IoT Risk and Recommended Controls

IoT devices are ubiquitous in personal and professional settings. Enterprises need to understand the unique risk associated with introducing IoT devices into their environment and the value to be gained.

Business value and organizational competitiveness can be gained as enterprises capitalize on the IoT capabilities of devices they purchase. Additionally, businesses can compete more effectively in the marketplace by providing IoT features in products they sell and incorporating them in service offerings.

Although specific risk depends on usage, guidance from NIST outlines some of the IoT-usage risk areas and recommended controls that an IT auditor should know about. Click the links below to learn more about each risk type.

Business Risk

Operational Risk

Business Risk

Potential risk types:

- Health and safety
- Regulatory compliance
- User privacy
- Unexpected costs

NIST controls:

- ID-BE.1: The organization role in the supply chain is identified and communicated.
- ID-BE-2: The organization place in critical infrastructure and its industry sector are identified and communicated
- ID-BE-3: Priorities for organizational mission, objectives and activities are established and communicated
- ID-BE-4: Dependencies and critical functions for delivery of critical services are established
- ID-BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)

Operational Risk

Potential risk types:

- Inappropriate access to functionality
- Shadow usage
- Performance

NIST controls:

- PR-AC-1: Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users, and processes
- PR-AC-2: Physical access to assets is managed and protected
- PR-AC-3: Remoted access is managed
- PR-AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- PR-BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)
- PR-DS-6: Adequate capacity to ensure availability is maintained