Understanding the FDA Cybersecurity Final Guidance

By: Gerald Rigdon

Fellow, R&D Software Engineering
Boston Scientific
gerald.rigdon@bsci.com

Disclaimer

Official Documentation

Guidance:

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

Other:

https://www.fda.gov/search?s=Cybersecurity+

Reaction to the Guidance

Cybersecurity Statutory Requirements

1. Not just an update to Code of Federal Regulations!
2. Amended the FD&C Act – Section 524B!

   https://www.congress.gov/117/plaws/publ328/PLAW-117publ328.pdf

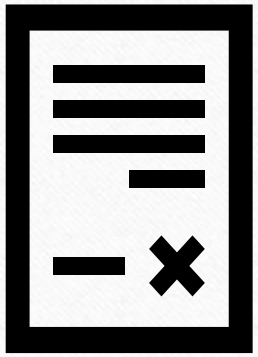
SEC. 3305. ENSURING CYBERSECURITY OF MEDICAL DEVICES.

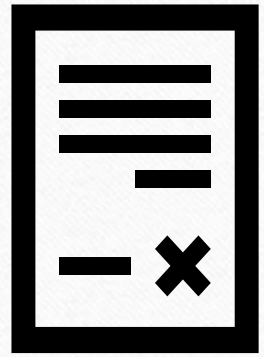
(a) IN GENERAL.—Subchapter A of chapter V of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 351 et seq.) is amended by adding at the end the following:

"SEC. 524B. ENSURING CYBERSECURITY OF DEVICES.

"(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as the Secretary may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

Statutory Requirements Continued





PUBLIC LAW 117–328—DEC. 29, 2022 136 STAT. 5833

"(b) CYBERSECURITY REQUIREMENTS.—The sponsor of an application or submission described in subsection (a) shall—

"(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures; Plan.

"(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address— Processes. Procedures. Updates.

"(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

"(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

"(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

"(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure. Compliance.

"(c) DEFINITION.—In this section, the term 'cyber device' means a device that—

"(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;

"(2) has the ability to connect to the internet; and

"(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

The 4 Requirements Per Section 524B

1. Submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including **coordinated vulnerability disclosure and related procedures**

2. Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and **make available postmarket updates and patches** to the device and related systems to address
   A. On a reasonably justified regular cycle, known unacceptable vulnerabilities; and
   B. As soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks

3. Provide to the Secretary a **software bill of materials**, including commercial, open - source, and off-the-shelf software components

4. **Comply with such other requirements as the Secretary may require** through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure

Definition Per Section 524B

524B(c) defines a Cyber Device as a device that:

1. Includes software that a sponsor has validated, installed, or authorized **as a device or in a device**;

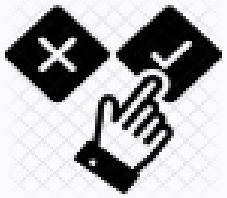
2. Has **ability to connect** to the internet; and

3. Contains any such technological characteristics a sponsor has validated, installed, or authorized that **could be vulnerable to cybersecurity threats**

All 3 must be true

Applicability - Submission Types, etc.

- Premarket Notification (510(k)) submissions
- De Novo Classification Requests
- Premarket Approval Applications (PMAs) and PMA supplements
- Product Development Protocols (PDPs)
- Investigational Device Exemption (IDE) submissions
- Humanitarian Device Exemption (HDE) submissions
- Biologics License Application (BLA) submissions
- Investigational New Drug (IND) submissions



"This guidance document is applicable to devices with cybersecurity considerations, including but not limited to devices that have a device software function or that contain software (including firmware) or programmable logic."

