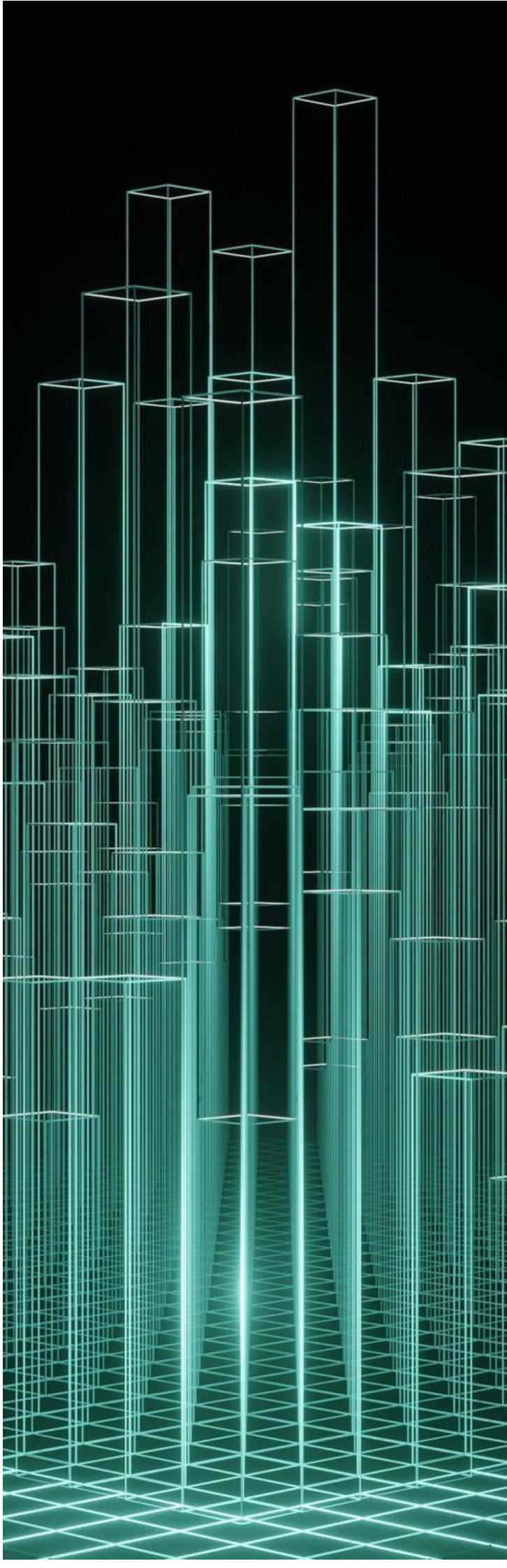
IoT Security Foundation



Building technology procurement guide: Procuring building technology securely

A practical guide for procurement teams and the stakeholders they consult. Aligning sustainability, compliance, and operational efficiency across the building technology lifecycle.

Release 1.0

Notices, disclaimer, terms of use, copyright and trademarks and

licensing notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org

Terms of use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF membership and partners.

IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high-quality guidance,

IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation. By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, trademarks and licensing

We wish to acknowledge significant contributions from the IoT Security Foundation Smart Built Environment Procurement Guide working group:

- Sarb Sembhi: Virtually Informed
- Nick Morgan: Derwent London
- James Willison: Unified Security Ltd
- Christopher Bennison: IoT Security Foundation (TechWorks)
- Mike Welch: Concentric IoT
- Tony Wood: Honeywell

We would also like to acknowledge contributions and peer reviews from:

- John Moor (IoT Security Foundation strategic/board-level support from 2023–2026)
- Jason Shaw: AECOM
- Jeff Day: BT – Editorial
- Kay Ng: Cyber Analytics
- Mo Ahddoud, Alan Jenkins and Dave King – CISO Group
- Ivo Krastins: Savills
- Will Brouwer: WiredScore

About this guide

Building technology has changed. Lighting, heating, ventilation, access control, lifts, CCTV, energy meters and intelligent parking now commonly share the same converged network as laptops and email. This connectivity between systems is what gives commercial real estate the data it needs to hit sustainability targets, and meet new rules. It also creates risks — the procurement decisions we make today will be lockedin for the next ten to fifteen years.

This guide is written for the people who buy, approve, operate, or rely on technology in buildings. It's in plain English. You do not need a background in IT, operational technology, cybersecurity, or law to use it. You DO need to know which colleagues and stakeholders should be in the room before a technology purchase is signed off.

It also draws directly on the Royal Institution of Chartered Surveyors' practice information 'Digital risks in buildings' (1st edition, June 2025), which sets out how property professionals should identify and manage these risks. Where RICS guidance applies, this guide says so.

Who is this guide for?

Use this guide if you are responsible for, or contribute to, the purchase of any technology that connects to a building network. That includes:

- Procurement professionals leading building technology purchases
- Property, facilities, and asset managers responsible for the systems being bought
- Sustainability managers who rely on the data those systems produce
- Physical security and IT security teams who keep the estate safe
- Risk, legal, and compliance teams who carry the consequences when something goes wrong

How to use it

Read sections 1 to 4 for context and roles. Use sections 5 to 8 as a working playbook for each purchase. The appendices are ready-made templates for tender packs and kick-off meetings. This is guidance, not regulation. Adapt it to your organisation and revisit it whenever a new system enters the pipeline.

1. Why this guide exists

The Royal Institution of Chartered Surveyors' practice information ‘Digital risks in buildings’ (1st edition, June 2025) sets out a clear message to the property sector. Buildings now depend on digital systems for their day-to-day operation, and the risks that come with those systems are growing faster than most organisations are managing them. This guide takes that message and turns it into a practical playbook for the people who buy building technology, because procurement is the point at which most of those risks are either locked in or designed out.

> **What RICS says**
> RICS practice information requires owners and managers to keep a documented register of digital risks (RICS, §4.1.2). The International Building Operation Standard (IBOS, 2023, p.26) places cybersecurity on the same footing as fire safety as part of operational compliance.

Three forces are converging on every building technology purchase: the drive to hit sustainability targets, a wave of new compliance obligations, and the need to deliver the operational efficiency that the business case promised.

If any one area lacks attention, the others are compromised. A meter that is easy to tamper with does not give reliable energy data. A system patched only at install will not be compliant in two years’ time.

