A potential (partial) IoT vendor checklist (Version 2.0)

operational risks (eg resourcing & planning)

- ❑Who pays for vendor systems requirements (eg hardware, supporting software, networking, etc?)
  - ❑Does local support (FTE) exist?
    - ❑Is it currently available?
    - ❑Will it remain available?
  - ❑If hosted in a data center, who pays for those costs?
  - ❑If cloud-hosted, eg AWS, who pays for those costs?
  - ❑Above questions answered for both implementation & long term support?

- ❑Does vendor need 1 (or more) data feeds/data sharing from your organization?
  - ❑Are the data feeds well-defined?
  - ❑Do they exist already?
    - ❑If not, who will create & support them
    - ❑What are those staffing costs?
  - ❑Are there privacy/sensitivity issues for data leaving the premises ?

- ❑What is total operational cost after installation?
  - ❑Licensing
  - ❑Support contracts
  - ❑Hosting requirements
  - ❑Business resilience requirements (eg redundancy, recovery, etc for OS, db, other)

- ❑Can IoT system vendor maintenance contract offset local IT support shortages?
  - ❑for 10's, 100's, 1000's of new endpoints ?

cybersec (bad guy) risks

- ❑Is there a commissioning plan? Or have installation expectations otherwise been stated?
  - ❑Default logins & passwords changed & recorded?
  - ❑Non-required default ports closed on each device ?
  - ❑Devices port scanned (or similar) after installation ?
  - ❑Other

- ❑For remote support, how does vendor safeguard login/account information?
  - ❑Is it in contract?
  - ❑How does vendor demonstrate good online hygiene ? eg, Can they show internal policy ?

- ❑Who, in your organization, will manage the IoT system vendor contract?
  - ❑Central IT?
  - ❑Facilities?
  - ❑Tenant/customer dept ?
  - ❑Other? PD/security? CISO? CSO?

both

- ❑How many endpoint devices will be installed?
  - ❑Is there a patch plan?
  - ❑Who manages this?
  - ❑How much FTE will this require?

- ❑How many IoT systems are you already managing?
  - ❑Are you anticipating more in next 18 months?

- ❑Is the IoT vendor system implementation documented?
  - ❑Architecture diagram ?
    - ❑w/IP addresses & physical location of devices?
    - ❑w/required ports documented

- ❑Does this vendor's system have dependencies on other vendor systems?

- ❑Is a risk sharing agreement in place for shared institutional information?