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-device-software-functions

Draft vs Final Guidance - Key Changes

Final was issued September 27, 2023

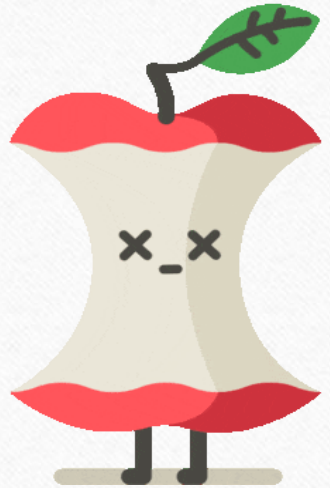
- Expanded Scope
  - Included CBER submission types (BLA and IND)
  - Included considerations for combination products
  - Added elements associated with the requirements under Section 524B of FD&C

- Software Bill of Materials (SBOM)
  - Alignment with 2021 NTIA SBOM Framing Document
  - Supporting materials can be separate from the SBOM

- Structural Changes
  - New subsections, Interoperability
  - Added Appendix 4 to clarify premarket submission documentation

Core Principles in the Guidance

- Security is part of device safety Quality System Regulation (QSR) 21 CFR Part 820
- Secure Design using a Secure Product Development Framework (SPDF)
- Transparency with proper labeling and technical information for users
- Submission documentation that should scale with cybersecurity risk



Security Objectives – Revisiting the Triad

CIA vs CAAAU

C – Confidentiality

A – Authenticity

A – Authorization

A – Availability

U – Updateability

"Authenticity" replaces "Integrity" given it is a broader term that includes integrity.

"Authorization" is an important addition since privileges and permission for access are critical for device security.

"Updateability" emphasizes the need for medical device manufacturers to be able to respond to discovered vulnerabilities with flexible designs that facilitate securely loading newer software versions into their medical devices that mitigate or address those vulnerabilities.

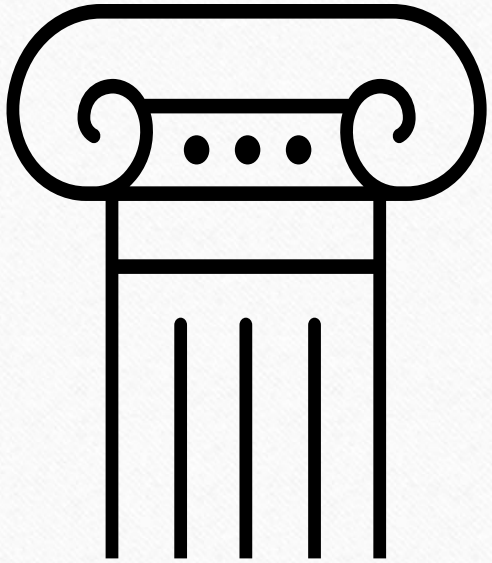
Secure Product Development Framework (SPDF)

3 Pillars

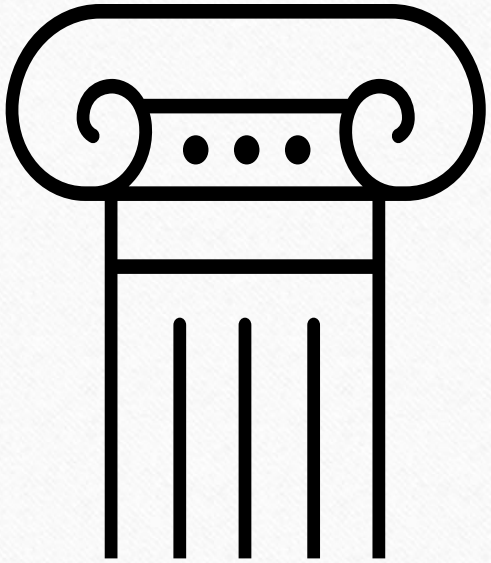
SPDF ***may*** satisfy QSR?