The convergence at a glance

Sustainability	Compliance	Operational efficiency
Net-zero targets, energy reporting, and ESG disclosure	Cyber regulation, data protection, fire and life safety	Operational savings, system interoperability, business case delivery
Every building technology purchase is now a sustainability, compliance and operational efficiency decision.		

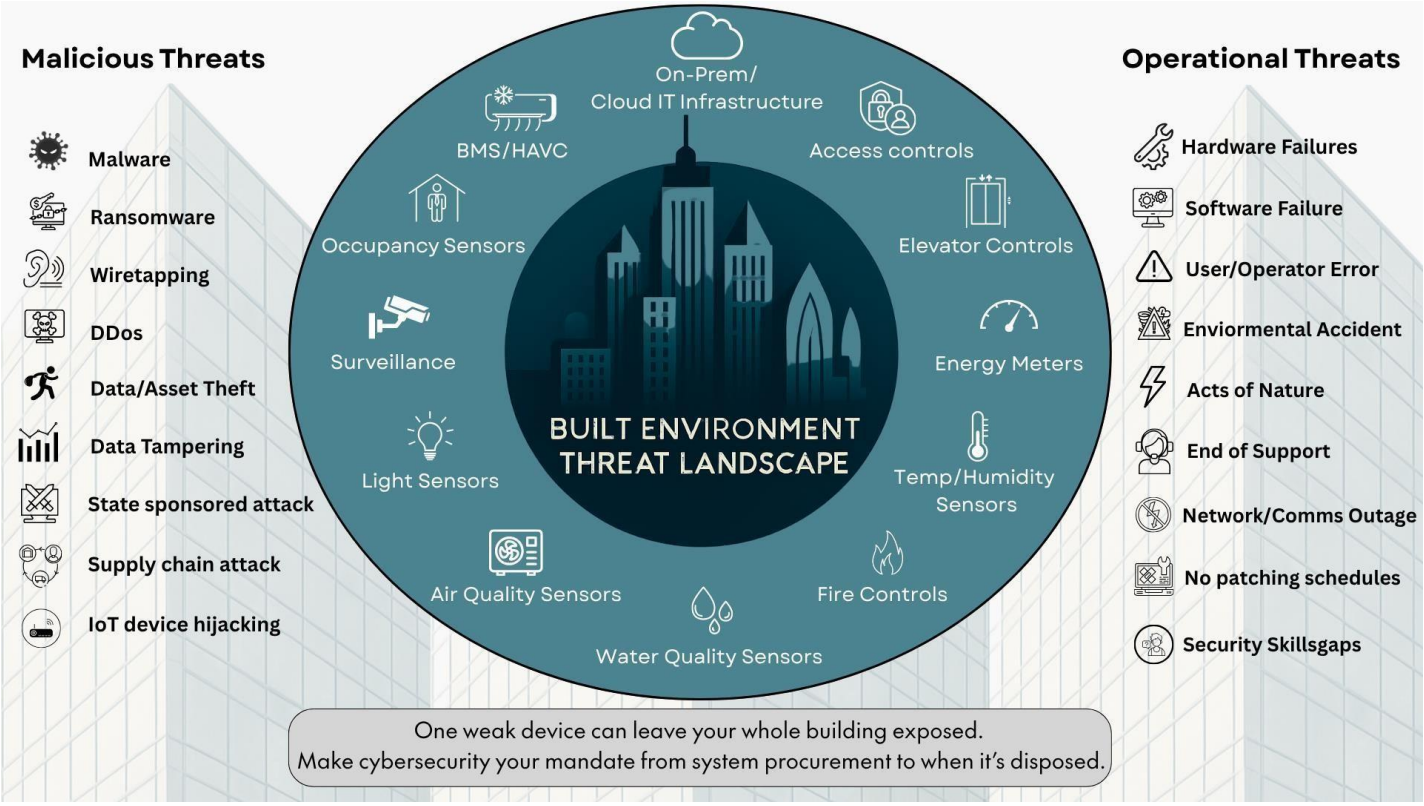
What’s changing?

For most of the last twenty years, Operational Technology ran on isolated networks, installed and maintained by specialist engineers and rarely discussed with IT. That model has broken. Almost every new system in a modern building now runs on a shared IP network and connects, directly or indirectly, to the internet.

That shift brings the same threats IT teams have managed for years. The difference is detection and recovery time. A compromised user account on an IT system can usually be contained quickly. A breach of an access control system, or manipulation of an energy meter used for Environmental, Social, and Governance (ESG) reporting, may go undetected for months and take far longer to rectify.

The diagram below maps the threat surface. The wheel shows connected systems on a shared IP network, with deliberate attacks on the left and operational threats that cause the same harm without intent on the right.

Procurement decides which of these systems enter the building, on what terms, and with what evidence of resilience. A single weak device in any of these categories is enough to create a gateway to the rest, which is why the question "is this safe to buy?" sits at the start of the chain rather than at the end.



The built environment threat landscape. One weak device can leave the whole building exposed.

What the IoT Security Foundation says

The IoT Security Foundation Assurance Framework sets out security requirements for connected products across their full lifecycle, from design and development through supply, deployment and ongoing support.

It groups those requirements into Compliance Classes scaled to risk, so the bar a low-impact sensor must meet differs from the bar an access control or life-safety system must meet. The IoTSF Assurance Framework gives buyers a common reference to use in tender questions and contractual evidence.

Old building tech versus new building tech

Aspect	Older building systems	Connected (IoT) building systems
Network	Dedicated cabling, isolated.	Shared IP network, exposure to the internet.
Lifespan	15 to 25 years. Replace at end-of-life.	5 to 10 years. Software updates required throughout.
Updates	Rarely needed.	Continuous security patching expected.
Data	Local readings, low value to attackers.	Continuous data feeds used for ESG and compliance reports.
Risk owner	Facilities management.	Shared across facilities, IT, security, sustainability, legal and compliance.

The hidden risk: false confidence

If the data your building reports for ESG and regulatory compliance comes from a system that has been tampered with, the numbers you publish are wrong even if your processes are correct. Buying secure systems is the only way to be confident in those numbers.

2. The PPSG

No procurement professional can balance sustainability, compliance, cyber, operational and financial trade-offs alone. The organisations that get this right bring those voices into the room from the start. We call that group the Procurement Project Steering Group, or PPSG.

