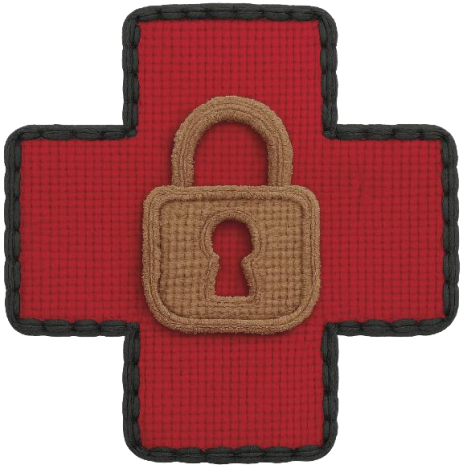
Northeastern University



Medical Device Cybersecurity – Week 10

03/10/2026

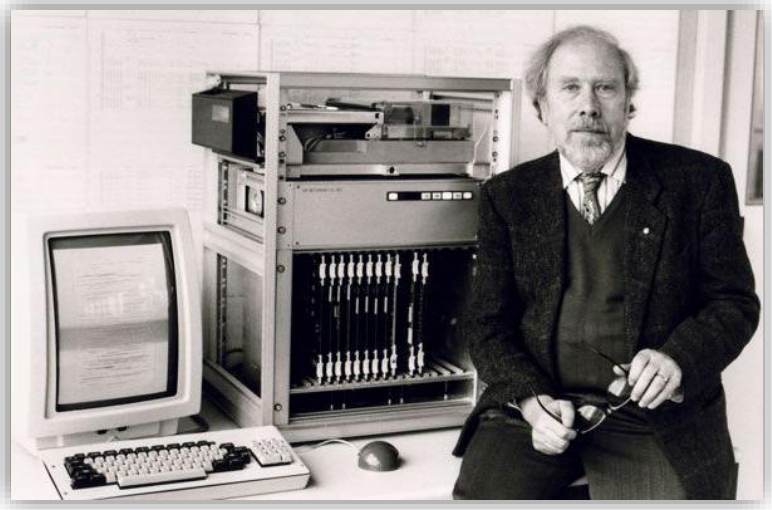
Manufacturer vs Operator Perspective

Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- General Introduction & Lifecycle Concept
- Total Product Lifecycle (TPLC)
- Pre and Postmarket Activities
- Example: SBOM

"Software is getting slower more rapidly than hardware becomes faster" – Wirth's Law (1995)



Shared Security Responsibilities

Manufacturer:

- Design secure devices
- Obtain market approval
- Manufacture devices securely
- Service & support:
  - Postmarket surveillance & mgmt
  - Secure service infrastructure
- EOL/EOS management / risk transfer

Operator (e.g., hospital):

- Security in procurement
- Secure installation & integration
- Ensure compliance with HIPAA
- Security maintenance
- Decommissioning

Where things may overlap:

- Manufacturer may cloud-host customer (incl. patient) data
- Hospital may contract maintenance to 3rd party or back to manufacturer
- Devices may be leased or loaned

Cybersecurity Perspectives

Generally (with some overlap) - manufacturer: implement security; HDO: manage and maintain security

Manufacturer (MDM)	Healthcare Organization (HDO)

• Governance / Quality System
• Secure Development Lifecycle (SDLC)
• Security Principles and Practices
• Identify Security Requirements
• Risk Management
  • Threat Modeling
  • Vulnerability Assessment
  • Supply Chain Management
• Security Testing and Traceability
• Regulatory Filing
• Documentation & Labeling
  • SBOM, MDS^2, Security IFU
• Postmarket Management
  • Surveillance
  • Vulnerability Management
  • Mitigation & Communication
  • EOL/EOS Management
	• Replacement Planning
	• Procurement and Contracting
	• Incoming Testing
	• Integration Best Practices
	  • Clinical integration
	  • Secure networking
	  • Security integration
	• Cyber Hygiene:
	  • Training
	  • Use
	  • Media handling
	• Operation:
	  • Asset Visibility & Risk Management
	  • Maintenance (incl. cybersecurity)
	  • Change and Vulnerability Mgmt.
	  • Incident Response
	• Decommissioning

Specific requirements and implementation will vary widely depending on need and capabilities.

Device Maintenance – Legal Requirements

U.S. Centers for Medicare & Medicaid Services (CMS) State Operations Manual:

"In order to ensure an acceptable level of safety and quality, the hospital must identify the equipment required to meet its patients' needs … In addition, the hospital must make adequate provisions to ensure the availability and reliability of equipment needed for its operations and services. Equipment includes both facility equipment … and medical equipment, which are devices intended to be used for diagnostic, therapeutic or monitoring care provided to a patient by the hospital (e.g., IV infusion equipment, ventilators, laboratory equipment, surgical devices, etc.)."

Centers for Medicare & Medicaid Services:
"Pub. 100-07 State Operations Provider Certification", Feb. 21, 2014
https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R103SOMA.pdf

However, some or all maintenance activities and responsibilities may be contracted out / back to an Independent Service Provider (ISP) or the manufacturer.