SPDF ***may*** be satisfied by frameworks like JSP or IEC 81001-5-1

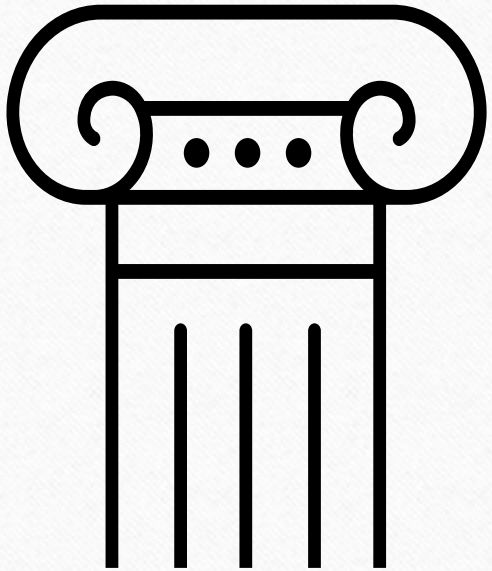
SECURITY RISK MANAGEMENT



SECURITY ARCHITECTURE



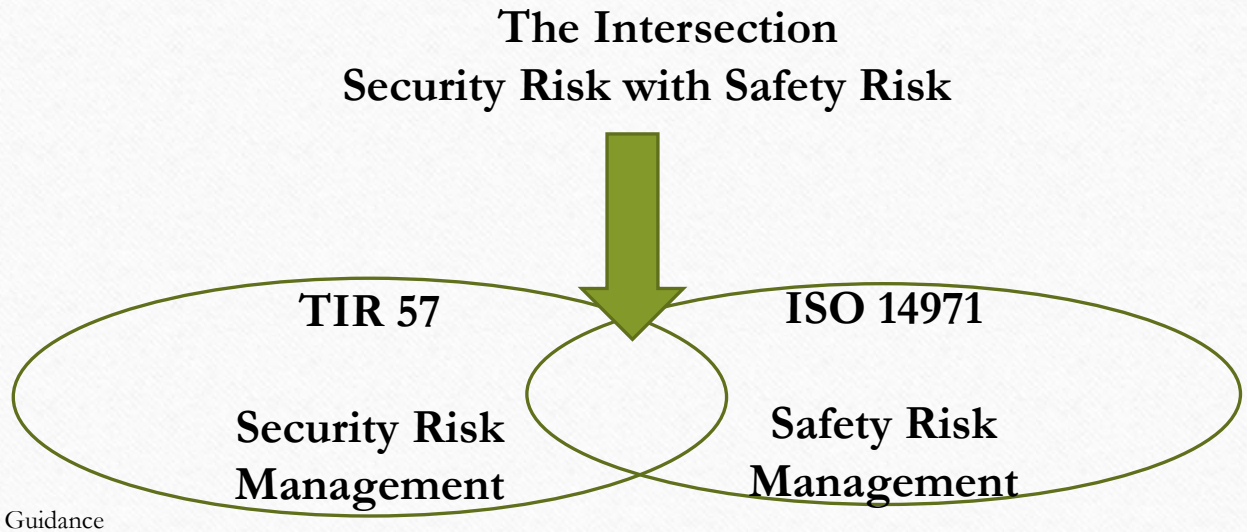
CYBERSECURITY TESTING



SPDF Pillar #1 - Security Risk Management

- ISO 14971 for safety risk management

- TIR 57 for pre-market security risk management
  - TIR 97 (post-market)
  - SW96 (new standard combining pre and post market or TPLC)



Security Risk Management… Big Picture

- Security risks are not probabilistic…focus on exploitability
- Design validation and Risk Analysis per CFR Title 21 Section 820.30 (g)

"Each manufacturer shall establish and maintain procedures for validating the device design. Design validation shall be performed under defined operating conditions on initial production units, lots, or batches, or their equivalents. Design validation shall ensure that devices conform to defined user needs and intended uses and shall include testing of production units under actual or simulated use conditions. Design validation shall include ***software validation and risk analysis****, where appropriate. The results of the design validation, including identification of the design, method(s), the date, and the individual(s) performing the validation, shall be documented in the DHF."*

Security Risk Management… Third Party Software

- Suppliers must conform to manufacturers requirements per 21 CFR 820.50
- Custodial control of source code encouraged (may be license restrictions, etc.)
  - If no control should have a plan of how third-party software can be updated or replaced
- Other References: 21CFR 820.30 (g), (j), and 820.181

Security Risk Management… SBOM

- OTS and Network Device FDA guidance document describe SBOM content
- Information consistent with elements identified in NTIA framing document

Supporting Materials in Submission:

- The software level of support provided through monitoring and maintenance from the software component manufacturer
- The software component's end-of-support date
- Any known vulnerabilities
  - A safety and security risk assessment of each known vulnerability
  - Details of applicable safety and security risk controls to address the vulnerability

Threat Modeling - Focus & Differences

Identify system risks and mitigations as well as inform the pre- and post-mitigation risks considered as part of the security risk assessment.