The PPSG is not a permanent committee. It's set up for a specific purchase, with the right people for that purchase, and stood down once the asset is in service.

What RICS says

RICS asks property professionals to apply systems thinking to digital risk (RICS, §2.2). Building technology now connects to networks, suppliers, and software outside the property boundary. The PPSG exists to make that boundary visible before procurement closes it off.

The diagram below shows the PPSG in practice. The outer ring is the eight-stage procurement cycle, from analysing the business need through to capturing lessons learned. The inner ring is the four behaviours the group demonstrates at every stage: capture, communicate, collaborate, continuously improve. The centre is the PPSG, where the cycle and the behaviours meet.

The PPSG procurement cycle. Source: IoT Security Foundation, Achieving Building Sustainability, Compliance and Resilience through Procurement.

Who sits in the PPSG

Membership will vary depending on the specific project and the technology or system being procured; however, the roles listed below typically form the core group.

Risk owner Owns the consequences if it goes wrong	**Cybersecurity** Defines technical requirements and vets suppliers	**Sustainability** Confirms the system supports reporting needs
Facilities or property Operates and maintains the asset day to day	**Procurement** Convenes the group, runs the process, captures decisions	**IT and network** Confirms the system can connect safely
Legal and DPO Contracts, privacy, regulatory exposure	**Physical security** Where systems affect access, safety, or guarding	**Finance** Total cost of ownership, including maintenance and replacement

Procurement sits in the middle. The job is not to make technical or commercial calls alone, but to make sure the right people make those calls together, on the record, and at the right time. The PPSG is how competing priorities get resolved in the open, before the tender pack is written.

What the PPSG is buying

Cybersecurity in procurement is not a separate goal. It's what protects four outcomes the business already cares about:

Costs	Avoid unbudgeted spend on securing a system after installation and reduce the future cost of a breach in the asset bought today.
Benefits	Assurance that the data the system reports, including the numbers used for regulatory and ESG reporting, has not been tampered with.
Opportunities	Confidence to act on the data quickly, because the underlying system is trusted to be available and intact.
Legal and regulatory	Protection of individuals, occupants and visitors, and a defensible position when the regulator asks.

What the PPSG owns

- Confirming that someone in the room owns the risk if the asset is breached or fails
- Collating all requirements: functional, sustainability, cyber, privacy and operational
- Identifying which suppliers can meet the requirements
- Agreeing in advance what to do when requirements conflict
- Agreeing the response when no supplier can meet a requirement
- Agreeing minimum warranty and support periods, including software updates
- Signing off the final selection
- Recording lessons learned for the next procurement

When to convene it

Convene the PPSG before the request for proposal goes out, ideally when the need is first identified. Late convening is the most common reason cyber and sustainability requirements get cut from the final selection.

A professionally managed building keeps a register of its largest digital risks and the steps being taken to manage them. The PPSG is how new systems get added to that register from day one, rather than being noticed years later.

3. Six core principles

These six principles run through every section that follows. Print them, pin them to the wall, and share them with stakeholders before the first PPSG meeting. They are the shared language the group falls back on when trade-offs get hard.

1

Plan early, plan together

Convene the PPSG before the requirements are written. Cyber, sustainability, and operational voices belong at the start, not at the end.

2

Buy secure by design

Insist on products and suppliers that have built security in from the start. Retrofitting security after install is always more expensive and never as good.

3

Demand evidence, not promises

Ask for certifications, software bills of materials (SBoM), and a published vulnerability disclosure policy. If a supplier cannot provide them, that is your answer.

4

Protect the whole lifecycle

A purchase covers ten or more years. Plan for patches, updates, end-of-support, and decommissioning before you sign.

5

Treat data integrity as critical

If the system feeds compliance, ESG, or operational reports, a tampered reading is a regulatory and financial risk. Integrity is not a nice-to-have.

6

Keep stakeholders informed

Document decisions, lessons, and trade-offs. The next person procuring a similar system should not have to start from zero.

4. Secure by design, in plain English

Secure by design means that security was built into the product from day one, rather than adding it later. It's the same idea as fire safety in buildings or crash safety in cars. Things should fail safely, not unsafely.

You don't need to assess this yourself. You need to know enough to ask the right questions and to recognise good evidence when you see it.

What RICS says
RICS notes that obsolete systems no longer receive security updates and are common targets for attackers (RICS, §2.2.2). Designing for security from the start means setting end-of-support dates and patch cadence into the brief, not negotiating them after install.

What good looks like

What to look for	In plain English
Engineered for security	The product was designed with attackers in mind, not just users. Default passwords are unique. Updates are signed.
Updates throughout life	The supplier commits to security updates for the full life of the product, not just the first year.
Vulnerability disclosure policy	The supplier has a public way for researchers to report security flaws, and a track record of fixing them (see IoTSF Vulnerability Disclosure Best Practice guidelines).
Software bill of materials (SBoM)	The supplier can list every software library inside the product. Without this, you cannot know if the product is affected when a new flaw is announced.
Failure mode is safe	If the network goes down, the fire alarm still works. If a sensor fails, the system flags it rather than reporting a healthy reading.
Identity and access control	Each user and each device has its own credentials. No shared admin accounts. Remote access is logged, approved, and centrally maintained.

Match the assurance to the risk

The IoT Security Assurance Framework (IoTSAF), published by the IoT Security Foundation, gives a simple way to match the level of evidence deemed appropriate based on the risk the system carries. The framework defines four Assurance Classes. The PPSG should agree which class applies before going to tender. Classes 1, 2 and 3 cover the systems found in most commercial buildings.

Class 4 is reserved for critical infrastructure (for example, hospital life-safety systems) and is rarely the right fit for a commercial office.

IoTSAF is the lens this guide uses, but suppliers may also cite ETSI EN 303 645, NIST IR 8259, ISO/IEC 27402, the UK PSTI regime or EU RED Article 3.3. Suppliers of industrial control or building management systems often cite ISA/IEC 62443, which is a heavier, OT-focused framework.

Treat that evidence as useful, but map it back to the IoTSAF Assurance Class agreed by the PPSG so that the bar is consistent across every purchase.