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- General Introduction & Lifecycle Concept
- Total Product Lifecycle (TPLC)
- Pre and Postmarket Activities
- Example: SBOM

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches

HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

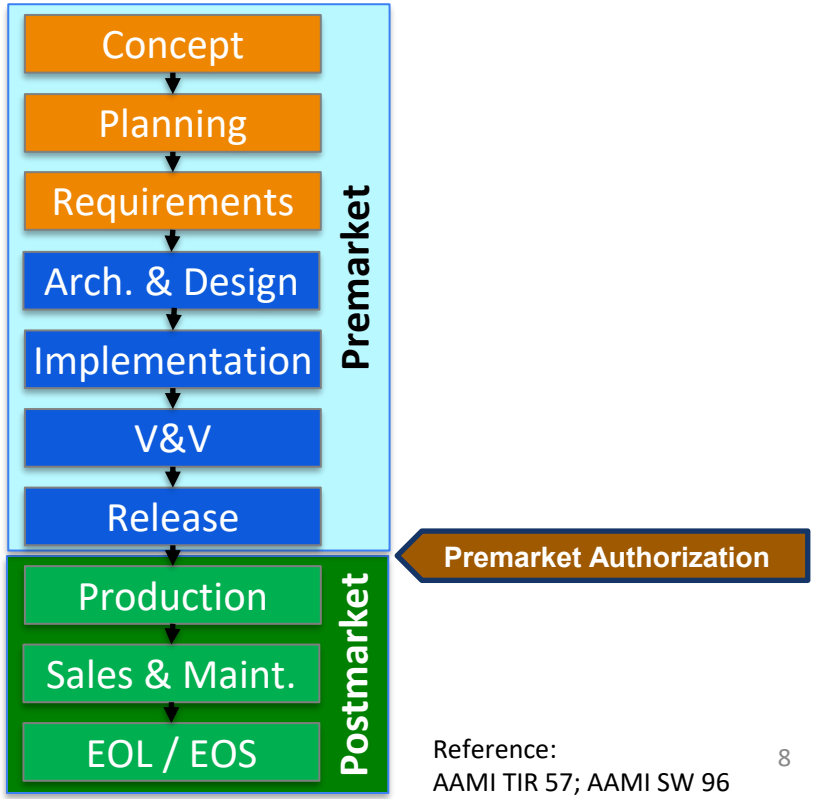
Manufacturer “Secure Development Lifecycle” (SDLC)

Find common ground across international regulators:

- SDLC per IEC 81001-5-1
  - FDA recognized consensus standard
  - Expected harmonized standard in the EU
- ISO 14971 as umbrella for risk management. Cybersecurity:
  - Premarket: AAMI TIR 57 and SW 96
  - Postmarket: AAMI TIR 97

Establish measures for managing cybersecurity risks:

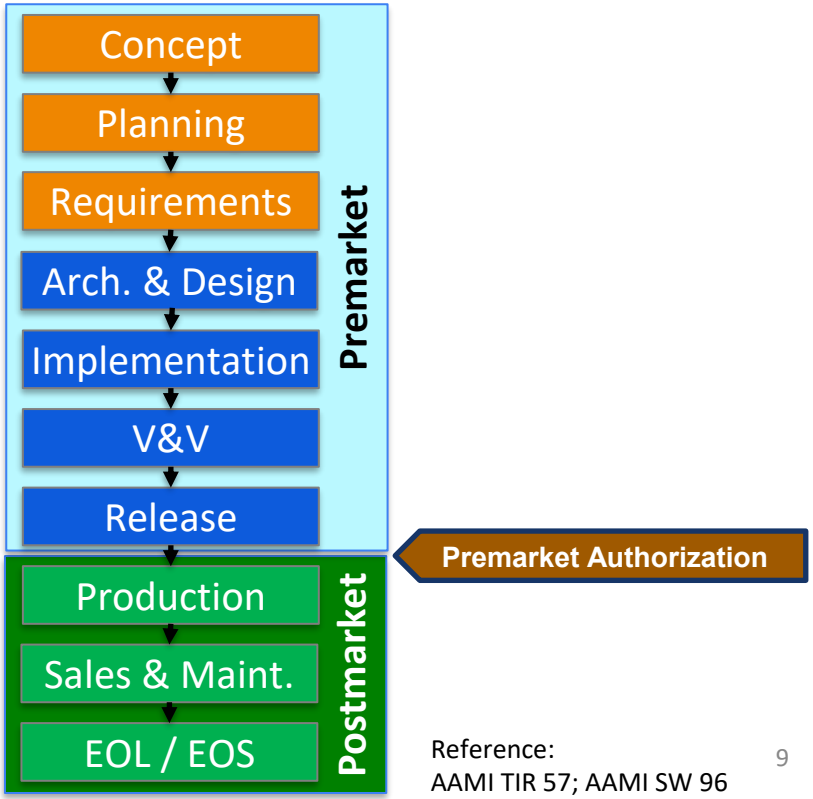
- Apply across SDLC
- Manage your supply chain risk
- Threat Modeling as early as possible
- Continual testing at integration stages
- Apply state-of-the-art security requirements, e.g.:
  - IEC 80001-2-2
  - Secure coding guidelines (e.g., OWASP)
  - Regulatory guidances via recognized practices, e.g., JSP V2)



