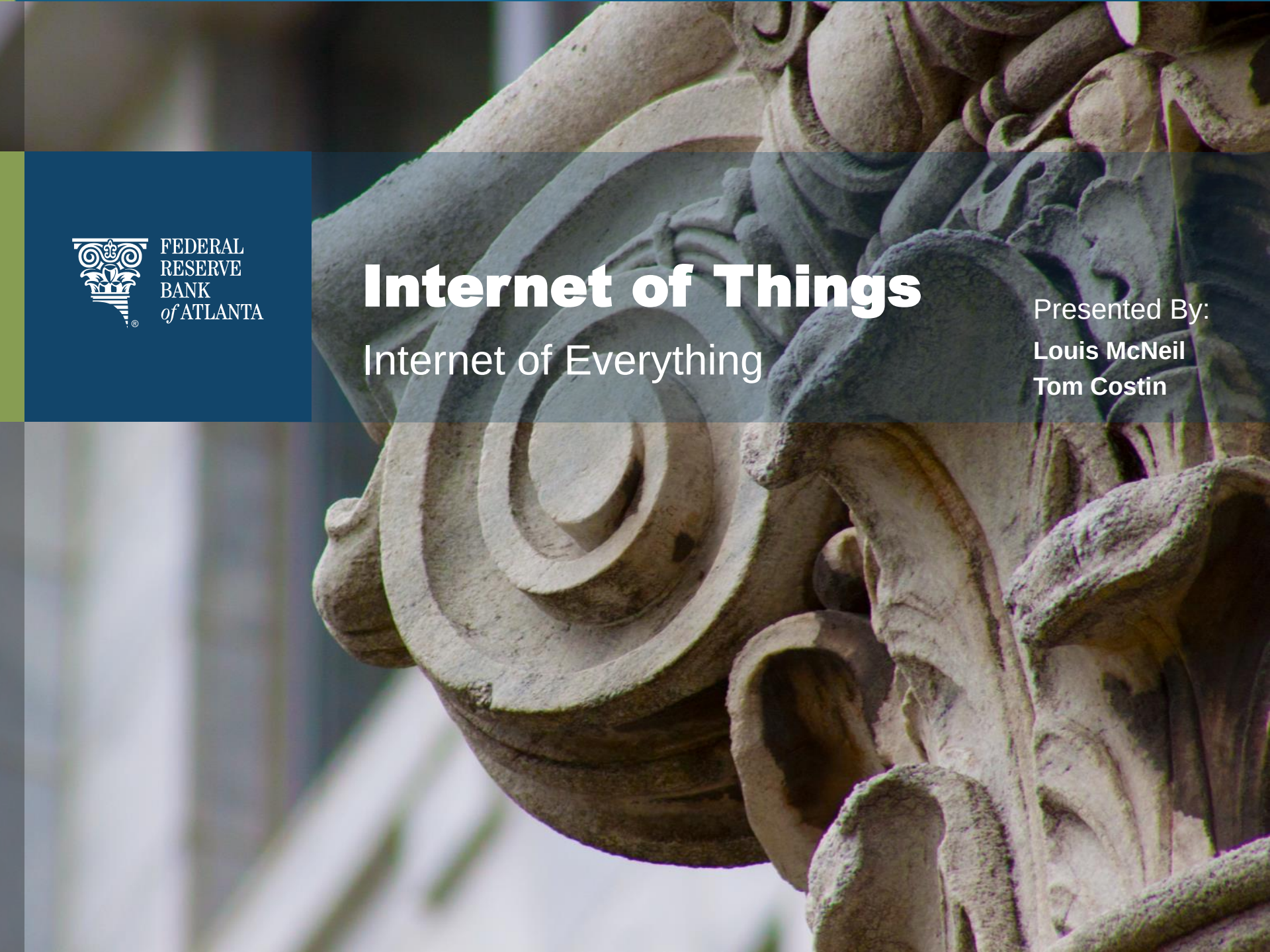


FEDERAL RESERVE BANK of ATLANTA

Internet of Things

Internet of Everything

Presented By:
Louis McNeil
Tom Costin

Agenda

FEDERAL RESERVE BANK of ATLANTA

Session Topics

- What is the IoT (Internet of Things)
  - Key characteristics & components of the IoT
- Top 10 IoT Risks
  - OWASP top 10
- Risk Assessment for IoT
  - Planning
  - Questions
  - Approach
- IT Controls for IoT
- Do's and Don'ts for IoT
- Question and Answer

So, what are these things anyway?

