using them in AI workflows.
Bid pricing and antitrust	If competitors upload pricing to a platform that draws on other users, the platform can produce aligned unit prices or markups, which regulators may view as algorithmic bid rigging even without intent (Bernstein Shur).	Keep pricing decisions with people, avoid shared pricing tools without counsel review, and keep records of independent pricing.
Federal work and CUI	Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 applies when covered defense information is involved. It calls for National Institute of Standards and Technology (NIST) SP 800-171 controls and cyber incident reporting, and for external cloud providers that handle that data to meet Federal Risk and Authorization Management Program (FedRAMP) Moderate equivalent requirements (acquisition.gov, as summarized by Cybersecurity Maturity Model Certification (CMMC) advisers).	Keep CUI out of AI tools not approved for it. Treat any cloud AI tool that would touch CUI as a cloud service provider review.
CMMC status	The Department of War suspended CMMC Phase II on July 13, 2026. The Associated General Contractors of America (AGC) notes that the suspension does not remove the obligation to protect federal data, and contractors remain bound by DFARS 252.204-7012.	Do not read the suspension as a pause on safeguarding. Confirm current requirements with your contracting officer and counsel.
Recorded calls and AI note-takers	Several states, including California, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania, and Washington, require all-party consent to record. In re Otter.ai Privacy Litigation and similar suits allege wiretap violations by AI note-takers. The allegations are unproven and the law is unsettled (Haynes and Boone).	Disclose AI note-takers and obtain consent from every participant. See Table 9.
Worker monitoring and biometrics	AI cameras and monitoring can collect biometric and location data, which raises privacy and collective bargaining questions (Lathrop GPM).	Define storage, use, and sharing in policy, and reflect it in owner contracts and subcontracts. Review with counsel before deploying.
Professional responsibility and BIM	AI does not erase the standard of care. Disputes may focus on how AI-supported outputs were reviewed, verified, and used, and on whether a BIM model is a contract document (AAA).	Define in contracts how digital tools may be used and relied on and keep a named reviewer on outputs.
AI-generated outputs and ownership	The U.S. Copyright Office's May 2025 report confirmed that works require human authorship, which raises questions about protection for AI-generated content (Browne Jacobson).	Address ownership and use of AI-assisted deliverables in contracts, with counsel.

Area	What to know	Practical action
Frameworks for your program	NIST publishes the AI Risk Management Framework and a Generative AI Profile (AI 600-1), and the Cybersecurity Framework 2.0 Small Business Quick-Start Guide (SP 1300).	Use them as a common vocabulary for your policy and evidence. They are voluntary guidance, not certifications.

Sources are law firm and industry commentary, plus the DFARS text and Department of War and AGC pages. Where a point rests on commentary, it is attributed. Confirm each point with counsel before relying on it.

Microsoft 365 readiness for AI

For most contractors, Microsoft 365 holds the office side of every project, and it is shared with many outside parties. Microsoft states that Copilot uses data a user already has permission to access. In a construction company that means owner contracts, bid libraries, payroll files, and subcontractor documents can surface in AI search if permissions are too broad. Table 7 is the checklist to work through before you widen AI search.

Table 7. Microsoft 365 readiness checklist for AI

Item	Why it matters on a construction team	Done when
Site and team ownership	Project sites multiply, and old ones stay open after closeout.	Every project and department site has a named owner, and closed projects are archived.
External guests and sharing	Owners, architects, engineers, subcontractors, and suppliers all need access.	Guests are sponsored, tied to a project, time-limited, and reviewed on a schedule.
Sensitive libraries	Payroll, HR, bonding, financial statements, and bid pricing share the same tenant as project files.	Those libraries are restricted, and sensitivity labels mark the most confidential material.
Bid and estimating libraries	Historical bids hold pricing logic that competitors would value.	Access is limited to the estimating team and reviewed when roles change.
Sign-in protection	A stolen account reaches everything the user can open.	MFA is enforced for all users, with older sign-in methods blocked.
Joiner, mover, and leaver process	Seasonal crews, transfers, and project-based staff change constantly.	Access follows people through hiring, project moves, and departure.
Copilot pilot group	A company-wide rollout before cleanup can expose files widely.	A small pilot group, with approved uses, starts after permissions are fixed.

Vendor and platform review: AI inside the software you already use

Project management, estimating, BIM, accounting, CRM, and meeting platforms are adding AI features, often switched on by default. Review them like any vendor that holds your data, and look for logging, audit, and strict data isolation between projects and customers, as Lathrop GPM recommends. Table 8 gives the questions to ask.

Table 8. Vendor and platform review questions

Question	Why it matters	A good answer
Does the vendor store our inputs or use them to train models?	Uploaded pricing, plans, or quotes may be stored and used for future model training.	No training on our data by default, with the term written in the contract.
Is our data isolated from other customers and between our projects?	Pooled data can leak logic to competitors and cross project confidentiality lines.	Documented isolation, tested and described in the contract or security documentation.
Does the tool pool customers' pricing or benchmarks into shared outputs?	Shared pricing outputs can align bids and create antitrust exposure.	Outputs are built only from our own data, or counsel has reviewed the design.
Which AI features are on by default, and can admins turn them off?	Features arrive with updates, and nobody approves them.	Admin controls, release notes, and notice before changes.
Which sub-processors and models receive our data?	Data may leave the vendor to third-party AI providers.	A current list, with change notice.
Can usage be logged and audited?	You need evidence for insurers, owners, and incident response.	Searchable logs available to our administrators.
If we handle CUI, is the cloud service FedRAMP Moderate equivalent?	DFARS 252.204-7012 requires it for external cloud services handling covered defense information.	Documented authorization or equivalency evidence, supplied on request.
How and when will you tell us about an incident?	Your own reporting duties may run on short clocks.	A defined timeline that fits ours, written into the contract.
What happens to our data if we leave?	Project and pricing data should not stay behind.	Export in a usable format and documented deletion.

AI note-takers and recorded meetings

AI note-takers are the fastest-spreading tool on owner and subcontractor calls, and they are the one most likely to put you in a legal dispute. Haynes and Boone notes that the all-party consent states include California, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania, and Washington, while most other states accept one participant's consent. A contractor's calls routinely cross state lines, and the stricter rule can apply. The suits against several AI note-taker vendors are allegations, and the law is unsettled. Haynes and Boone's practical advice is to disclose the tool and secure affirmative consent from all participants. Table 9 turns that into rules.

Table 9. AI note-taker and recorded meeting rules

Rule	What it means in practice
Disclose every time	Say at the start of the call that an AI note-taker is recording, and make the tool visible to participants.
Get consent from everyone	Ask every participant to agree, including outside parties. If anyone is in an all-party state, treat the call as all-party.
Approve the tool and its terms	Choose tools that do not use recordings for the vendor's own purposes or model training. A vendor that retains rights to use meeting data can create exposure for you.

Rule	What it means in practice
Know what is retained	Set how long recordings and transcripts are kept, who can open them, and how they are deleted. Recordings and transcripts can raise discovery questions in a dispute.
Keep sensitive calls off	No AI note-takers on HR matters, legal and claims discussions, bid strategy with outside parties, or calls involving CUI.
Review before sharing	A person checks every summary before it goes to anyone outside the company.
Cover personal accounts	Prohibit personal note-taker accounts on company calls, so recordings stay in approved systems.

The AI acceptable use policy outline

A two-page policy is enough to start, if it is specific. Table 10 gives the sections. Pair it with the data rule list in Table 5, name an owner, and review it on a schedule.

Table 10. AI acceptable use policy outline

Section	What it covers
Purpose and scope	Who it applies to: employees, field crews, contractors, and temporary staff, on company and personal devices, in company and personal accounts.
Approved tools	A list of approved tools, by function and by data tier, with the name of the person who decides.
Prohibited data	The never-list from Table 5, in plain language.
Human review	Who reviews what before anything leaves the company: bids, owner correspondence, RFIs, pay applications, and safety documents.
Recorded meetings	The rules in Table 9.
Pricing and bidding	No shared or pooled competitor pricing, and pricing decisions made by people.
Federal and controlled work	CUI and export-controlled data stay out of AI tools not approved for them.
Agents and connected apps	Registration, permissions, and approval for any tool that acts or connects (Table 12).
Requesting a new tool	A one-line request, an answer within a set time, and a named approver.
Reporting and training	How to report an accidental paste or a wrong answer without blame, and what training is required.
Review and enforcement	The review schedule, and what happens when the policy is not followed.