Reference:
AAMI TIR 57; AAMI SW 96

Manufacturer “Secure Development Lifecycle” (SDLC)

Concept	• Clinical need, general concept, integration • Target markets and security context
Planning	• Applicable processes, tools, training, … • Security principles and practices
Requirements	• Detailed security requirements • General risk considerations and mitigation strategies
Architecture & Design	• High level, initial build vs buy decisions • Initial risk assessment activities (e.g., threat modeling)
Implementation & Integration	• Code development, integration, code analysis and testing • Continual risk management and testing • Security documentation (SBOM, testing, IFUs, …)
Verification & Validation	• Verification – testing against requirements (fuzz, ..) • Validation – objective security assessment (pen testing)
Release	• Obtain market approval based on final documentation • Secure transfer to production
Production	• Secure manufacturing • Controlled update / version maintenance
Sales & Maintenance	• Security documentation • Patches, updates, … and related communication
EOL / EOS	• Continual communication of change in EOS dates • At EOS – formal risk transfer



Reference:
AAMI TIR 57; AAMI SW 96

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- General Introduction & Lifecycle Concept
- Total Product Lifecycle (TPLC)
- Pre and Postmarket Activities
- Example: SBOM

Medical Device Security – Practices and Strategies

Document and provide traceability:

- Security requirements
- Identified risks
- Implemented controls and mitigations
- Confirmation through testing

Continual and comprehensive security analysis and testing:

- SAST, DAST, code reviews, misuse and abuse cases, attack surface analysis, vulnerability scanning, SCA, malformed input testing (fuzzing), penetration testing (independent).

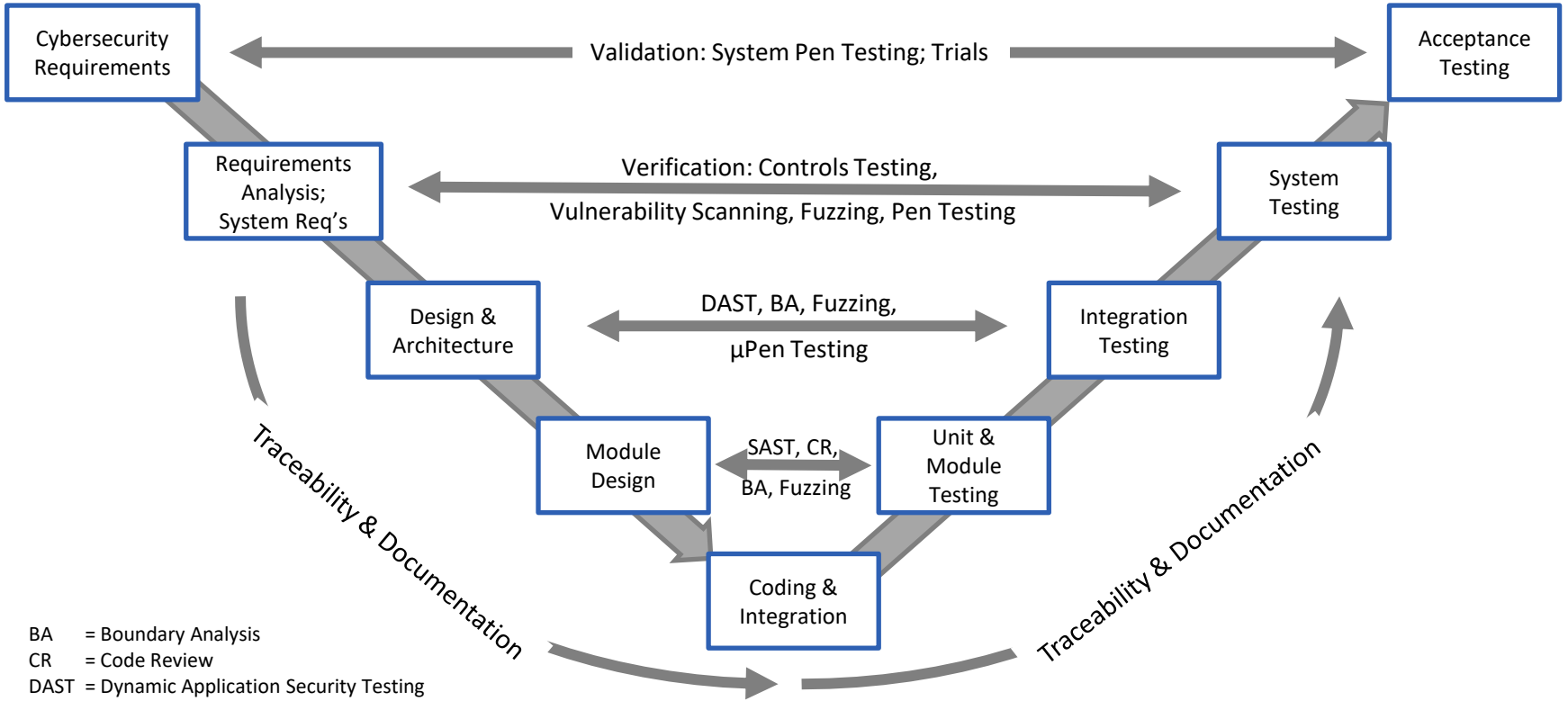
Best practices to foster cross-Atlantic and international cooperation in regulatory compliance:

- Markets may have similar requirements, but some specific details vary.
- Avoid surprises:
  - E.g., usability tests must be done with US citizens
  - Consult where needed

SAST = Static Application Security Testing; DAST = Dynamic Application Security Testing; SCA = Software Composition Analysis

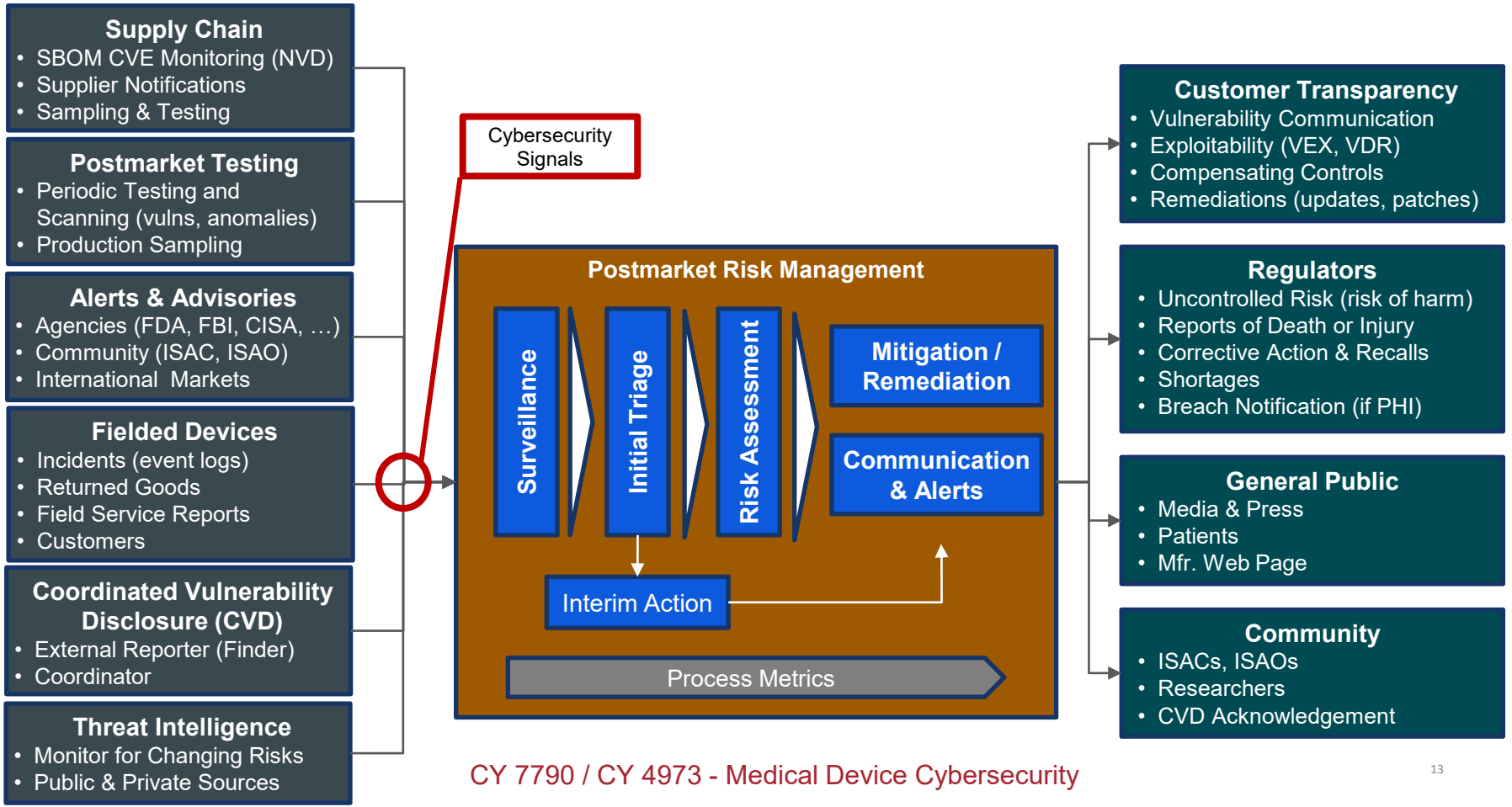
MDM Premarket Activities

Alignment of Development and Testing

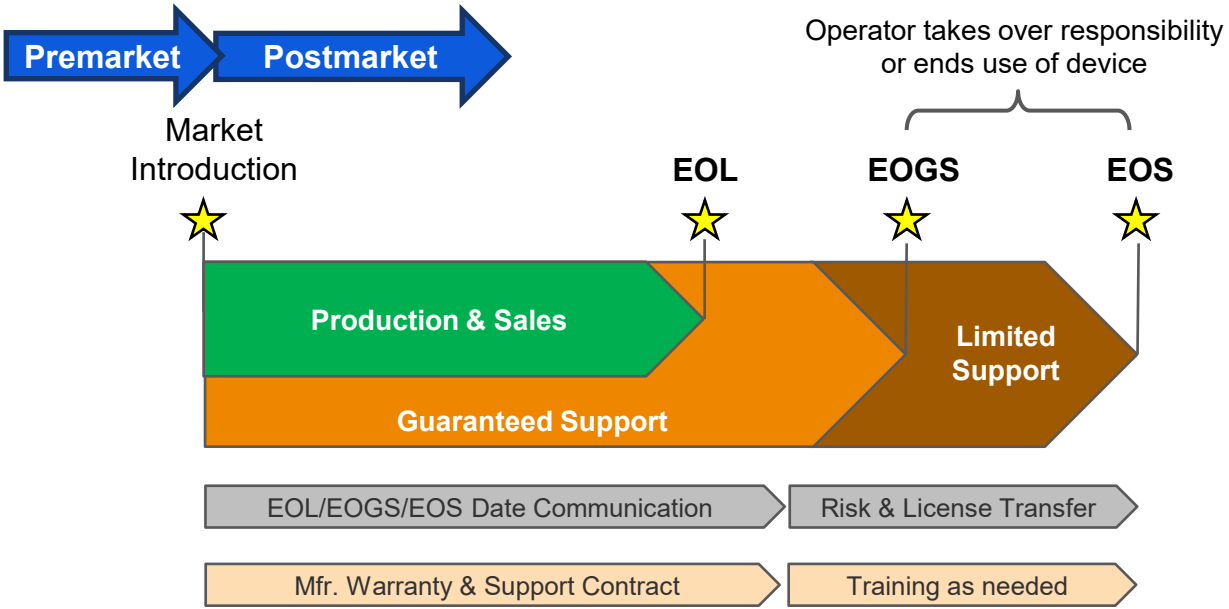


BA = Boundary Analysis
CR = Code Review
DAST = Dynamic Application Security Testing
SAST = Static Application Security Testing
µPen = Pen Testing at the subsystem level

General Cybersecurity Postmarket Risk Management Flow



Postmarket in the End-of-Life (EOL) Context



Market Introduction typically requires some formal approval by regional regulators (AKA premarket authorization).

EOL: (1) the manufacturer no longer sells the product, and (2) the product has gone through a formal EOL process, including notification to operators and/or users.

EOGS: Point after which the manufacturer no longer guarantees full support.

EOS: Point after which the manufacturer has terminated all support activities.

But manufacturer recall / corrective action obligations do **not** end with EOS!

Decommissioning: End-of-Use from the Hospital / Operator perspective

Source: HSCC: "Health Industry Cybersecurity-Managing Legacy Technology Security (HIC-MaLTS)" https://healthsectorcouncil.org/legacy-tech-security/

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- General Introduction & Lifecycle Concept
- Total Product Lifecycle (TPLC)
- Pre and Postmarket Activities
- Example: SBOM

Software Bill of Materials (SBOM)

"A formal inventory of software components and dependencies, information about those components, and their hierarchical relationships. The software components in an SBOM include, but are not limited to, commercial, open source, off-the-shelf, and custom software components."

FDA Cybersecurity Premarket Guidance, June 2025

Purpose of SBOM (per FDA)

SBOM as part of the documentation required to comply with the requirements of Section 524B of the FD&C Act – new devise and modifications.

A tool to help manage supply chain risk as well as clearly identify and track the software incorporated into a device.

Part of the Security Risk Management Report should include:

- Summarize the risk evaluation methods and processes,
- Detail the residual risk conclusion from the security risk assessment,