FEDERAL RESERVE BANK of ATLANTA

Network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment

Components of IOT

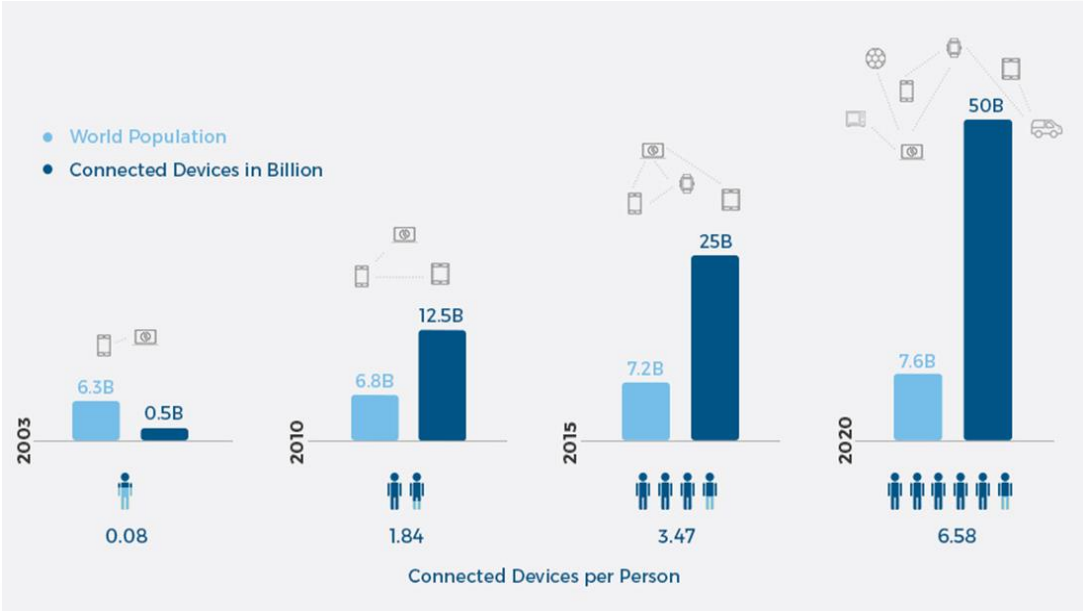
- **Data collection –** sensors and actuators that collect create store transmit and act on data
- **Connectivity –** WiFi, NFC, BlueTooth, NB-IoT, Wired, cellular, internal and external networks and services
- **People and Processes, risk management –** manage devices and data in alignment with strategic objectives and risk management goals

They're Everywhere

FEDERAL RESERVE BANK of ATLANTA

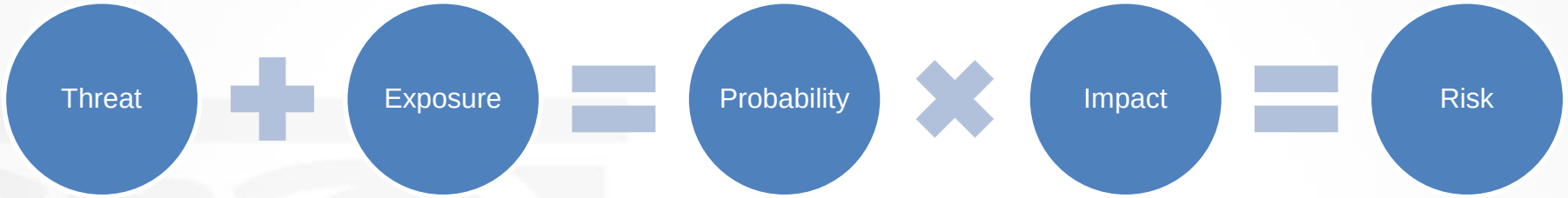
Internet of Things now, Internet of Everything soon. IPv6 means that every atom on the surface of the earth could be assigned an IP address

