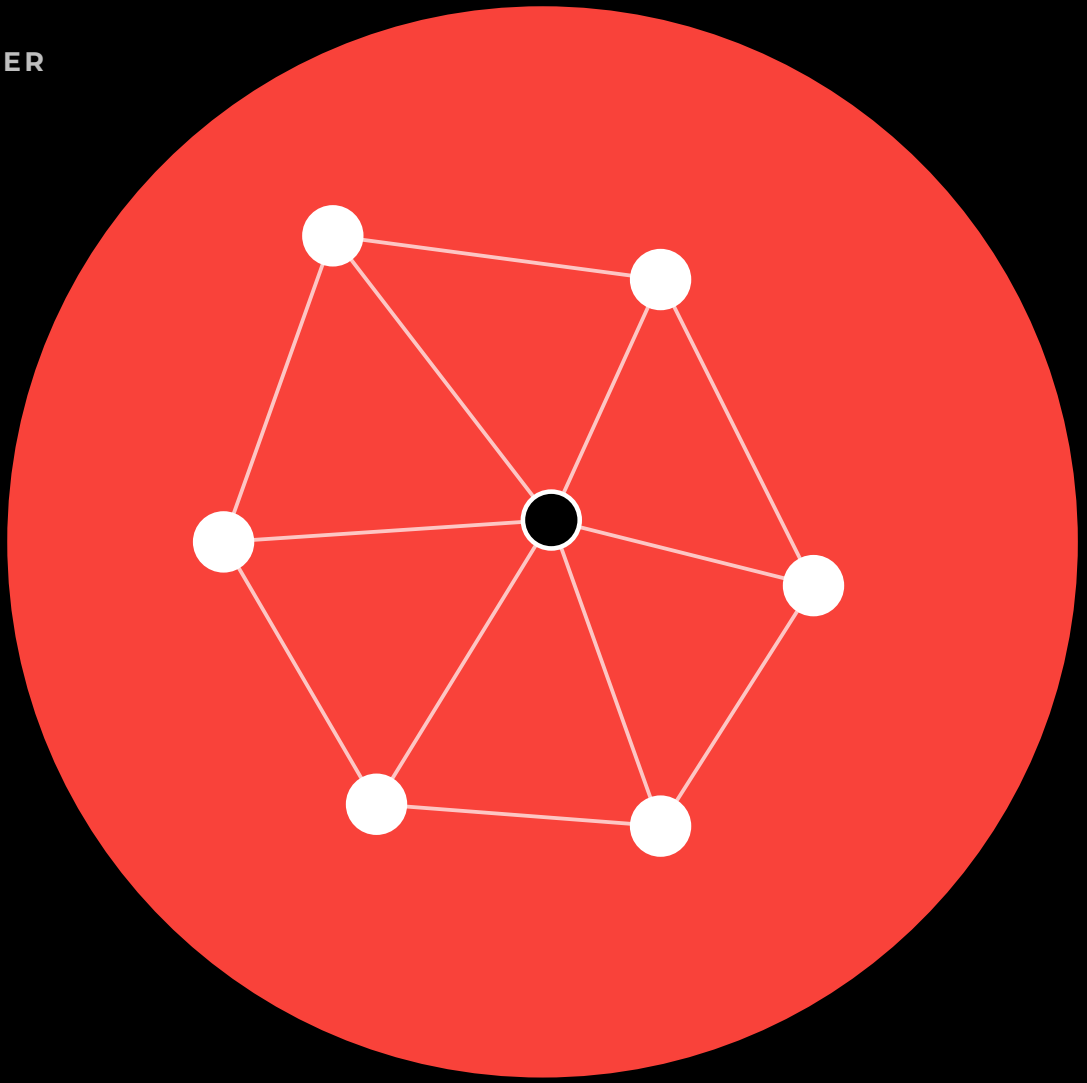
SMART BUILDINGS SHOW 2026 | LONDON | 14 OCTOBER

DE-RISKING TECHNOLOGY DELIVERY

Proving it works before site ever sees it



Christian Lowes
Technical Director, Building Technology Systems, WSP

Smart buildings don't have a technology problem.

They have a trust problem.



THE CLIENT

Am I paying for a capability, or a promise?



THE OPERATOR

Will I inherit something I can't run, support or secure?



THE DELIVERY TEAM

Who owns it when the integration fails on site?