- Detail the risk mitigation activities undertaken as part of a manufacturer's risk management processes, and
- Provide traceability between the threat model, cybersecurity risk assessment, SBOM, and testing documentation.

Customer documentation (i.e., labeling): An SBOM … to effectively manage assets, to understand the potential impact of identified vulnerabilities to the medical device system, and to deploy countermeasures to maintain the device's safety and effectiveness. Manufacturers should provide SBOM information to users on a continuous basis.

What SBOM Enables

- Risk management during pre- and post-market
  - Identify vulnerabilities in the supply chain
  - Version and change management
- Software processes
  - Component EOL/EOS management
  - CI/CD integration
- Business functions
  - Contract and License management
  - Understand export controls
- Customer facing
  - Security during procurement
  - Vulnerability, EOL/S communication
  - Risk transfer

SBOM Common Formats, Content, and Challenges

Common Formats:

- CycloneDX, SPDX
- JSON, XML, YAML

Content defined:

- NTIA Framing Document (2021), NTIA Minimum Elements (2021), CISA Framing Document (2024)
- FDA - NTIA Framing plus Software level of support and Component End-of-Support

Challenges:

- SBOM availability and supplier adherence
- Complexity and depth as well as **sheer volume of vulnerabilities**
- Challenges with identifying components and matching them to vulnerabilities
- Data source(s) - most commonly NVD (but enrichment falling behind since early 2014, 26k behind)
- Definition of “risk” vs. raw “vulnerability score” (CVSS)
- The need to **triage vulnerabilities** in the context of the implementation and use case.
- Vulnerability communication (exploitability, severity in current implementation and use context)
- Missing data common sources for license data and **Level of Support / EOS**

Regulations and Standards that Stipulate SBOM

US FDA Cybersecurity Premarket Guidance (June 2025):

- Building on Section 524B of the FD&C Act
- 524B(b)(3): Provide machine-readable SBOM for all “cyber devices” (or justification why not).
- To support pre- and post-market risk management.
- Emphasizes traceability between threat model, risk assessment, controls, SBOM, and testing.
- 3rd party (purchased, licenses, open source) and manufacturer-developed components.
- Include in customer documentation to help manage their assets, understand potential impact, and to deploy countermeasures to maintain the device’s safety and effectiveness.