Class 1 **Baseline**	Class 2 **Resists availability attacks**	Class 3 **Protects sensitive data**
When to use it Low-impact systems where a fault affects only a small group, with no sensitive data. **Examples** Standalone meeting room booking screens, low-value sensors	**When to use it** Systems whose failure significantly affects the building, occupants, or many individuals. **Examples** HVAC, lifts, lighting control, building management systems	**When to use it** Systems handling personal, biometric, or operationally sensitive data. **Examples** Access control, CCTV, visitor management, payment systems

Once the class has been agreed, IoTSAF turns it into a clear list of mandatory and advisory requirements that the PPSG can include in the tender pack.

Each IoTSAF requirement is tagged with a minimum class (‘Mandatory for Class 2 and above’, for example), so questions and evidence should be scaled to match.

Asking a Class 1 supplier for Class 2 evidence is overkill and not proportionate to the risk the system carries.

Failing to ask a Class 3 supplier for Class 3 evidence puts the asset at risk. The supplier provides evidence against each requirement that applies to their class.

That gives procurement an objective way to compare bids on cyber, in the same way they already do on price or delivery.

Zero Trust

No device, system, or user is trusted by default. Every connection is verified, every action is logged. The PPSG should ask whether the supplier’s product can fit a Zero Trust architecture, because most modern corporate IT networks are moving that way.

A product that looks secure on its own may behave differently alongside other technology. The PPSG should assess how systems work together, not how each performs in isolation.

5. The procurement lifecycle

A secure purchase is not a single decision. It's a flow of decisions across six stages. Each stage builds on the one before. Skipping or rushing a stage usually causes problems further down the line.

What RICS says
RICS practice information places a direct duty on property managers for the Building Management System (§4.1.1; Commercial property management 2011, p.16). The lifecycle stages set out here translate that duty into the decisions a procurement team can actually own.

Stage 1: Pre-plan

Pre-planning sets up everything that follows. The heavy lifting is done once and re-used in every project. The PPSG sets a default IoTSAF Assurance Class per procurement type: Class 1 for low-impact sensors, Class 2 for HVAC, lifts and lighting control, Class 3 for access control, CCTV and any system handling personal data. The default can be raised for a project but never lowered.

What the PPSG does at this stage

1. Convene the PPSG and confirm membership for this type of procurement
2. Group building technologies into procurement types (for example HVAC, access, CCTV, EV charging) and build a standard requirements pack for each
3. List the legal and regulatory obligations that apply to each type
4. List the policies and procedures that apply (see checklist below)
5. Identify the standards, certifications and codes of practice required (for example ISO 27001, Cyber Essentials, IoTSAF, BSIA codes)
6. Confirm that legacy systems with known vulnerabilities are isolated from the main network using gateways or other controls
7. Set a separate process for cloud services, including data location requirements
8. Standardise non-cyber requirements such as interoperability, communication protocols, and maintenance
9. Standardise cybersecurity requirements at the procurement level

Policy checklist for the PPSG

The PPSG does not author or own these policies. Its job is to make sure they exist and are referenced in the tender pack. If a policy is missing, raise it with the policy owner before tender, not after.

Existing policies (example)	Existing procedures (example)
• Procurement Policy • Procurement Cybersecurity Policy • Information or Cybersecurity Policy • Data Protection Policy • Cyber Resilience Policy • Network Security Policy • Patching Policy • Hardware and Software Update Policy • Auditing and Logging Policy • Encryption Policy • Access Control Policy for Building Systems • Business Continuity Policy • CCTV Policy • Cybersecurity Awareness Policy	• Cybersecurity risk assessment • Auditing and logging for building systems • Data Protection Impact Assessment • Wireless communication hardening • Network segmentation and segregation • Penetration testing of building systems • Third party and supplier due diligence • Vulnerability disclosure handling (see IoTSF Vulnerability Disclosure Best Practice guidelines) • Incident response playbooks for building systems • Decommissioning and secure disposal

Stage 2: Plan

The PPSG decides whether to proceed and on what terms. The output is a go or no-go, and a tender pack the group can defend.

Five planning activities

10. Network, hardware, and licence assessment. List everything the system will need on top of the supplier's package: cloud storage, management workstations, additional software licences, physical space, and staff time.
11. Risk assessment of the new system. Cover the impact on other systems, on the organisation's risk position, and on existing policies. Flag any conflicts.
12. Threat assessment for the type of system. Identify the threats that this category of asset typically faces over its lifetime.
13. Data Protection Impact Assessment where personal data, including biometrics, is involved. Start it early, even if it cannot be completed until later.
14. Supplier eligibility criteria. Set the bar for who can bid based on the risk assessment, the threats, and the IoTSAF Assurance Class agreed.

If the assessments fail

If the available suppliers cannot meet the eligibility criteria, the PPSG has three options. Raise the budget to bring a supplier up to standard. Change the scope of what is being bought. Or stop. Lowering the cyber requirements to fit the supplier pool is not an option, because it locks in the risk for the life of the asset.

Stage 3: Source

Each bidder returns evidence tagged to the IoTSAF requirements at the agreed Assurance Class, so responses can be compared like-for-like. Three activities sit alongside the standard procurement process.

Three sourcing activities

15. Cybersecurity training for site suppliers. Anyone working on your network or your assets must understand your cybersecurity policies before they touch them. Build the training into the schedule.
16. Document remote access. Make the supplier list every form of remote administration they will use. Agree the rules in advance with the network team. Default to no remote access where the system is critical.
17. Start the incident response plan. The cybersecurity team needs to know what is being installed and when, so the response playbook for that system is ready before it goes into use.

Stage 4: Manage

The asset is being installed and brought into service. Three activities make sure what was promised is what gets delivered.

Three manage activities

18. Asset inventory and configuration baseline. Confirm that the installed system matches the agreed design. Record the baseline so any later change is detectable.
19. Dedicated access controls. Each system should have its own access model, with role-based permissions and segregation of duties. No shared admin accounts.
20. Penetration testing. Test the system before it goes live and after any major change. Scope the test against the IoTSAF requirements that apply at the agreed Assurance Class, so findings map directly back to the tender. Agree in advance who acts on the findings and who pays for the remediation.

Stage 5: Operate and maintain

This is where most damage happens. An unmaintained system can become a liability within months.

- Patch systems on the cadence agreed in the support and maintenance contract
- Track who patched what, and when
- Review the supplier's vulnerability disclosure activity quarterly. New vulnerabilities reported and fixed is a healthy sign
- Maintain the SBoM and check it whenever a new vulnerability is announced in a major library
- Run the agreed monitoring, logging and alerting through the IT and cyber teams' existing tools, not a separate console
- Re-test after any architectural change
- Refresh the incident response playbook as the threat picture changes

Stage 6: Decommission

Buildings outlive most of their technology. Plan for decommissioning at the start: the handover from old to new is when sensitive data, credentials and network access are most likely to be left exposed.

- Wipe configuration, credentials and data from devices, including any cloud backups
- Remove network access and decommission the management workstations
- Update the asset inventory and the network diagrams
- Capture lessons learned for the next procurement of this type

6. Five must-ask questions

If the PPSG asks only five questions of a prospective supplier, ask these. Each is tagged with the minimum IoTSAF Assurance Class that requires it.

Q1	**Applies to: Class 1 and above** **Show us your published vulnerability disclosure policy and your last twelve months of fixes.** Suppliers who care about security publish a way for researchers to report flaws and a track record of fixing them. Suppliers who don't, often have undisclosed flaws sitting in your asset. (IoTSAF 2.4.3.11 to 2.4.3.13, mandatory all classes.)
Q2	**Applies to: Class 1 and above** **Demonstrate compliance with the IoTSAF Assurance Class we have specified, with evidence.** This turns a vague security request into a checkable list. The supplier provides evidence against each requirement for their class, and the PPSG compares bids objectively.

Q3	**Applies to: Class 2 and above** **Commit, in the contract, to a security update policy that covers the full life of the asset.** Building technology runs for 10 to 15 years; many products stop receiving updates within 3 to 5. The gap is the window of attack. (IoTSAF 2.4.3.23, mandatory Class 2+. For Class 1, ask for the minimum support period under IoTSAF 2.4.3.9.1.)
Q4	**Applies to: Class 2 and above** **Describe your remote access model in detail and explain how it can be turned off.** Remote access is how most building system breaches happen. You need to know exactly who can connect, from where, and how to revoke access in a hurry. (IoTSAF 2.4.3.22 and 2.4.3.25, mandatory Class 2+. For Class 1, ask only for authenticated remote access.)
Q5	**Applies to: Class 2 and above** **Provide a software bill of materials (SBoM) for the proposed product.** When a flaw is announced in a common library, you need to know within hours whether your asset uses it. Without an SBoM, you cannot tell. (IoTSAF 2.4.14.25, mandatory Class 2+. Do not ask this of Class 1 suppliers.)

7. Red flags: when to stop and reconsider

Some answers should make the PPSG pause. None of them are automatic disqualifications. All of them should be on record before the PPSG signs off.

What RICS says
RICS cites Target (2013, HVAC contractor compromise) and MGM Resorts (2023, helpdesk social engineering on building access) as evidence that connected building systems are a credible attack path (§2.2.4).

Red flag	Why it matters
⚠ **Supplier cannot, or will not, provide SBoM.**	You will have no way to assess vulnerability exposure for the life of the asset.
⚠ **Default passwords are shared across all installations.**	One leaked password gives access to every customer of that supplier.
⚠ **Updates are manual and require an engineer on site.**	In practice, the system will not be patched.

⚠ **Remote access uses a single shared credential.**	Cannot be revoked when staff change. Cannot be audited.
⚠ **No published vulnerability disclosure policy.**	The supplier has no plan for what to do when a flaw is found, except deny it.
⚠ **End-of-support date is shorter than the asset lifespan.**	You will be running an unsupported, unfixable system on your network.
⚠ **Cyber requirements treated as optional in the proposal.**	Indicates how the supplier will treat cybersecurity in service.
⚠ **No reference customer with a similar deployment.**	Your implementation could be the proving ground.

8. Balancing competing priorities

Sustainability, compliance, cyber, cost, operational fit, and tenant experience will conflict on every procurement sooner or later. The PPSG exists so that those conflicts are resolved by the right people, with the right information, at the right time.

> **What RICS says**
> RICS warns that where responsibility for digital systems is not explicitly assigned in contracts, the owner usually carries the liability by default (§3.2). Section 8 is about resolving that ambiguity at procurement, not at incident.

Where conflicts typically arise

- The lowest-carbon product on the market does not have a vulnerability disclosure policy
- The most secure product is supplied by a vendor whose products do not interoperate with the existing estate
- The cheapest product has a five-year support window in a building expected to run for twenty years
- The product that meets a regional sustainability standard does not meet your data protection rules for cloud storage

How to resolve conflicts

The PPSG agrees prioritisation rules in advance, in pre-planning, before any specific procurement. Those rules are organisation-wide, not vendor-specific.

Typical rule. Legal and regulatory compliance is non-negotiable. Cyber controls required by the agreed Assurance Class are non-negotiable. Trade-offs happen below that line, with the C-suite risk owner signing off any exception.

Take fire alarms, for example: in most jurisdictions they must remain operational whether the network is up or down. That kind of legal requirement sets the floor for every trade-off above it. Privacy rules around CCTV and biometric access work the same way.

Legislation, standards and good practice: an example matrix

This is an illustrative matrix, not an exhaustive list. Each organisation should produce its own version with its compliance team.

Sustainability and ESG	Cybersecurity	Privacy and data
Energy Performance of Buildings	NIS / NIS2 Directive	UK GDPR / EU GDPR
MEES, BREEAM, NABERS	Cyber Essentials, ISO 27001	ICO codes of practice
Streamlined Energy and Carbon Reporting	IoTSAF, IoTSF Best Practice guides	Surveillance Camera Code of Practice
Net-zero corporate commitments	NIST Cybersecurity Framework	PECR for cookies and electronic comms

The PPSG is where each column is read by the right specialist, summarised, and translated into tender requirements. Other instruments to check project-by-project include the Building Safety Act 2022 (the ‘golden thread’ duty), DORA for financial-sector occupiers, the PSTI Act for consumer connected products, and ISO/IEC 30141 for IoT reference architecture. Different jurisdictions take different approaches, so any solution needs to be localised.

9. AI in building technology

Artificial intelligence is moving from the cloud into the building. Predictive maintenance, occupancy analytics, energy optimisation, anomaly detection in CCTV, biometric access and tenant experience apps now ship with AI features built in. Many suppliers describe these as ordinary product enhancements.

From a procurement point of view, they are not. AI brings a new class of risk that sits alongside, and sometimes inside, the cyber, privacy and operational risks the PPSG already manages.

The EU AI Act is not directly binding on UK organisations and there is no equivalent UK statute today. The Government's 2023 white paper sets out a principles-based, regulator-led approach instead. Even so, the Act matters here. UK organisations should not treat it as law that applies to them but should treat it as the most detailed reference framework currently available, the shared vocabulary used by ESG raters, tenants and insurers, and a likely template for whatever UK regulation follows. UK-specific authority sits with the National Cyber Security Centre, covered later in this section.

The PPSG should treat AI as a distinct topic, with its own due diligence, before signing any contract that includes AI features. Three reference points anchor everything else.

EU AI Act **Regulation**	ISO/IEC 42001 **Management standard**	AAISM **Security management credential**
What it is Binding EU regulation classifying AI systems by risk: unacceptable, high, limited, minimal. Many building uses (biometrics, workplace monitoring) fall in the high-risk tier.	**What it is** International standard for an AI Management System. The closest AI equivalent of ISO 27001. Suppliers can be certified.	**What it is** ISACA's Advanced in AI Security Management certification. Signals that the people designing, deploying, and assuring AI systems have been independently assessed against a common body of AI security knowledge.

UK guidance: NCSC

Procurement in a UK building should also refer to the National Cyber Security Centre. The EU AI Act is not binding on UK organisations, but two NCSC publications give the PPSG a UK-anchored complement to the international standards above. They sit alongside the EU framework rather than replacing it.

The AI Cyber Security Code of Practice, published by DSIT and NCSC in January 2025, is a voluntary code for everyone in the AI supply chain: developers, system operators, data controllers and end-user organisations. It sets thirteen principles covering secure design, secure development, secure deployment, secure maintenance, and end of life. The Code was written to feed into a future ETSI global standard, so suppliers aligning with it today are positioning for what comes next. The PPSG should ask AI suppliers which of the Code's principles they meet today and which sit on a roadmap.

Guidelines for Secure AI System Development, published by NCSC and CISA in November 2023 and co-signed by more than twenty national cyber agencies, are the closest thing to a global baseline for securing AI. Any serious AI supplier should already be working with them. Treat the absence of a clear answer as a maturity signal.

Where the EU AI Act sets out legal obligations a supplier must meet to sell into the EU: the NCSC material sets technical security expectations a supplier should meet to sell to anyone serious about cyber. For a UK building, NCSC is the more directly relevant authority, even though the EU tiers remain useful as a shared vocabulary for risk.

> **What RICS says**
> *Ask suppliers to map their product to the thirteen principles of the AI Cyber Security Code of Practice, and to confirm alignment with the NCSC and CISA Guidelines for Secure AI System Development. Where they cannot, ask why.*

Why AI raises new questions

Traditional cyber due diligence asks whether a supplier protects the system from being tampered with. AI due diligence asks an extra question: even when the system works as designed, can we trust what it does? Three properties of AI systems sit behind that question.

- AI learns from data. The quality, source, and bias of the training data flow directly into the outputs. A model trained on the wrong population can systematically misjudge the right one
- AI is probabilistic, not deterministic. The same input can produce different outputs over time. Test results from last year do not guarantee behaviour this year
- AI is difficult to explain. Even the supplier may not be able to tell you exactly why a model made a particular decision. That's a problem when the decision affects access, safety, or compliance.

> **Where AI typically appears in building tech**
> Predictive maintenance for HVAC and lifts. Occupancy and people-counting analytics. Energy optimisation that adjusts plants in real time. Anomaly detection in CCTV. Facial recognition or behaviour analytics in access control. Tenant chatbots and virtual assistants. Smart parking and EV charging optimisation.

Classify the AI use case before you classify the supplier

The EU AI Act is the most useful starting point because it forces the PPSG to be explicit about what the AI is doing, not just who is selling it. The Act sets four risk tiers. Procurement decisions should sit on top of the tier, not the brand.

Risk tier	What it covers	Building tech examples
Unacceptable	Banned outright. Includes social scoring and untargeted scraping of facial images.	Most building uses are clear of this tier but check any system that profiles occupants by inferred characteristics.
High risk	Strict obligations on data quality, transparency, human oversight, logging, and post-market monitoring.	Biometric identification, workplace monitoring AI, AI used in safety-critical building systems, AI deciding access to services.
Limited risk	Transparency obligations. Users must know they are interacting with an AI.	Tenant chatbots, virtual concierges, AI-generated content in tenant comms.
Minimal risk	No specific obligations beyond existing law. Voluntary codes of conduct encouraged.	Energy optimisation, predictive maintenance recommending engineer visits, occupancy heatmaps.

PPSG decision point
Before tendering, the PPSG agrees the EU AI Act risk tier for the proposed use case. That decision sets the level of evidence demanded by the supplier. A high-risk classification is not a reason to abandon procurement. It is a reason to demand a higher standard of evidence.

AI vendor due diligence: The question set

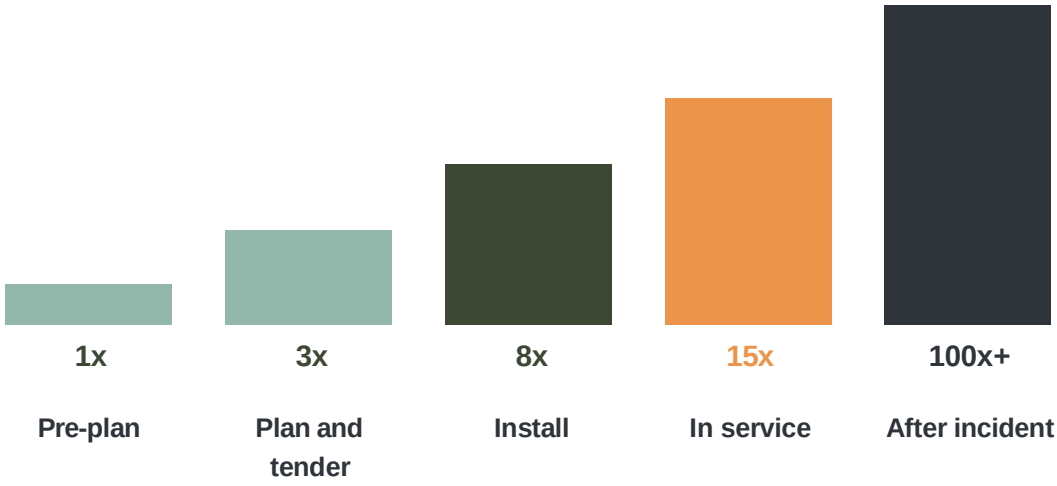
The questions in Appendix C sit alongside the standard cyber and privacy questions, not in place of them. Match the depth to the EU AI Act risk tier. For high-risk uses, every question below should have a documented answer with evidence. For limited or minimal risk, a proportionate subset is reasonable. Where AI fits in the rest of this guide