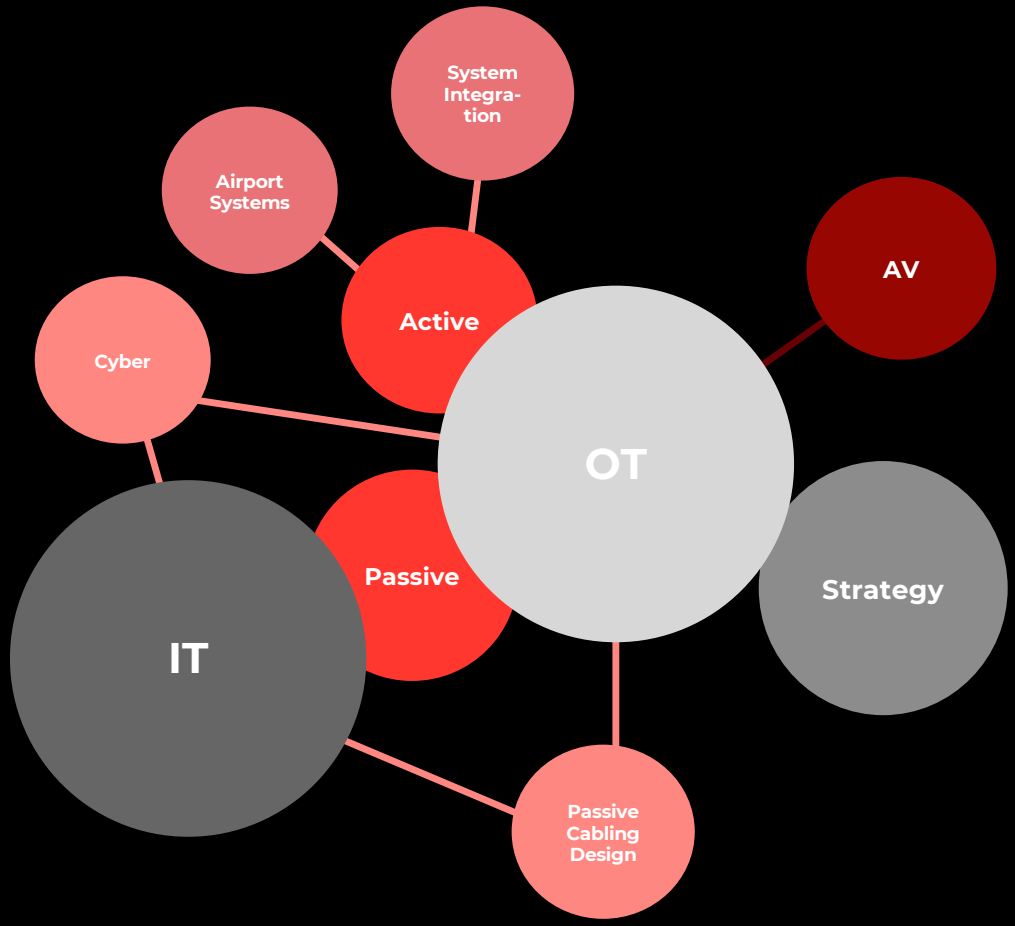
Copyright WSP 2026

BACKGROUND

MY STORY



Christian Lowes



Copyright WSP 2026

THE WHY?

WHY INVEST IN SMART BUILDING?

CONTEXT

1



SOCIAL IMPACT AND ENVIRONMENTAL CONCERNS

2



ADVANCEMENT OF TECHNOLOGY

3



CHANGING USER REQUIREMENTS

VALUE



ENERGY USE INTENSITY

Smart building technology plays an important part in closing the energy performance gap and using data to optimise operations



REALTIME NET ZERO

Climate change related energy performance aims, are setting ambitious real-time renewable energy targets, smart building technology enables demand response to match supply.



AUTOMATE ESG REPORTING

ESG related reporting is common place, increasingly automated collection of data is requested via smart building software.



USE DATA FOR BUILDING OPTIMIZATION

Cloud based analytics software linked to building sub-systems and dedicated IoT sensors, are becoming the norm.



USE DATA FOR MAINTANENCE

Facilities management is moving from a reactive, through scheduled to a predictive maintenance model, allowing problems to be solved before complaints come in.



FUTURE PROOF YOUR BUILDING

Smart enablement of the building starting with a converged IT network, device naming and enforcement of open protocols, allows for cost effective software addons in future.



ENHANCE USER EXPERIENCE

SMART building technology must be user centric to maximise value. Leveraging system integration and interaction touchpoints to respond to high value user needs.



TEAM BUILDING AND RETENTION

Make buildings healthier (e.g. improving air quality) and more interactive (e.g. dashboards/apps) to attract and retain talent.



CYBER SECURITY PRIORITY

SMART must be delivered with cyber security principles to allow portfolio management and lower asset risk for tenants and landlords.

Copyright WSP 2026

A FAMILIAR STORY

IT WORKED ON THE DATASHEET

AS DESIGNED

Stage 4 system architecture



Segregated, monitored, approved by client IT

AS INSTALLED

Two weeks before handover



Programme pressure wins. The quick fix becomes permanent.

Missing hardware that nobody declared, found on site at the worst possible moment.

Copyright WSP 2026

THE EVIDENCE GAP

SOLD A DREAM, OR A REALITY?

> **Plug and play**
>
> On which network? Under whose security policy?

> **Secure by design**
>
> On which network? Under whose security policy?

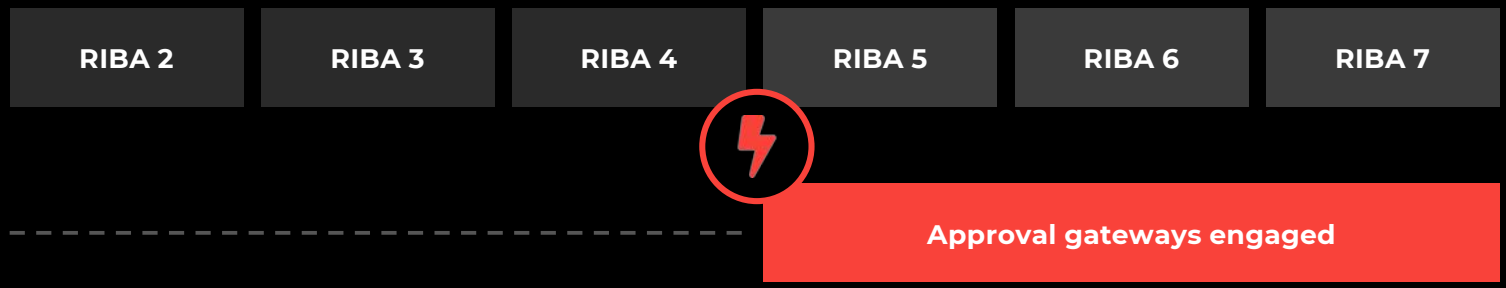
> **Integrates with your BMS**
>
> On which network? Under whose security policy?

Usually, true somewhere. The question is whether it is true on your network, alongside your other systems, and signed off by your cyber team.

Copyright WSP 2026

WHY IT KEEPS HAPPENING

TWO PROGRAMMES THAT MEET TOO LATE



01 GATEWAYS

Smart building technology must pass corporate approval and security gateways before it can go live on client IT or OT networks.

02 OWNERSHIP

Traditional construction delivery tends to treat this as a client owned risk, outside the programme.

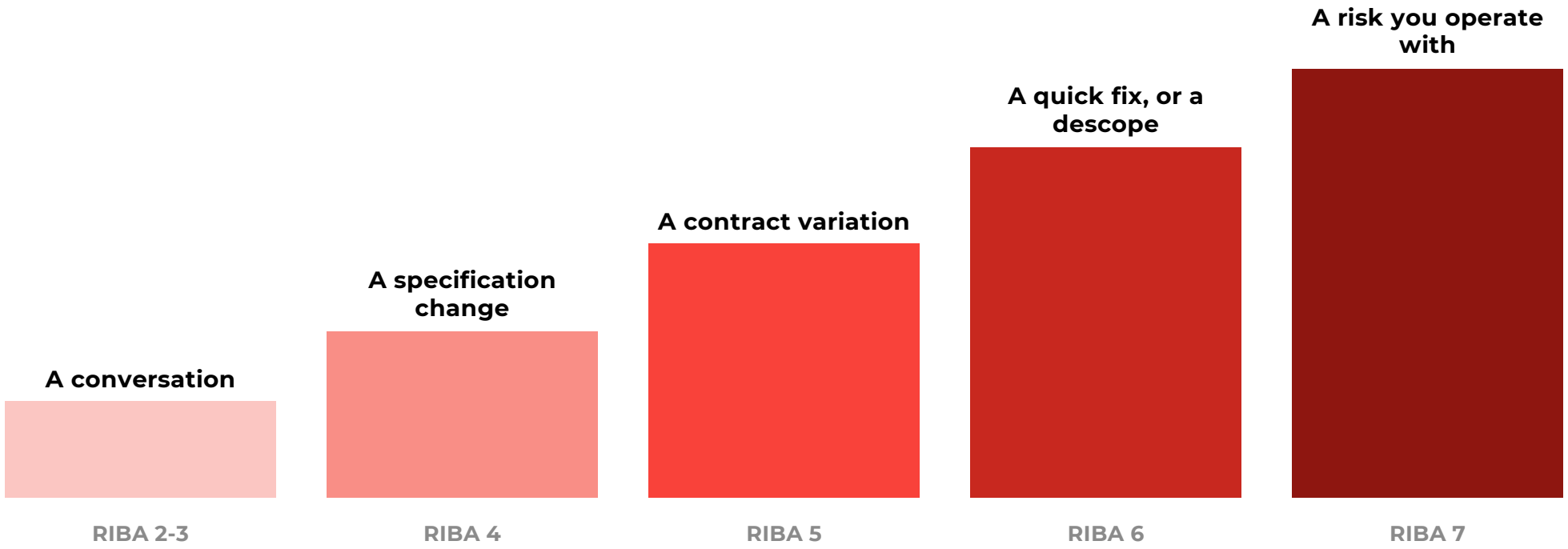
03 CONSEQUENCE

Non-compliant designs surface late: delays to installation, or systems removed from scope on site.

Copyright WSP 2026

THE COST OF LATE DISCOVERY

THE LATER YOU FIND IT, THE MORE IT COSTS



Copyright WSP 2026

SHIFT THE RISK LEFT

Turn assumptions into evidence before time pressure and site constraints start making the decisions.

Copyright WSP 2026

OUR APPROACH

A CONTROLLED ENVIRONMENT, NOT A SHOWROOM



INNOVATE

Closed test environment, isolated from live operational systems

INTEGRATE

Prove devices deliver the expected function in practical scenarios

VALIDATE

Resolve interoperability issues against client technology and building standards

SECURE

Test cyber measures against client requirements and industry standards

OPTIMISE

Use the data to plan operation and continuous optimisation

Copyright WSP 2026

WHERE IT SITS

VALIDATED BEFORE IT REACHES SITE



6-8

weeks for a typical testing sequence

2+

vendors per device type can be tested before procurement

1

shared room for vendors, MSI, client IT and FM

Copyright WSP 2026

LONDON HQ | BUILDING TECHNOLOGY SYSTEMS

OUR PERMANENT TEST LAB



Competing vendors side by side, on one network, under the same rules.

BUILDING MANAGEMENT

1. BMS System Controllers A
2. BMS System Controllers B
6. BMS System Controllers C

LIGHTING CONTROL

3. Lighting Control Components
5. Lighting Drivers and Sensors
7. Lighting Headends

IOT & INFRASTRUCTURE

4. General IoT System and Sensors
8. Test Lab Network

Copyright WSP 2026

INSIDE THE LAB

A SMALL-SCALE VERSION OF THE REAL BUILDING

CLOUD ANALYTICS
Smart building analytics platforms, dashboards

MIDDLEWARE
Integration layer, MQTT broker, data normalisation

NETWORK
OT switching, firewall rules, DMZ, VLANs

FIELD DEVICES
BMS, lighting, metering, IAQ, occupancy, LoRaWAN

WHO'S IN THE ROOM

Vendors
integrating their own kit, not presenting it

MSI
owning the integration pattern

Client IT & cyber
the approvers, watching it happen

FM & operations
the people who inherit it

Delivered directly or with MSI partners, including WSP's permanent lab at 70 Chancery Lane.

Copyright WSP 2026

HOW A LAB RUNS

FIVE STEPS FROM ASSUMPTION TO EVIDENCE



PLAN & DESIGN

- Define objectives
- Design the lab architecture
- Agree logistics

PROCURE & SET UP

- Engage vendors
- Procure and connect devices
- Build the test network

TEST & VALIDATE

- Functional testing
- Device security testing
- Compliance with client standards

ANALYSE & REPORT

- Evaluate performance
- Compare vendors
- Present findings to client

OUTCOME

- Select final products
- Update the design and spec
- Carry lessons into Stage 5