IMDRF N73 WG “Principles and Practices for SBOM for Medical Device Cybersecurity”:

- Detailed inventory reports: component name, origin, version, and build.
- Commercial, open-source, or off-the-shelf components.
- SBOM to help operators manage assets and risks, support purchasing decisions.

IEC 62304 “Medical device software — Software life cycle processes”:

- Document SW processes, incl. identification and management of software components.
- SBOM as list of third-party and open-source components, versions, and dependencies.

FDA SBOM Content

- FDA references 2021 NTIA "Framing Software Component Transparency" document, not NTIA Minimum Elements nor updated CISA 2024 Framing document (3rd edition).
- SBOM Elements required per FDA:
  - Author Name
  - Timestamp
  - Supplier Name
  - Component Name
  - Version String
  - Component Hash*
  - Unique Identifier
  - Relationship

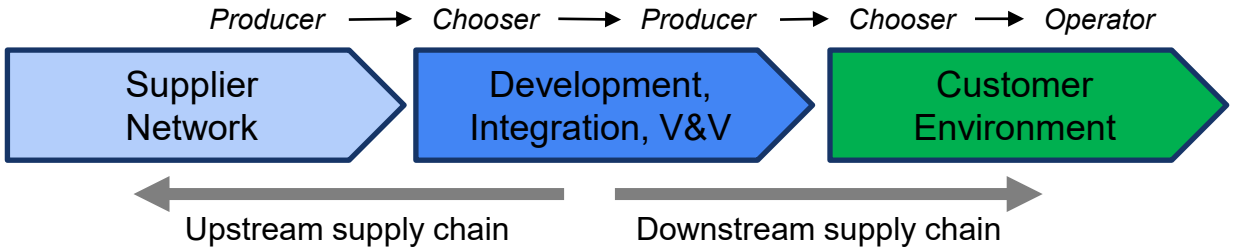
  } NTIA Framing - Baseline Attributes

  - Software level of support (actively maintained, no longer maintained, abandoned)
  - Component End-of-Support date

* = included in 2021 Framing but not 2021 Minimum Elements

SBOM Sharing

- Vision: SBOM sharing along the value chain will enable greater security risk visibility and enable proactive action: *Producer* → *Chooser* → *Operator*
- Reality: There are multiple challenges along the path and end customer use of SBOM for the purpose of security hygiene is (today) an aspirational goal.
- Challenges:
  - Quality and completeness of inventory data
  - Complexity of inventory (multi-device and multi-vendor)
  - Matching inconsistencies: SBOM to physical device
  - Security resources and expertise to interpret and meaningfully respond
  - Matching inconsistency: SBOM component to vulnerability
  - Interpretation of exploitability



Does FDA Care? Example Rejections (summarized)

- No SBOM: Your device meets the definition of a cyber device under section 524B(c) of the FD&C Act. However, you did not provide a software bill of materials (SBOM), including commercial, open-source, and off-the-shelf software components as required by section 524B(b)(3) of the FD&C Act.
- Missing elements in SBOM: You provided a software bill of materials (SBOM); however, it does not appear to include all baseline attributes. Therefore, please provide an updated SBOM.
- Missing elements in SBOM - EOL/EOS and level of support: You did not provide level of support provided through monitoring and maintenance from the software component manufacturer (e.g., the software is actively maintained, no longer maintained, abandoned) or the end-of-support date for each software component contained within the software bill of materials (SBOM). This information is important to comply with the requirement specified in section 524B(b)(2) of the FD&C Act to provide a reasonable assurance that the device and related systems are cybersecure.
- Missing elements in SBOM - "unknown": The information you provided is inadequate because you have indicated you do not know the level of support or the end of support date. This information is important to comply with the requirement specified in section 524B(b)(2) of the Federal Food, Drug, and Cosmetic Act to provide a reasonable assurance that the device and related systems are cybersecure.

Regulations and Standards that Stipulate SBOM

EU MDR:

- SBOM not explicitly called out but emphasizes cybersecurity "state-of-the-art“.
- Requires list of SOUP components and SBOM is one way to fulfill this.

EU Cyber-Resilience Act (CRA):

- Regulated medical devices are excluded but personal health devices etc. need to comply.
- Mandatory for “products with digital elements” by Dec. 2027.
- Machine-readable format; top-level dependencies.
- Supply SBOM to authorities and operators but not published.
- Improve transparency, manage supply chain risks, identify and manage vulnerabilities.
- Non-compliance can result in significant fines.