- Multifunction printers
- Building Management Systems
- Lighting controllers
- Smartboards
- Elevator controllers
- IP phones
- IP cameras
- Timeclocks
- IP radios
- Physical Actuators
- Smart plugs
- Smart Speakers



What Could Go Wrong?

FEDERAL RESERVE BANK of ATLANTA



Increasing attacks and vulnerabilities

Ineffective Control Environment

High Likelihood

Loss of CIA
Privacy
Physical Actuation

- **Reduced visibility into common vulnerabilities and enumerations** – these devices do not often appear in threat intelligence feeds
- **Reduced manufacturer support cycles** – Traditional 5-7 year support before EOL is uncommon in this space, especially in consumer oriented devices
- **Reduced configuration management controls**, practices and procedures, both technical and operational; including configuration checklists, ongoing assurance monitoring and inconsistent patching or the availability of updates
- **Limited technical expertise**, familiarity and consistency of control application
- **Low Maturity** of implementation and continuous monitoring of controls
- **Lack of understanding** and acknowledgement that all of these devices, almost without exception are Linux based servers that have similar security risks and threat vectors as many full-fledged traditional platform based information systems, with additional **sensing** capabilities

For the Lack of a Control, a Vulnerability

FEDERAL RESERVE BANK of ATLANTA

OWASP Top 10	Critical Security Controls (CSC)
Insecure Web Interface	**CSC 3:** Secure Configurations
Insufficient Authentication/ Authorization	**CSC 5:** Controlled Administrative Privileges
Insecure Network Services	**CSC 9:** Ports & Services **CSC 15:** Wireless Access Control
Lack of Transport Encryption	**CSC 11:** Secure Configurations
Privacy Concerns	**CSC 13:** Data Protection
Insecure Cloud Interface	**CSC 3:** Secure Configurations
Insecure Mobile Interface	**CSC 3:** Secure Configurations **CSC 18:** Application Software Security
Insufficient Configurability	**CSC 5:** Controlled Administrative Privileges **CSC 6:** Logging, Data Recovery
Insecure Soft/Firmware	**CSC 4:** Vulnerability Assessments **CSC 20:** Pen Testing & Red Team
Poor Physical Security	**CSC 14:** Controlled Access

Risk Assessment

FEDERAL RESERVE BANK of ATLANTA

Risk assessment is a process by which an auditor *identifies and evaluates* the *quantity* of the organization's risks and the *quality* of its controls over those risks

Risk Assessment Planning for IoT

FEDERAL RESERVE BANK of ATLANTA

Key Considerations

- Assessment should analyze the risks inherent in a given business line or process, the mitigating controls processes , and the resulting residual risk exposure to the institution
- Assessment should be well documented and dynamic, reflecting changes to the system of internal controls, infrastructure, work processes and new/changed business lines or laws and regulations.
- Assessment should consider thematic control issues, risk tolerance, and governance within the organization
- Assessment may be qualitative and quantitative and include factors such as impact/likelihood of an event occurring
- Assessment should be formally documented and supported with written analysis of the risks
- Assessment should include specific rationale for the overall auditable entity score
- Assessment results should be provided to the audit committee and include the most significant risks, as well as how those risks have been addressed in the audit plan

Risk Assessment Questions for IoT

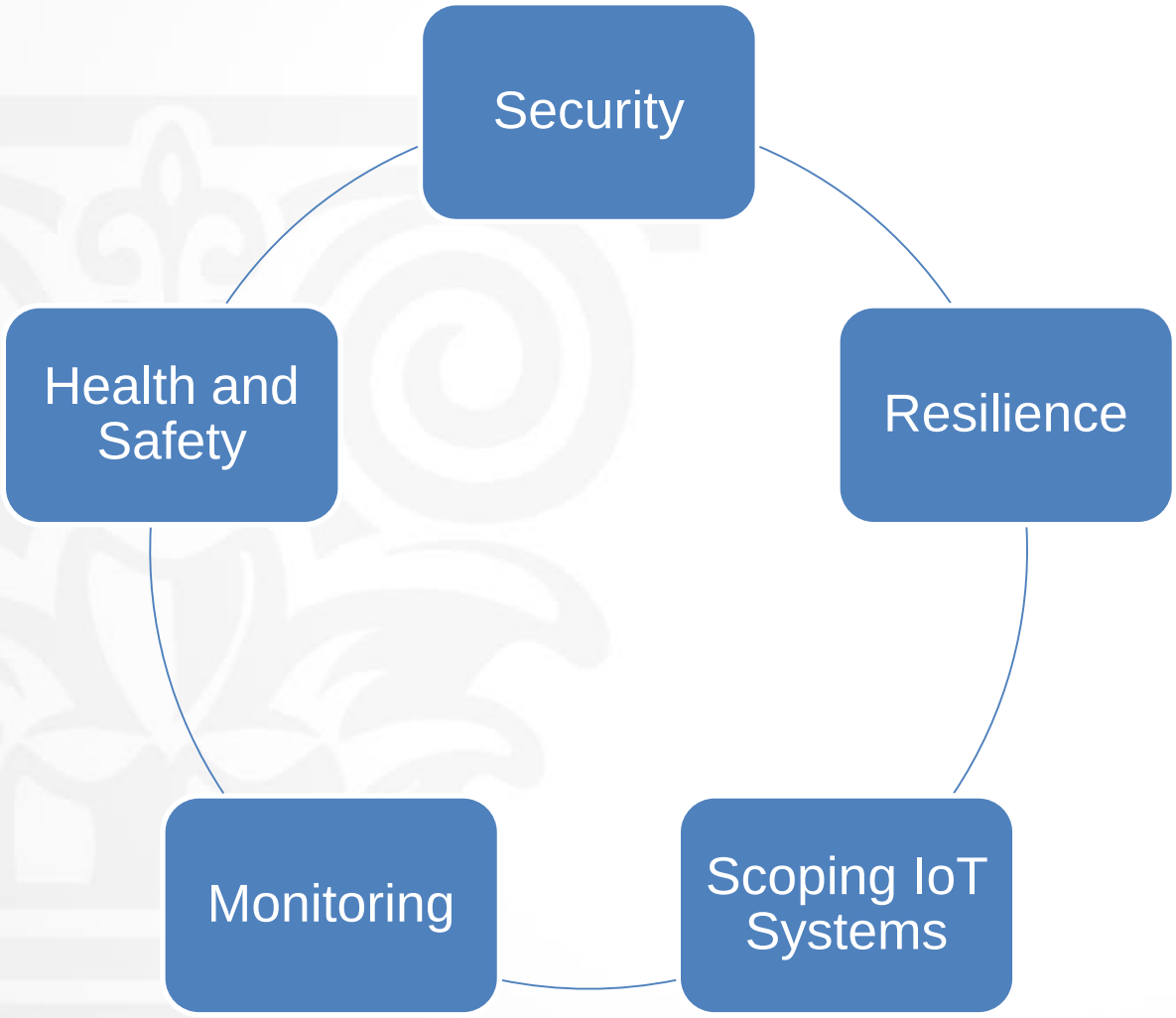
FEDERAL RESERVE BANK of ATLANTA

- How will the device be used from a business perspective?
- What business processes are supported and what business value is expected to be generated?
- What is the threat environment for the device?
- What threats are anticipated and how will they be mitigated?
- Who will have access to the device and how will their identities be established and proven?
- What is the process for updating the device in the event of a published attack or vulnerability?