AI doesn't replace the PPSG model; it extends it. The same principles, lifecycle stages and red flags apply, with one addition: if a supplier cannot clearly explain the AI in their product, show ISO 42001 alignment, or classify the use case under the EU AI Act, that points to unmanaged AI risk. AI questions should therefore become a standard annex in every tender, with expectations rising over time, though existing trade-off rules still apply and legal and regulatory compliance stays non-negotiable. Even where the EU AI Act is not in force (for example, the UK), its evidence requirements should still be met, since they line up with UK GDPR, ICO, NCSC, ISO 42001 and ESG expectations.

AI is best treated as an amplifier of existing risks, raising problems such as opaque ‘black box’ outputs and closer scrutiny of training data, which makes PPSG the right forum to deal with them.

10. The cost of getting it wrong

Cybersecurity retrofitted late costs more than cybersecurity designed in from the start. The graphic below is the rule of thumb most cyber teams use. The exact numbers vary by sector and asset, but the shape is consistent.



ndicative cost of fixing a security issue by lifecycle stage

The action is the same on every project, whatever its size. Before your next scheme reaches tender, convene the PPSG and put security on the agenda from the first meeting. Write the security requirements into the brief, not the snag list. Ask every supplier the questions in this guide and hold them to their answers. Name who is accountable for each decision, and record what was agreed. None of this needs a large budget, it needs the right conversations, in the right order, early enough to shape the outcome.

What RICS says
In 2023 the RICS Disciplinary Panel fined a global real estate firm £200,000 over the Mander Centre in Wolverhampton. That sat on top of a £1.3m health and safety fine. The panel’s concern was not the maintenance that failed. It was the failure to identify the risks and raise them with the client. RICS judges each case on its facts, but the same duty to spot a risk and flag it applies to digital risk. Get that wrong on building technology and the same logic follows. (RICS, §4.2)

11. Glossary

Plain-English definitions for the terms used in this guide.

Term	Plain-English meaning
AAISM	Advanced in AI Security Management. An ISACA certification covering AI security governance, risk, controls and assurance.
AI Cyber Security Code of Practice	Voluntary code of practice published by DSIT and NCSC in January 2025. Thirteen principles for the secure design, development, deployment, and operation of AI systems. Intended to feed into a future ETSI global standard.
BMS	Building Management System. The control system for HVAC, lighting control, and other building services.
CCTV	Closed Circuit Television. A video surveillance system.
DPA	Data Processing Agreement. A contract between a data controller and a data processor setting out how personal data is handled.
DPIA	Data Protection Impact Assessment. A required review when a system processes personal data.
EOSL	End Of Supported Life. The date after which a supplier no longer issues security updates.
EU AI Act	EU regulation that classifies AI systems by risk (unacceptable, high, limited, minimal) and sets out obligations for each tier.
HVAC	Heating, Ventilation and Air Conditioning.
IoT	Internet of Things. Physical devices that connect to a network and exchange data.
IoTSAF	IoT Security Assurance Framework. An IoT Security Foundation framework that defines four Assurance Classes (1, 2, 3 and 4) with mandatory and advisory requirements. Each requirement is tagged with the minimum class to which it applies.
IoTSF	IoT Security Foundation. A not-for-profit body publishing best practice guidance for IoT security. Its parent organisation is TechWorks.
ISO/IEC 42001	International standard for an AI Management System. The closest AI equivalent of ISO 27001. Suppliers can be certified.

MFA	Multi-Factor Authentication. Require more than one form of identity check to log in.
NCSC	National Cyber Security Centre. The UK government authority on cybersecurity and part of GCHQ. Publishes guidance for organisations, including the AI Cybersecurity Code of Practice and joint guidelines on secure AI development.
OT	Operational Technology. The systems that monitor or control physical equipment, distinct from traditional IT.
PPSG	Procurement Project Steering Group. The cross-functional group convened to make a building technology purchase.
SBE	Smart Built Environment. A building that uses connected technology to operate.
SBoM	Software Bill of Materials. A complete list of every software component inside a product.
SLA	Service Level Agreement. The supplier's contractual commitment to specific service levels, including response times for security updates and incidents.
TLS	Transport Layer Security. The standard way to encrypt data moving across a network.
VDP	Vulnerability Disclosure Policy. A published process for receiving and responding to security gap reports.
Zero Trust	A security approach where no device, user, or system is trusted by default. Every action is verified and logged.

12. References and further reading

The materials this guide draws on. The RICS practice information and the IoT Security Foundation publications are the most directly useful for procurement teams looking to go deeper.

RICS

- RICS, Digital Risks in buildings, RICS practice information, 1st edition, June 2025.
- RICS, International Building Operation Standard (IBOS), 1st edition, 2023.
- RICS, Property agency and management principles, 1st edition, 2024.
- RICS, Rules of Conduct, 2021.
- RICS, Data handling advice.

IoT Security Foundation

- IoT Cybersecurity for Facilities Professionals in the Smart Built Environment, Release 1.0, 2023.
- IoT Security Assurance Framework (IoTSAF), Release 4.0.
- IoTSF Vulnerability Disclosure Best Practice Guidelines, Release 2.0, 2021.
- IoTSF Best Practice Guides, Release 2.

Standards and frameworks

- ISO/IEC 27001 Information Security Management Systems.
- ISO/IEC 42001 Information technology, Artificial intelligence, Management system.
- NIST Cybersecurity Framework.
- NIST AI Risk Management Framework (AI RMF 1.0).
- Cyber Essentials and Cyber Essentials Plus, NCSC.
- ETSI EN 303 645 Cyber Security for Consumer Internet of Things.
- ISA/IEC 62443 series for industrial automation and control systems.
- CAPSS, the Cyber Assurance of Physical Security Systems.