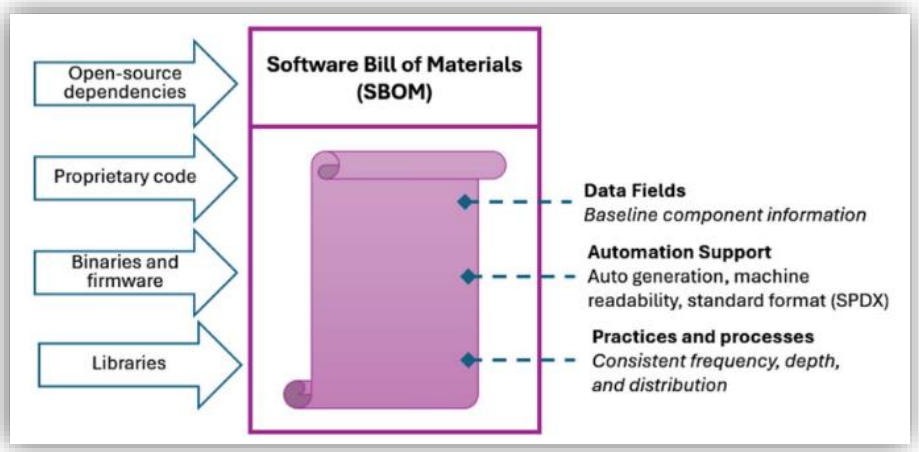
BSI Guideline TR-03183 (Germany):

- JSON or XML; CycloneDx v1.6+ or SPDX v3.0.1+
- SBOM Creator; Time Stamp; SBOM URL
- Component Creator; Name; Version; File Name; Dependencies; Licenses; Hash; URI
- Note – not explicitly calling out EOL/EOS

Regulations and Standards that Stipulate SBOM

ETSI TR 104 034 "SBOM Compendium":

- Reiterates SBOM Minimum Elements
- Defines SBOM Types:
  - Design – initial, intended
  - Source – source files, dependencies and artifacts
  - Build – derived from build process, e.g., represents executable
  - Analyzed – derived through tooling, e.g., from binaries
  - Deployed – present on a system
  - Runtime – derived from running system, instrumented, dynamic
- Challenges:
  - Unique identifiers and discovery
  - Level of dependencies
  - Lifecycle and change dynamics
  - Trust and data quality
  - Interoperability



Regulations and Standards that Stipulate SBOM

Financial Sector Regulations:

Payment Card Industry Data Security Standard (PCI DSS):

- Mandates SBOM as of March 2025 (requirement 6.3.2)
- Maintain an inventory of software components, including open-source libraries and other dependencies, and keep it current for vulnerability management.

EU Digital Operational Resilience Act (DORA):

- Applicable to financial entities
- Does not explicitly stipulate a Software Bill of Material (SBOM)
- Mandates to track "third-party libraries, including open-source libraries" for vulnerability management and risk assessment - SBOM is a way to fulfill this requirement

SBOM in Procurement and Customer Communication

Executive Order EO 14028 (2021):

- Enhance cybersecurity measures to mitigate risks and bolster national security.
- Software vendors to provide SBOMs for all government purchases.
- Also, initiated CISA project to standardize SBOMs.

HSCC Joint Security Plan v2 (JSP2) multi-faceted use of SBOM:

- Supplier contracting and performance management
- Internal use: component assessment, development, testing, transfer to manufacturing
- Customer security communication

HSCC Model Contract-Language for Medtech Cybersecurity (MC2) - Vulnerability Management:

- Supplier to provide a complete Software Bill of Material (SBOM).
- Monitor for security vulnerabilities and mitigate any severe and exploitable vulnerabilities.
- Notify customer if a component is no longer actively maintained.

Joint International Guidance

https://www.cisa.gov/resources-tools/resources/shared-vision-software-bill-materials-sbom-cybersecurity

SBOM = a formal record of the details and supply chain relationships of components in software; a "list of ingredients".

SBOMs = a key tool to address challenges in securing software because of the visibility they provide.

Should be machine-processable and contain enough information to correlate with other data sources, such as vulnerability databases and security advisories.

Automation is a key goal for SBOM generation and use.

Value Proposition – Support Risk Management Practices:

- Vulnerability Management
- Supply Chain Risk Management
- Improved Software Development Processes
- Managing Software Licenses

SBOM Value Provided to:

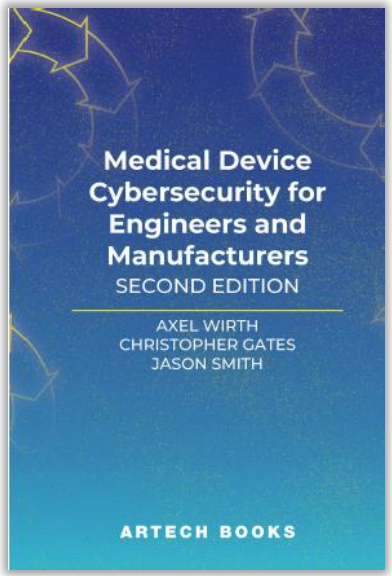
- Producers, Choosers, Operators
- National Cybersecurity Organizations

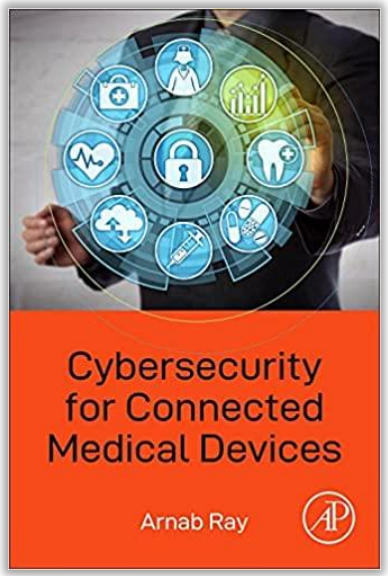
SBOM is a key element of "Secure by Design"