- Who is responsible for monitoring for new attacks or vulnerabilities pertaining to the device?
- Have all risk scenarios been evaluated and compared to anticipated business value?
- What personal information is collected, stored or processed by the IoT devices and systems?
- Do the individuals about whom the personal information applies know that their information is being collected and used?
- Have they given consent to such uses and collection?
- With whom will the data be shared/disclosed?

Risk Assessment Approach for IoT

FEDERAL RESERVE BANK of ATLANTA



Security - Perform a vulnerability assessment of such devices and consider conducting penetration tests on those systems periodically.

Resilience - Assess whether controls are in place to recover IoT systems in the event of a failure.

Health and Safety - Assess whether such IoT systems have undergone sufficient testing using appropriate test cases before being deployed into production.

Monitoring - Assess whether adequate monitoring controls are in place and whether all such controls have been operating effectively over time.

Scoping of IoT systems - Assess where and when IoT systems are deployed by different departments and prioritize IoT systems audits according to their criticality and sensitivity.

IT Controls for IoT

FEDERAL RESERVE BANK of ATLANTA

IT Controls	Critical Security Controls (CSC)
Validate the existence and completeness of an inventory of IoT devices with designated owners	**CSC 1:** Inventory of Authorized and Unauthorized Devices
Ensure the use of Hardening Guides and checklists specific for each class of IoT device	**CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Verify that network diagrams exist depicting what segments of the network contain these devices and how they are isolated from segments containing proprietary, GLB, PCI, PII and HPI data.	**CSC 12:** Boundary Defense
Ensure configuration records are being captured (preferred automatically) for each IoT device attached to the corporate network	**CSC 4:** Continuous Vulnerability Management and Remediation

IT Controls for IoT

FEDERAL RESERVE BANK of ATLANTA

IT Controls	Critical Security Controls (CSC)
Validate that patching procedures have been developed for IoT devices, and that devices which can't or don't allow for firmware updates are documented in exception management with tested compensating controls	**CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers **CSC 11:** Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
Verify that user awareness training has been provided to everyone who installs, maintains, or uses these devices	**CSC 17:** Security Skills Assessment and Appropriate Training to Fill Gaps
Assess the completeness of IoT device activity monitoring and logging procedures	**CSC 6:** Maintenance, Monitoring, and Analysis of Audit Logs
Ensure the Incident Response Plan articulates how to conduct triage, analysis, containment, and eradication of various IoT targeted exploits, including the results of a round table exercise that involves an IoT scenario	**CSC 19:** Incident Response and Management **CSC 20:** Penetration Tests and Red Team Exercises

IoT Do's

FEDERAL RESERVE BANK of ATLANTA

Do's	
	Prepare a threat model.
	Evaluate business value.
	Holistically evaluate and manage risk.
	Balance risk and rewards.
	Notify all stakeholders of anticipated usage.
	Engage with business teams early.
	Gather all stakeholders to ensure engagement and thorough planning.
	Look for points of integration with existing security and operational protections.
	Examine and document information that is collected and transmitted by devices to analyze possible privacy impacts.
	Discuss with relevant stakeholders when, how and with whom that information will be shared and under what circumstances.

IoT Don’ts

FEDERAL RESERVE BANK of ATLANTA

Don’ts	
	Deploy quickly without consulting business or other stakeholders.
	Disregard existing policy requirements, such as security and privacy.
	Ignore regulatory mandates.
	Assume vendors (hardware, software, middleware or any other) have thought through your particular usage or security requirements.
	Disregard device-specific attacks or vulnerabilities.
	Discount privacy considerations or "hide" data that are collected/transmitted from end users.

Resources

FEDERAL RESERVE BANK of ATLANTA

OWASP Internet of Things Security Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main

OWASP Foundational Security Checklist
https://www.owasp.org/index.php/IoT_Security_Guidance#Consumer_IoT_Security_Guidance

CIS IoT Security Companion
https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf?x60581

IoT Security Foundation Security Compliance Framework
https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

FEDERAL RESERVE BANK of ATLANTA