State any assumptions about the system or environment of use (e. g. hospital networks are inherently hostile, therefore manufacturers are recommended to assume that an adversary controls the network with the ability to alter, drop, and replay packets).

FDA Guidance

- Supply chain
- Manufacturing
- Deployment
- Interoperability
- Maintenance
- Decommission

IEC 81001-5-1

- Flow of information
- Trust boundaries
- Data stores
- Interacting external entities
- Internal and external communication protocols
- Externally accessible physical ports
- Circuit board connections
- Etc.

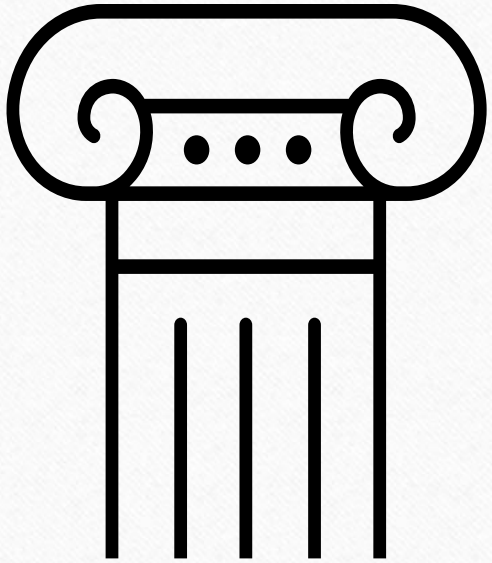
Secure Product Development Framework (SPDF)

3 Pillars

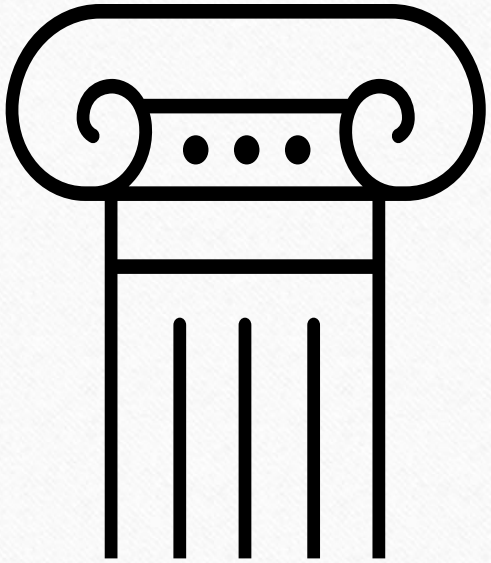
SPDF ***may*** satisfy QSR?

SPDF ***may*** be satisfied by frameworks like JSP or IEC 81001-5-1

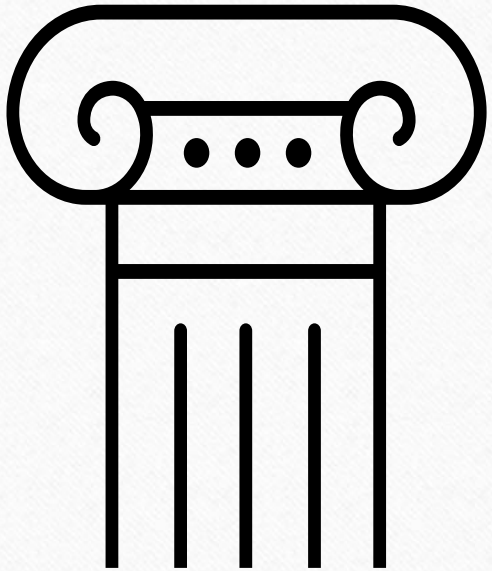
SECURITY RISK MANAGEMENT



SECURITY ARCHITECTURE

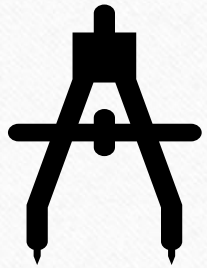


CYBERSECURITY TESTING

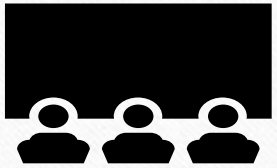


SPDF Pillar #2 - Security Architecture

- Implementation of Security Controls
  - Authentication & Authorization
  - Cryptography
  - Code, Data, Execution Integrity
  - Confidentiality
  - Event Detection and Logging
  - Resiliency and Recovery
  - Updatability and Patchability