Thank you!

axel@medcrypt.com

General Resources - For Medical Device Manufacturers

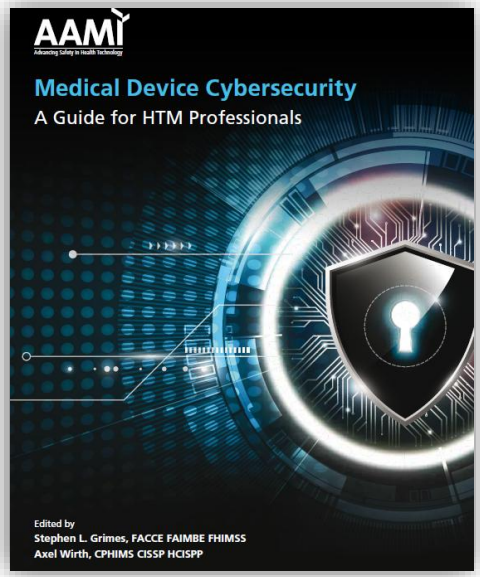




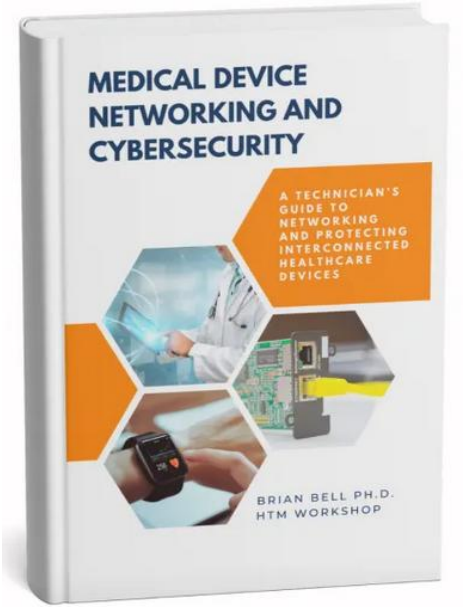
US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

https://www.amazon.com/Cybersecurity-Connected-Medical-Devices-Arnab/dp/0128182628/ref=sr_1_4

General Resources - For Healthcare Delivery Organization



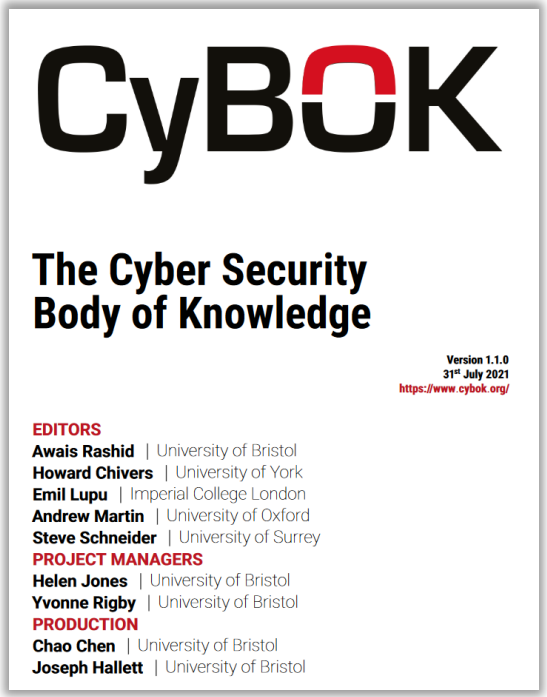
https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA



https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

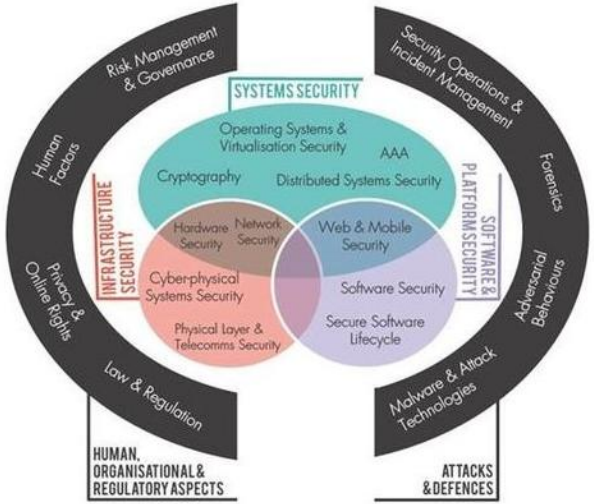
CY 7790 / CY 4973 - Medical Device Cybersecurity

General Resources - CyBOK



The Cyber Security Body of Knowledge v1.1,
https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK Knowledge Base
https://www.cybok.org/knowledgebase1_1/



Staying Informed on the Day-to-Day

- Security briefs and threat alerts via Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) medical device alerts (ICSMA) https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A96
- Healthcare and Public Sector Highlights - Cybersecurity (via HHS) https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
- CISA HPH Sector https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector