Vetting Vendors: IoT Risk Due Diligence

GOVERNANCE

Is accountability for approval, monitoring, use and deployment of each IoT device and their associated applications assigned to an owner?

Do you know who owns IoT in your organization?

Is your Sourcing Policy approved by C-suite?

>>SIG U.2.4

ASSET MANAGEMENT+ INVENTORY

Do asset inventory and management processes include all physical objects with network connectivity? (IoT Devices)

Maintain an IoT inventory and require your third parties to do the same.

>>SIG U.2

RISK MANAGEMENT

Are IoT devices identified by scanning for non-802.11 wireless technologies like Bluetooth, Zigbee, and Z-Wave?

Are vendor products/services using IoT devices and applications to support outsourced functions / services vetted?

>>SIG U.2.1

NETWORK CONNECTIVITY

Who approves attaching IOT devices to a production network prior to their attachment How is this checked?

Do you require IoT devices to be placed on a segregated network?

INFOSECURITY + PRIVACY

Are IoT security / Privacy requirements included and validated as part of third party risk management requirements?

Know the business functions the IoT device support/perform

Ensure the IoT device has appropriate logical and physical security controls

Ensure IoT device can protect the data it collects, stores and transmits from unauthorized access and modification

When IoT devices are found to have inadequate security controls, are they removed as soon as possible and scheduled for replacement?

>>SIG U.2.5 + U.2.3

CONTRACTS

Are specific third-party IoT-related controls included in contract clauses, policies and procedures and monitored for compliance?

>>SIG U.2.5.1

INCIDENT RESPONSE PLAN

Does your IR plan address incidents caused by IoT devices?

Is your incident response plan tested?

RESOURCES

Does your organization allocate sufficient budget and staff?