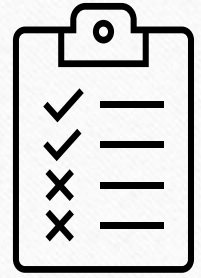
- Security Architecture Views
  - Global
  - Multi-patient harm
  - Updatability
  - Use Case



Other References: 21CFR 820.30 (c), (d)

SPDF Pillar #3 - Cybersecurity Testing

- Security Requirements
- Threat Mitigation
- Vulnerability Testing
- Penetration Testing



- Other References: 21CFR 820.30 (f), (g)

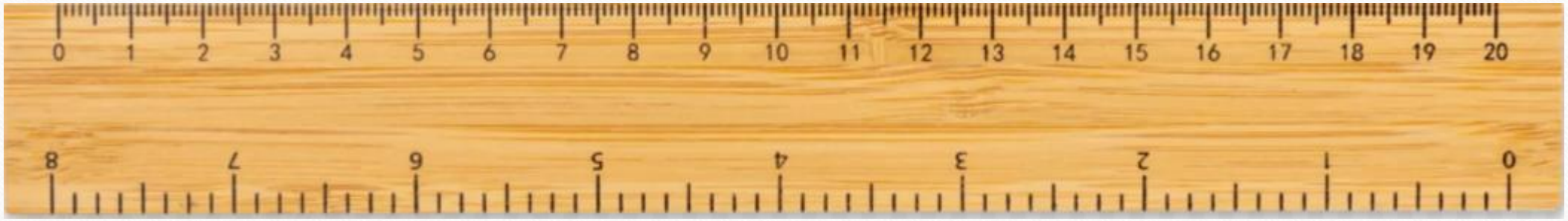

SPDF
Security Requirements
Security Architecture
Threat Modeling
Security Risk Assessment
Security Control Verification
Authentication
Authorization
Cryptography
Code & Data Integrity
Confidentiality
Event Detection & Logging
Resiliency & Recovery
Updatability / Patchability

Submission Documentation – Appendix 4

- Risk Management Report
  - Threat Model
  - Risk Assessment
  - SBOM
  - Vulnerability Assessment
  - Unresolved Anomalies
  - Traceability
- Measures and Metrics
- Architecture Views
- Testing
- Labeling
- Management Plans

Scaling With Risk

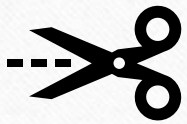
Less Documentation But What About SPDF?



Few and simple interfaces
No sensitive data
Non-network connectable
Non-network connected
Single use devices

Network connectable
Network connected
New systems & tech
Multiple interfaces
Sensitive data

Excerpts from the Guidance



"Device cybersecurity design and documentation are expected to **scale** with the **cybersecurity risk of that device**."

"Therefore, the recommendations in this guidance regarding information to be submitted to the FDA are intended to address the **cybersecurity risk**, as assessed by the cybersecurity risk assessment during development of a device and are expected to **scale** based on the cybersecurity risk."

"These views can therefore be an effective way to provide threat modeling information to FDA and will naturally **scale** the documentation provided with the cybersecurity **risk of the device**."

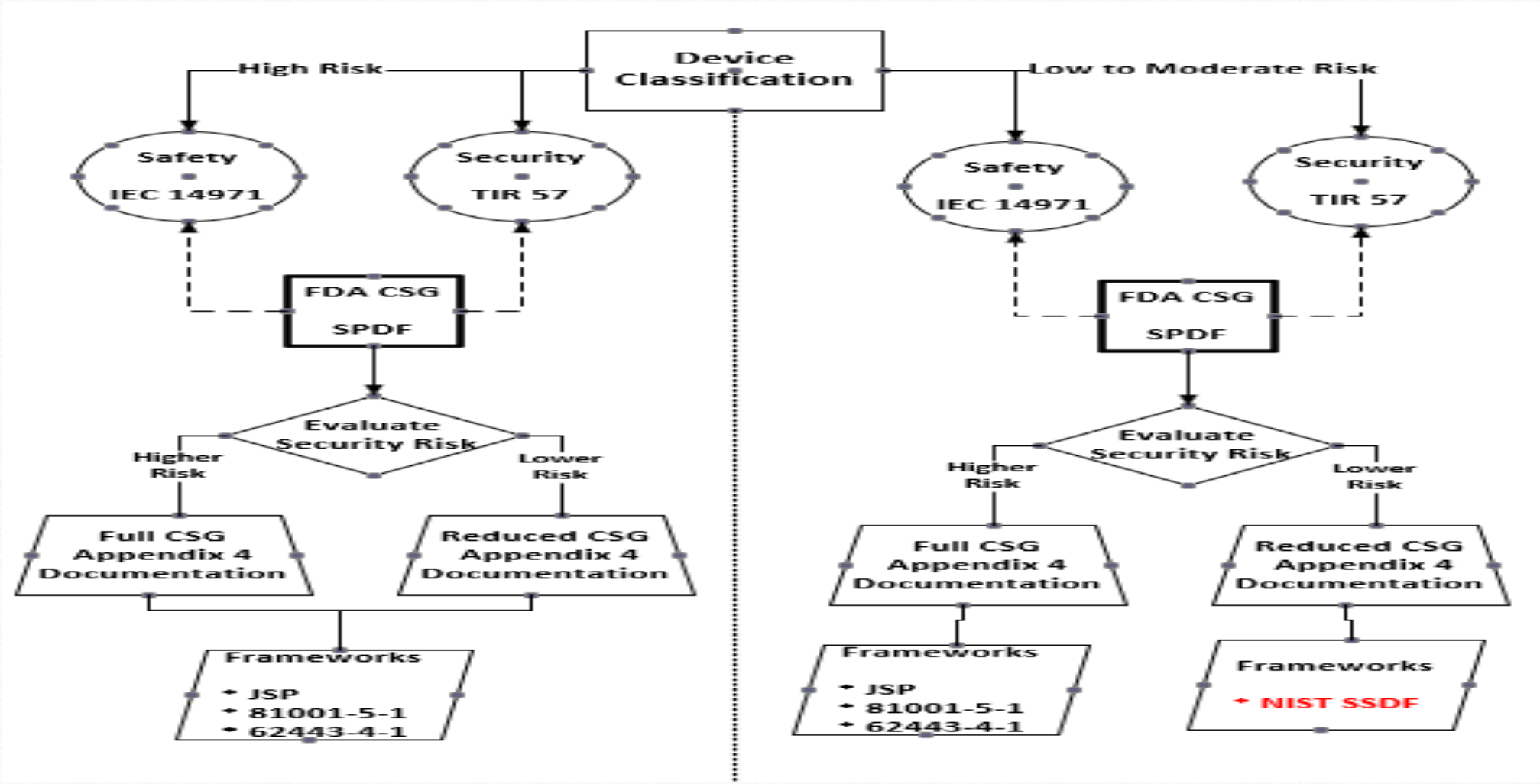
"The extent of these security views in a premarket submission is expected to **scale** based on the architecture and potential cybersecurity **risk posed to the device**."

"The number of security use cases that should be assessed will **scale** with the cybersecurity complexity and **risk of the device."**

"As stated in Section IV.D. and throughout the guidance, device cybersecurity design and documentation are expected to **scale** with the cybersecurity **risk of that device**. While documentation breadth is expected to **scale**, each type of documentation identified throughout the guidance is recommended for all premarket submissions for devices with potential **cybersecurity risks."**

"The below documentation will naturally **scale** with the level of **cybersecurity risk**."

Considering NIST SSDF – A Lighter Weight SPDF



Additional References To Consider!

- My Conference Paper

  Rigdon, G. (2024, January). *FDA CYBERSECURITY GUIDANCE FOR MEDICAL DEVICESA BRIEF ON THE LAW, SPDF, JSP, AND NIST SSDF*

- MDM NIST SSDF Profile….Work in progress, email me if you want to know more