Match the review to the risk

Not every AI use needs the same level of control. Smith Currie warns that AI tools can produce confident but false text, misread contract clauses, and lack traceability, which is why review must scale with what is at stake. Table 11 sorts common contractor uses into three tiers.

Table 11. AI use-case risk tiers for construction

Tier	Typical uses	Required controls
Lower risk	Summarizing public information, drafting internal documents from non-restricted material, researching building code or product literature, and brainstorming with no company data	Approved tools only, and a personal check of the result against the source
Medium risk	RFI and correspondence drafts, meeting minutes, daily report drafts, schedule and cost narratives, proposal drafts, and document search across governed libraries	Approved tools, a named reviewer, a source check, and no outgoing document without human approval
Higher risk	Pricing and bid numbers, contract interpretation that someone will rely on, safety-critical or structural decisions, payment and banking changes, HR decisions, worker monitoring, and anything touching CUI	Leadership approval, documented review, counsel where noted, and often a decision not to use AI at all

Controls for AI agents, plug-ins, and automation

AI that acts on its own needs tighter control than AI that drafts. That includes agents, workflow automations, and connected apps and plug-ins. IBM's 2026 report found that more than 20% of organizations had a breach targeting AI models or applications, and that fewer than half were securing the non-human identities AI workflows depend on. Table 12 sets baseline standards.

Table 12. Controls for AI agents, plug-ins, and automation

Control	Standard
Register everything	Every agent, automation, plug-in, and connected app is listed, with an owner, a purpose, and the data it can reach.
Least privilege	Each gets only the access it needs, on named sites or systems, and never broad tenant-wide access.
No payment authority	No AI agent or automation approves, changes, or releases a payment, a banking detail, or a lien waiver.
Human approval for outgoing messages	Messages to owners, subcontractors, and suppliers are reviewed by a person before sending.
Secure the non-human accounts	Service accounts and tokens used by AI workflows are inventoried, protected, rotated, and removed when unused.
Log and audit	Actions are logged and available to administrators and reviewed on a schedule.
Test before production	New automations run first on non-sensitive data in a limited group, with a way to switch them off quickly.

Working checklists for AI governance in construction

Four checklists turn the model into work. Use them in order: find what is in use, record it, set the governance, and keep the evidence.

1. Tool discovery worksheet

You cannot govern what you cannot see. The goal is a complete picture of tools, accounts, and connected apps, gathered without blame. Table 13 lists where to look, and Table 14 lists what to record.

Table 13. Tool discovery worksheet: where to look

Where to look	What to find	Who can help
Conversations by role	Which AI tools estimators, project managers, superintendents, accounting, HR, and executives use, and for what. Ask in a no-blame way.	Department leads, with HR present only if needed
Microsoft 365 sign-ins and app permissions	Which third-party apps users have signed into or granted access to, including AI apps and plug-ins.	Your IT administrator or provider
Managed devices	AI apps, browser extensions, and desktop tools installed on company laptops and phones.	Your IT administrator or provider
Calendars and meeting platforms	Note-taker bots and AI assistants that join or record calls.	Project managers, IT
Expense reports and card statements	Paid AI subscriptions, including small ones bought on a company card.	Accounting
Software you already license	AI features inside project management, estimating, BIM, accounting, CRM, and field apps, and whether they are on.	Vendor documentation and admin settings
Personal accounts and phones in the field	Free AI apps used for daily reports, photos, and safety talks.	Superintendents, foremen, through conversation
Subcontractors and consultants	Whether outside parties use AI on your project data.	Project managers, procurement

Table 14. AI tool inventory: fields to record

Field	What to record
Tool and version	Name, vendor, and whether it is a standalone tool, a feature inside other software, or a plug-in.
Owner and users	The accountable person who uses it, by department.
Data it touches	Which tier of Table 5 the data belongs to, and where the data goes.
Account type	Company account with single sign-on, company account without it, or personal account.
Terms that matter	Training on inputs, retention, sub-processors, logging, and incident notice.
Status and review date	Approved, restricted, prohibited, or under review, with the date of the last review.

2. Four-part governance checklist

A policy states intent. Governance is knowing, and being able to show, what is actually happening. Test your program against these four parts.

Table 15. Four-part governance checklist

Part	Done when	Evidence to keep
1. An inventory of tools, accounts, and connected apps	Every tool, account type, and connected app is listed, including AI features inside existing software.	The inventory from Table 14, with a review date
2. A short, approved list, and what data each may touch	Each approved tool is mapped to the data tiers it may handle, and everything else is restricted or prohibited.	The approved list and the data rule list (Table 5)
3. Simple rules by role, with a named person who answers requests	Each role has a one-page set of rules, and one named person answers requests within a set time.	The policy, role summaries, and the request log
4. A regular check that reality matches the policy	A scheduled review compares actual use to the policy and records what changed.	Review notes, with dates and actions

3. Evidence checklist for insurers, owners, and regulators

Commentary from insurance and IT providers keeps pointing to the same controls for contractors: enforced MFA, endpoint detection, tested backups, a written incident response plan, and a documented funds-transfer verification procedure, increasingly shown with evidence rather than a checked box. Table 16 adds the AI-specific evidence to keep, so you can answer an owner, an insurer, or a regulator with dates. Requirements vary by carrier and contract, so review yours with your broker.

Table 16. Evidence checklist for insurers, owners, and regulators

Evidence item	What it shows	Who tends to ask
Dated AI acceptable use policy and training records	Rules exist, employees have seen them, and they are current.	Insurers, owners, auditors
AI tool inventory and approved list	You know what is in use and what each tool may touch.	Insurers, owners, regulators
Vendor review records, including AI terms	Vendors were checked for training, retention, and sub-processors.	Owners, insurers
MFA coverage and access review reports	Accounts and project-site access are controlled.	Insurers, owners
Funds-transfer verification procedure and log	Payment and banking changes are verified by call-back.	Insurers, lenders, owners
Recorded meeting practice and consent approach	AI note-taker use follows disclosure and consent rules.	Counsel, owners
CUI scoping record (federal work)	You know where covered information lives and which tools may touch it.	Contracting officers, primes, assessors
Incident and exception log	Mistakes and accidental uploads are reported, handled, and learned from.	Insurers, regulators

4. The one-page data rule list

The fourth checklist is **Table 5, earlier in this guide**. Keep it next to the policy and review it with each department.

A 90-day AI readiness roadmap

You can build the foundations in **90 days**. Each phase has a finish line, so progress is visible to leadership.

Table 17. 90-day roadmap

Timeframe	Priorities	Done when
Days 1 to 30: See	Run the discovery worksheet. Build the inventory. Name an owner. Publish the data rule list. Check which owner contracts and NDAs touch AI use.	Leadership can list the tools, the data each touches, and the contracts that apply.
Days 31 to 60: Govern	Adopt the acceptable use policy and the recorded-meeting rules. Fix Microsoft 365 permissions and guest access. Review vendors and AI features. Close MFA and payment-verification gaps.	The policy is in force, high-risk gaps are closed, and a named person answers requests.
Days 61 to 90: Pilot and prove	Pilot approved uses with named reviewers and baselines. Set up the evidence file. Run the first scheduled check against the policy. Plan for the next 6 to 12 months.	Each pilot has a keep, change, or stop decision, and the evidence checklist is current.

Score your readiness: ten questions

Answer for your company today. Give yourself 2 for a clear yes, 1 for partly, and 0 for no or not sure. A clear yes means you could show the evidence to an owner or insurer.

Table 18. Ten-question readiness self-check

Question	A clear yes means
1. Can you list the AI tools your people use, and what data goes into each?	You have an inventory that is less than a quarter old.
2. Do you have a written AI policy with a named owner?	It is dated, current, and people know who to ask.
3. Do employees know what must never go into an AI tool?	A one-page data rule list has been reviewed with each department.
4. Have you checked owner NDAs and design licenses against your AI use?	Counsel or a named reviewer has done so for current projects.
5. Are Microsoft 365 permissions and guest access reviewed?	Sites have owners, and guests are sponsored and time limited.
6. Are MFA and payment call-back verification in place everywhere?	No exceptions list, and a written payment procedure.
7. Have you reviewed the AI features and terms of your key software?	You know what is on, what is stored, and who processes it.
8. Do AI note-takers follow disclosure and consent rules?	A written rule exists and is followed on outside calls.

Question	A clear yes means
9. Does a person review AI output before it leaves the company?	Reviewers are named by use case.
10. Could you show an insurer or owner your AI evidence, with dates?	The Table 16 items are collected and current.

Table 19. What your score usually means

Score (0 to 20)	Level	What to do first
0 to 6	Unaware or reactive	Run the discovery worksheet and publish the data rule list.
7 to 12	Defined	Adopt the policy, fix permissions, and review key vendors.
13 to 17	Managed	Collect evidence, test controls, and measure pilots.
18 to 20	Optimized	Keep reviewing and expand uses that prove value.

This is a rough planning guide, not an audit. A professional assessment tests the answers rather than accepting them.

How AdvancedBITS supports AI readiness for construction firms

AdvancedBITS brings more than 11 years of managed services experience and a SOC 2 Type II examined security practice to construction firms building a secure, governed foundation for AI. Table 20 shows the support models, and Table 21 shows how that support maps to this guide.

Table 20. Support models for AI readiness

Model	How it works	Best fit
Self-guided	You use this guide, the four checklists, and your own team and counsel.	Firms with an IT lead and time to run the discovery and policy work.
Co-managed	AdvancedBITS works alongside your IT person or team on discovery, Microsoft 365 clean-up, vendor review, security, and evidence.	Firms with some internal IT who need depth and capacity.
Fully managed	AdvancedBITS runs the technology and security foundation, and reports to leadership.	Firms with no internal IT, or that want it off their plate.

Table 21. How AdvancedBITS supports AI readiness for construction firms

What you need	What AdvancedBITS provides
Know what AI is already in use	A no-blame discovery of tools, AI features, plug-ins, and connected accounts, and an inventory you can keep current
Safe files for AI search	Microsoft 365 review covering site ownership, guest access, external sharing, labels, and permissions
Rules people follow	Policy and data rule list development, role-based training, and a process to approve new tools
Vendor and platform confidence	Review of AI features and terms in your key software, with a record you can show owners and insurers

What you need	What AdvancedBITS provides
A secure base	Managed sign-in protection, endpoint and email security, monitoring, backup, and payment-verification support
Evidence that holds up	An evidence file built from the checklists, with dates, and regular reporting to leadership

Take the next step

Request a complimentary AI Visibility Scan. We will review the AI tools, AI-enabled apps, and connected accounts we can find in your Microsoft 365 environment and give you a plain-language summary of what we found and what data it can reach. No obligation. Call **561-300-3015** or email sales@advancedbits.com.

AdvancedBITS | Business IT Solutions | www.advancedbits.com

Related resources

- For managed IT, cybersecurity, and construction-specific incident and statistics coverage, see our construction technology and AI page.
- For a worked AI adoption scenario, see our AI in Construction case study.
- For a worked security and continuity scenario, see our Cybersecurity in Construction case study.
- For how to evaluate any managed IT provider, see our Why AdvancedBITS for Construction guide.

AI readiness for construction firms: frequently asked questions

What is AI readiness for a construction firm?

It is the set of decisions, controls, and evidence that let a contractor use AI safely: knowing what is in use, setting rules for which data may go where, securing accounts and Microsoft 365, reviewing vendor terms, keeping a person in the loop, and being able to show all of it with dates.

What should never go into an AI tool at a construction company?

Owner-restricted plans, specifications, geotechnical reports, and BIM files; architect and engineer design documents; bid numbers, unit costs, labor productivity models, margins, and subcontractor quotes; federal contract information and Controlled Unclassified Information; employee records such as payroll, SSNs, I-9s, and injury files; banking and payment data; and credentials, claims and dispute files, and privileged legal communications. Table 5 sorts these into tiers, and your contracts and counsel decide the edge cases.

What should a construction company's AI acceptable use policy include?

A two-page policy is enough to start, if it is specific. It should cover who it applies to, approved tools and who decides, the data that must never be entered, human review before anything leaves the company, recorded meeting rules, pricing and bidding, federal and controlled work, agents and connected apps, how to request a new tool, how to report mistakes without blame, and how the policy is reviewed and enforced. Table 10 gives the outline.

Can estimators use ChatGPT or Copilot on bid documents?

Only with approved tools and only for data your contracts allow. Owner-provided plans, geotechnical reports, and BIM files may be covered by confidentiality terms, and architect and engineer documents are usually licensed for use on a specific project. Pricing and subcontractor quotes can also be stored or used for training by some platforms. Check the contract and the tool's terms first and keep pricing decisions with people.

Are AI note-takers legal on owner and subcontractor calls?

It depends on where participants are. Several states, including California, Florida, Illinois, and Pennsylvania, require every participant's consent to record, and suits against several AI note-taker vendors allege wiretap violations. Those allegations are unproven, and the law is unsettled. The cautious approach is to disclose the tool and obtain consent from everyone, and to confirm your rules with counsel.

Does AI use affect cyber insurance?

Market commentary lists the same core controls for contractors: enforced MFA, endpoint detection, tested backups, a written incident response plan, and a funds-transfer verification procedure, increasingly with evidence. Applications vary by carrier, so ask your broker whether AI use is asked about, and keep the evidence in Table 16.

What changes for federal and defense work?

DFARS 252.204-7012 requires safeguarding of covered defense information, NIST SP 800-171 controls, incident reporting, and FedRAMP Moderate equivalent cloud services for CUI. The Department of War suspended CMMC Phase II on July 13, 2026, but AGC notes the obligation to protect federal data remains. Keep CUI out of AI tools not approved for it and confirm requirements with your contracting officer and counsel.

Can AI estimating tools create antitrust risk?

Possibly. Bernstein Shur notes that if competitors upload pricing to a platform that draws on other users, the output can align unit prices or markups, which regulators may view as algorithmic bid rigging even without intent. Keep pricing decisions with people, and have counsel review any shared pricing tool.

Who owns AI-generated outputs?

It is unsettled. The U.S. Copyright Office's May 2025 report confirmed that works require human authorship, so purely AI-generated material may not be protected. Address ownership and use of AI-assisted deliverables in your contracts, with counsel.

Where should a contractor start?

Find out what is already in use, publish a one-page data rule list, name an owner, fix Microsoft 365 permissions and guest access, and review the AI features in your key software. Table 17 lays out 90 days.

Does AdvancedBITS replace our attorney or insurance broker?

No. We provide technology, security, and AI readiness services, and we work alongside your attorney, insurance broker, and compliance advisors.

Sources

Opened or checked on October 23, 2026. Survey figures are self-reported. Law firm and vendor pieces are commentary, not legal authority, and are attributed as such in the text.

1. Grant Thornton. Construction and real estate insights: 2026 AI Impact Survey. <https://www.grantthornton.com/insights/survey-reports/real-estate/2026/construction-and-real-estate-insights-2026-ai-impact-survey>
2. Bluebeam. New Bluebeam Report Shows Early AI Adopters in AEC Seeing Significant ROI Despite Uneven Adoption (October 28, 2025). <https://press.bluebeam.com/2025/10/new-bluebeam-report-shows-early-ai-adopters-in-aec-seeing-significant-roi-despite-uneven-adoption/>
3. For Construction Pros. Industry Report Finds AI Adoption Accelerating Across Commercial Construction (April 8, 2026), on ServiceTitan's 2026 report. <https://www.forconstructionpros.com/construction-technology/project-management/article/22963634/servicetitan-industry-report-finds-ai-adoption-accelerating-across-commercial-construction>
4. Microsoft and LinkedIn. 2024 Work Trend Index on the state of AI at work (May 8, 2024). <https://news.microsoft.com/source/2024/05/08/microsoft-and-linkedin-release-the-2024-work-trend-index-on-the-state-of-ai-at-work/>
5. Verizon. Vulnerability exploitation top breach entry point, 2026 industry-wide DBIR finds (May 19, 2026). <https://www.verizon.com/about/news/breach-industry-wide-dbir-finds>
6. IBM. What data leaders need to know from the Cost of a Data Breach Report 2025. <https://www.ibm.com/think/insights/data-matters/cost-of-a-data-breach>
7. Cybersecurity Dive. 'Shadow AI' increases cost of data breaches, report finds (July 30, 2025), on the IBM 2025 report. <https://www.cybersecuritydive.com/news/artificial-intelligence-security-shadow-ai-ibm-report/754009/>
8. IBM. One in Four Malicious Breaches are AI-Enabled, Costing Companies \$6 Million on Average (July 29, 2026). <https://newsroom.ibm.com/2026-07-29-ibm-study-one-in-four-malicious-breaches-are-ai-enabled.-costing-companies-6-million-on-average>
9. IBM and Ponemon Institute. Cost of a Data Breach Report 2026, source of the non-human identity finding. <https://www.ibm.com/reports/data-breach>
10. Pierson, D. Bernstein Shur. The Hidden Legal Risks of Using Artificial Intelligence in Construction (February 26, 2026), law firm commentary. <https://www.bernsteinshur.com/insights-events/the-hidden-legal-risks-of-using-artificial-intelligence-in-construction/>
11. Smith Currie. The Hidden Risks of Using AI on Construction Projects (May 28, 2025), law firm commentary. <https://www.smithcurrie.com/publications/common-sense-contract-law/the-hidden-risks-of-using-ai-on-construction-projects/>
12. Lathrop GPM. AI in Construction: What Contractors and Legal Teams Should Know (November 11, 2025), law firm commentary. <https://www.lathropgpm.com/insights/ai-in-construction-what-contractors-and-legal-teams-should-know/>
13. Proler, S., and Young, T. Haynes and Boone, via Bloomberg Law. AI Notetaking Poses Wiretapping, Discovery, and Ethical Pitfalls (January 28, 2026), law firm commentary. <https://news.bloomberglaw.com/legal-exchange-insights-and-commentary/ai-notetaking-poses-wiretapping-discovery-and-ethical-pitfalls>
14. American Arbitration Association. How AI and BIM Are Changing Construction Disputes. <https://www.adr.org/news-and-insights/how-ai-and-bim-are-changing-construction-disputes/>
15. Browne Jacobson. AI and emerging legal challenges in construction (January 13, 2026), law firm commentary, source of the Copyright Office reference. <https://www.brownejacobson.com/insights/2026-horizon-scanning-in-construction/ai-and-emerging-legal-challenges>
16. Acquisition.gov. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. <https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>
17. CMMC Audit Preparation. FedRAMP Equivalent Memo released (January 4, 2024), adviser commentary on the FedRAMP Moderate equivalent requirement. <https://www.cmmcaudit.org/fedramp-equivalent-memo-released/>
18. AGC of America. Cybersecurity and Federal Contractors (CMMC) (updated September 18, 2026). <https://www.agc.org/cmmc>
19. U.S. Department of War, CIO. About CMMC (Phase II suspension, July 13, 2026). <https://dodcio.defense.gov/CMMC/About/>
20. Microsoft Learn. Configure a secure and governed foundation for Microsoft Copilot. <https://learn.microsoft.com/en-us/microsoft-365/copilot/configure-secure-governed-data-foundation-microsoft-365-copilot>
21. National Institute of Standards and Technology. AI Risk Management Framework, and the Generative AI Profile (NIST AI 600-1). <https://www.nist.gov/itl/ai-risk-management-framework>

22. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide, SP 1300. <https://csrc.nist.gov/pubs/sp/1300/final>
23. Surable. Cyber insurance for construction contractors: what carriers require in 2026 (July 9, 2026), vendor commentary. <https://www.surable.ai/blog/cyber-insurance-requirements-construction>
24. Strondex. Cyber Insurance Requirements for Construction Firms, vendor commentary. <https://strondex.com/cyber-insurance-requirements-for-construction/>