Concerto

IT risks

and mitigations

For UK Estates Teams in the public and private sector

Risks

Data security and privacy breaches

CAFM/IWMS platforms often store sensitive data on assets, building layouts, access points, and potentially staff information. A weak security posture exposes the organisation to cyber threats and data protection violations (e.g. UK GDPR breaches).

Mitigation steps

- Involve IT security early to perform a **vendor risk assessment**
- Insist on **Cyber Essentials Plus** or **ISO 27001** certification from vendors
- Require **UK-based data hosting**
- Check for **role-based access controls, encryption at rest and in transit**
- Review vendor's **data processing agreement (DPA)** for GDPR compliance

Poor integration with existing systems

Failure to integrate with HR, finance, access control, or IoT systems leads to siloed data and duplication of work, undermining efficiency and digital transformation goals.

Mitigation steps

- Map required integrations during **requirements gathering**
- Ask vendors for **API documentation** and shy away from open or existing APIs, as they will not be as secure as bespoke APIs
- Have IT confirmed compatibility with existing systems (e.g. ERP, Active Directory)
- Conduct **technical evaluation workshops** before selection
- Include integration capabilities in RFP scoring

Risks

Vendor lock-in or proprietary data formats

Some platforms restrict data exports or use closed data models, making it difficult to switch systems or change FM providers in future.

- Insist on full **data export capabilities** in open formats (e.g. CSV, JSON, IFC)
- Include clauses in the contract for **data portability on exit**
- Require visibility of **data model structure** during evaluation
- Have IT/legal review contracts for **ownership of data clauses**

Unvetted cloud or hosting environments

Cloud-based platforms must be hosted securely. Using unvetted or offshore environments can breach organisational or sector policies (especially in health, defence, or local government).

- Verify **vendor's cloud provider (e.g. AWS UK, Azure UK)** is compliant
- Reject platforms hosted in non-compliant jurisdictions (e.g. US-only with no UK/EU fallback)
- Confirm **backups, failover procedures, and SLAs**
- Request a **Business Continuity and Disaster Recovery plan (BCDR)**

Risks

Underestimating total cost of ownership (TCO)

Some platforms appear cheap upfront but require high integration, customisation, or user support costs later, especially when IT involvement is delayed.

Mitigation steps

- Include **implementation, licensing, support, training, and integrations** in cost model
- Ask for 3–5 year **TCO projection**
- Engage IT to assess ongoing **support workload** and resource needs
- Ask vendor for clear **pricing structure for upgrades, modules, and APIs**

Inflexible system configuration

Choosing a rigid, hard-coded system limits the ability to adjust workflows or adapt to new FM providers, legislative changes, or internal processes.

Mitigation steps

- Select systems with **configurable (not custom-coded)** workflows
- Ask vendors for demo of how workflows and dashboards are adjusted
- Test use cases like **changing PPM frequency or SLA thresholds** during pilot

Risks

Limited user access and support models

Platforms that charge per user or restrict subcontractor access hinder adoption and limit visibility.

- Clarify user licensing model early (named vs concurrent)
- Ensure the platform supports **multi-user, multi-role** access (e.g. Estates, IT, FM contractors)
- Ensure **service desk support model** is sufficient

No exit strategy or poor handover capability

Poor planning for future offboarding leads to data loss, compliance gaps, and transition issues when changing FM contracts or platforms.

- Build **offboarding and data export clauses** into the contract
- Require regular (e.g. quarterly) **data backups in open format**
- Develop an **Exit Plan** jointly with IT and Estates before go-live

Summary

Estates checklist for mitigating IT risks

Risk area	Mitigation action
Data security	Vendor security review, encryption, GDPR alignment
Integration	IT-led evaluation of APIs and data mapping
Vendor lock-in	Exportable data, contract clauses, open formats
Cloud compliance	UK hosting, DR plans, service SLAs
Cost management	Full TCO analysis, no hidden API/license costs
Flexibility	Configurable workflows, test during pilot
User management	Licensing model review, multi-role support
Exit planning	Offboarding plans, data backups, contract clauses

Final advice to estate teams

- Engage IT from day one – not just post-selection
- Make technical due diligence part of vendor evaluation
- Treat IT risks as strategic risks, not just operational issues
- Build a cross-functional procurement team with IT, Procurement, Legal and Estates from the start

Concerto

Book a demo

01925 989 500
keri.barton@concerto.co.uk