AI regulation and assurance

- Regulation (EU) 2024/1689, the EU Artificial Intelligence Act.
- ISACA, Advanced in AI Security Management (AAISM) certification programme.
- ISACA, Artificial Intelligence Audit Toolkit and AI security guidance.

UK AI guidance

- DSIT and NCSC, AI Cyber Security Code of Practice, January 2025.
- NCSC and CISA, Guidelines for Secure AI System Development, November 2023.
- NCSC, Principles for the security of machine learning, 2022.

- DSIT, A pro-innovation approach to AI regulation, UK white paper, March 2023.
- ICO, Guidance on AI and data protection.

Regulatory and policy

- UK Network and Information Systems Regulations (NIS / NIS2).
- UK GDPR and Data Protection Act 2018.
- ICO Codes of Practice on CCTV and surveillance.
- ENISA Procurement Guidelines for Cybersecurity.
- UK Data (Use and Access) Act 2025.
- Building Safety Act 2022 (the golden thread).

Appendix A: Supplier question sheet

A ready-to-use question sheet to drop into a request for proposal. Each question is tagged with the minimum IoTSAF Assurance Class that requires it. Use only the rows that match the class the PPSG has agreed for the system. Asking a Class 1 supplier for Class 2 evidence is overkill, not proportionate to the risk, and risks of losing good suppliers who do not see why the question is being asked.

	Min class	Question	Supplier response
1	1+	List the certifications held by your organisation (for example, ISO 27001, Cyber Essentials Plus). Provide expiry dates.	
2	1+	Provide a copy of your published vulnerability disclosure policy and a link to your security contact.	
3	1+	State the end-of-support date for each component of the proposed product.	
4	1+	Describe the default authentication model. Are credentials unique per device or per installation?	
5	1+	Describe how the product fails when the network is unavailable, and any safety implications.	
6	1+	List the data the product collects, where it is stored, and the retention period.	
7	1+	Confirm the IoTSAF Assurance Class that the product meets, and provide supporting evidence.	
8	1+	Provide three reference customers with similar deployments. Include contact details, with permission.	
9	1+	List the cybersecurity issues fixed in the product in the last twelve months and the time from disclosure to patch.	
10	2+	Provide an SBoM for the proposed product in a machine-readable format (CycloneDX or SPDX).	
11	2+	Describe how security updates are delivered, the typical cadence, and how customers are notified.	

12	**2+**	Describe all forms of remote access, including supplier-initiated remote support, and how the customer can disable each.	
13	**2+**	Describe the installer training programme. State how installers are kept current on cybersecurity.	
14	**2+**	Confirm support for our network segmentation, identity and logging requirements (attached separately).	
15	**3+**	For systems handling personal data, describe how that data is protected at rest, in transit, and on disposal.	
16	**3+**	List any sub-processors and where they operate.	

Appendix B: PPSG kick-off agenda

A 60-minute agenda for the first PPSG meeting on a new procurement. Adjust the timings to suit the size of the project.

Time	Item	Outcome
00:00	**Welcome and roles**	Each member confirms their role and what they own.
00:05	**What is being procured and why**	Shared understanding of the business needs and timelines.
00:15	**Risk owner identified**	Named individual accepting risk, with sign-off authority.
00:20	**Sustainability, compliance and operational requirements**	Each specialist gives a 5-minute headline of must-haves.
00:35	**IoTSAF Assurance Class**	Class 1, 2, 3 or 4 agreed for the system, with rationale. Most building technology lands in Class 1, 2 or 3.
00:40	**Conflict resolution rules**	Pre-agreed rules for resolving competing requirements.
00:50	**Open actions and owners**	Numbered actions, named owners, due dates.
00:55	**Next meeting**	Cadence and decision points for the rest of the project.

Appendix C: AI vendor due diligence question set

AI1	**Describe every AI or machine learning component in the proposed system, and the EU AI Act risk tier you assess each to fall under.** **Why it matters** Suppliers will not always volunteer that AI is inside the product. Naming it forces transparency and gives the PPSG a defensible record of what was disclosed.
AI2	**Are you certified to ISO/IEC 42001, or working towards it? Provide the certification scope or your implementation of roadmap.** **Why it matters** ISO 42001 certification is the clearest signal that AI risk is managed at organisation level, not left to individual product teams.
AI3	**Describe the training data: source, jurisdiction, age, demographic representation, and any synthetic data used.** **Why it matters** AI inherits the bias of its training data. For systems making decisions about people in the building, biased data is a discrimination, safety and reputational risk.
AI4	**Describe the human oversight model. Who reviews AI decisions, how often, and what is the override process?** **Why it matters** The EU AI Act requires meaningful human oversight for high-risk use. "The model decides" is not an acceptable answer when the decision affects access, safety or employment.
AI5	**Provide your bias testing methodology and results. How often is the model re-tested in production?** **Why it matters** Bias is not a one-time check. Models drift as input data drifts. The supplier should show ongoing monitoring, not just pre-launch testing.
AI6	**Describe how the system explains its decisions to operators and to people affected by them.** **Why it matters** Explainability is required by the EU AI Act for high-risk systems and is increasingly expected by the public. ‘Black box’ answers create operational and legal exposure.
AI7	**Describe the model of update of governance. How are model changes tested, approved and rolled back?** **Why it matters** An AI model that updates without governance can change behaviour overnight. The change control you accept for software must extend to the model itself.
AI8	**Where are training, fine-tuning, and inference performed? What data leaves our environment, and to whom?**

	Why it matters Many AI products send data to third-party model providers. The PPSG needs to know before signing, not after a regulator asks.
AI9	**Describe your AI incident response process: what counts as an AI incident, how you detect it, and how you notify customers.** **Why it matters** Failures of AI systems often look different from cyber incidents. The supplier needs a defined process, or the customer carries the risk alone.
AI10	**Provide evidence of conformity assessment for any high-risk AI under the EU AI Act, and your data protection impact assessment for the use case.** **Why it matters** These documents are mandatory for high-risk systems and good practice everywhere else. Their existence is the simplest test of supplier maturity.
AI11	**Describe your compliance posture against the EU AI Act and, separately, your position on UK regulation, NCSC guidance and ICO expectations. Note any UK-specific AI guidance you follow today.** **Why it matters** The EU and UK regimes are diverging. Suppliers serving both should be able to describe each separately. A combined or vague answer is a sign the supplier has not yet thought through the UK-specific obligations that are likely to land first for a UK estate.