Copyright WSP 2026

THE EVIDENCE

WHAT THE LAB ACTUALLY TOLD US

DEVICE CONNECTIONS

FOUND Extra hardware needed that vendors hadn't declared

ACTION Architecture updated with client IT before procurement

CYBER SECURITY

FOUND Insecure or unknown open ports on some devices

ACTION Port closure specified, secure design enforced

INTEGRATION

FOUND Devices didn't always match expected standards or claims

ACTION Resolved with vendors while it was cheap to do so

ACCURACY

FOUND Platform data didn't always reflect real conditions

ACTION Structured tests identified the most accurate option

DATA USAGE

FOUND Some devices sent far more data than equivalents

ACTION Ongoing cloud messaging cost became a selection metric

VENDOR SUPPORT

FOUND Some devices needed multiple follow ups to work

ACTION Service quality assessed before contract, not after

Copyright WSP 2026

CASE STUDY | LONDON | CLIENT CONFIDENTIAL

FINANCIAL SERVICES HEADQUARTERS

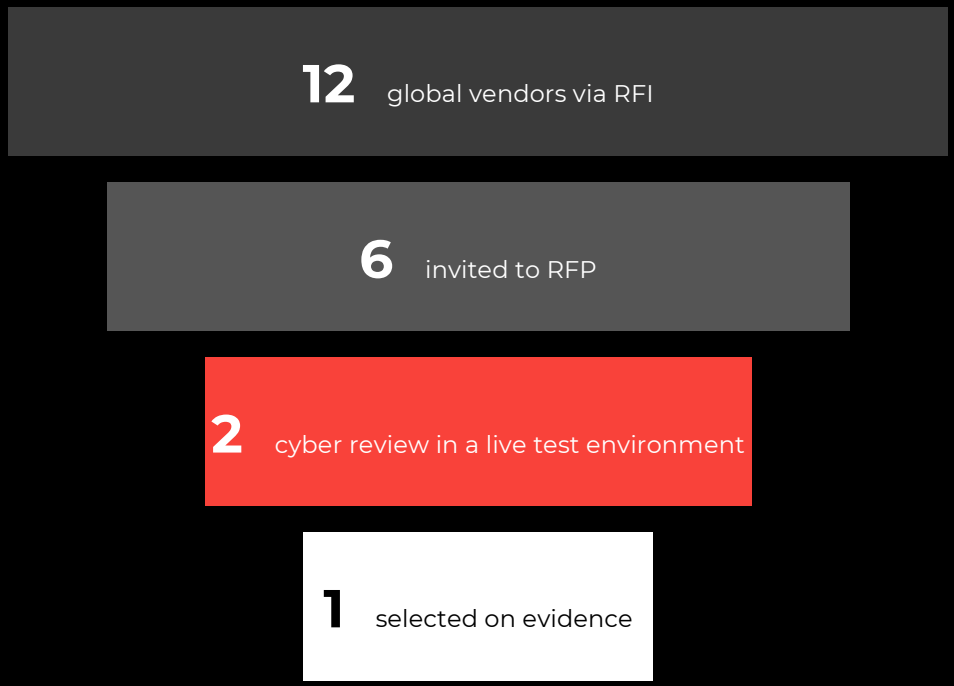
Demanding global corporate IT and cyber standards. Integrations had to work across procurement and responsibility boundaries.

We worked with the project MSI to deploy, integrate and validate selected technologies in a test lab ahead of construction installation.

OUTCOMES

- Devices assessed at granular level in a simulated financial services environment
- Deployment aligned with the client's global technology standards
- Lessons fed into the client's engineering standards for OT cyber security

ANALYTICS PLATFORM PROCUREMENT



Copyright WSP 2026

WHAT IT PROTECTS

FOUR THINGS EARLY VALIDATION BUYS YOU



COST CERTAINTY

Hidden hardware, integration effort and ongoing data costs are known before the price is fixed.



PROGRAMME

Approvals and integration happen off the critical path. Commissioning is rehearsed, not improvised.



CYBER RESILIENCE

Weaknesses are designed out, not patched in. No quick fixes left on the OT network.



TRUST

Client, operator and IT have seen it work with their own eyes before they sign.

Copyright WSP 2026

BEING HONEST

WHAT WE'VE LEARNED THE HARD WAY

01	**Appoint the integrators first**	If the OT network contractor isn't in contract when the lab is built, secure comms such as BACnet/SC and certificates can't be tested end to end.
02	**Bring cyber in on day one**	Client IT and security are the approvers. If they only see the report, you have lost most of the value.
03	**Budget it as a defined package**	Scope the lab within the technology fee from the start, not as an add-on when problems appear.
04	**Write findings into the spec**	Lessons that stay in a lab report do not de-risk anything on site.

A test lab reduces risk. It doesn't remove it.

Copyright WSP 2026

THREE QUESTIONS FOR YOUR NEXT PROJECT

1. Has this been proven on a network like ours?
2. Who owns integration risk before Stage 5?
3. What evidence will our cyber team sign off against?

Copyright WSP 2026

“

Trust is built by showing your client their technology works before the site ever sees it.

QUESTIONS?

Christian Lowes
Technical Director, Building Technology Systems
christian.lowes@wsp.com

Copyright WSP 2026