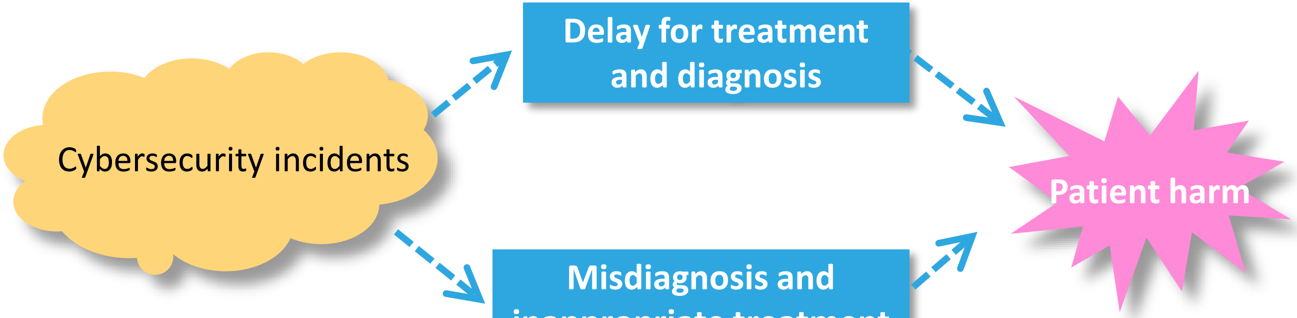
独立行政法人 医薬品医療機器総合機構
Pharmaceuticals and Medical Devices Agency

Cybersecurity requirements for medical device product registration.

Kuniki Imagawa
Deputy Division Director
Division of Standards for Medical Devices / Office of Software as a Medical Device
Pharmaceuticals and Medical Devices Agency

Background

- The need for effective cybersecurity to ensure medical device safety has become more important with the increasing use of wireless, Internet, and network-connected devices.
- Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities.
- Such incidents may lead to patient harm through delays and/or errors in diagnoses and/or treatment interventions, etc.


Cybersecurity incidents

Delay for treatment and diagnosis

Misdiagnosis and inappropriate treatment

Patient harm

Background

- To minimize cybersecurity risk especially for patient safety, the "shared responsibility among the manufacturer, healthcare provider, and regulator, etc.", also "Total Product lifecycle Cycle Management" becomes to be important.
- Since 2015, several notifications for healthcare providers and for manufacturers have already been published.

- In this year, the Essential Principal in Pharmaceuticals and Medical Devices Act has been revised to clarify especially for premarket medical device requirements.
- We are currently working with the manufacturer to discuss how the cybersecurity requirements can be specified in the application material.(Transition Period: until Mar 31, 2024)

→ This is main topic in this session.

Pharmaceuticals and Medical Devices Act

Act	**Pharmaceuticals and Medical Devices Act (PMD Act), 1960**
Cabinet Order	Cabinet Order on PMD Act, 1961
Ministerial Ordinance	Ministerial Ordinance on PMD Act, 1961 GCP/GLP for medical device, 2005 Good Vigilance Practice (GVP) Quality Management System (QMS) etc.
Ministerial Notification	**Essential Principles** Certification criteria for class II/III devices Classification of medical devices ,etc.
Notification	Information on application procedures Essential Principle Checklist Guidelines for clinical evaluation ,etc.

Essential principle

- Essential Principles (EPs) from GHTF/IMDRF document※ titled “Essential Principles of Safety and Performance of Medical Devices” has been introduced in Japanese regulation and all Medical Devices shall be in conformity with the EPs.
- Fundamental design and manufacturing requirements are described to provide assurance the device is safe and performs to its specification
- It will provide benefits in establishing, in a consistent way, an economic and effective approach to the control of medical devices in the interest of public health.

※ The GHTF document was superseded as IMDRF document (IMDRF/GRRP WG/N47 FINAL 2018) with same title on 31th Oct. 2018.

GHTF/SG1/N68:2012

GHTF

FINAL DOCUMENT

Global Harmonization Task Force
(revision of GHTF/SG1/N41:2005)

Title: Essential Principles of Safety and Performance of Medical Devices

Authoring Group: Study Group 1 of the Global Harmonization Task Force

Date: November 2nd, 2012

Dr. Kazunari Asanuma, GHTF Chair

This document was produced by the Global Harmonization Task Force, a voluntary international group of representatives from medical device regulatory authorities and trade associations from Europe, the United States of America (USA), Canada, Japan and Australia.

The document is intended to provide non-binding guidance to regulatory authorities for use in the regulation of medical devices, and has been subject to consultation throughout its development.

There are no restrictions on the reproduction, distribution or use of this document; however, incorporation of this document, in part or in whole, into any other document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the Global Harmonization Task Force.

Copyright © 2012 by the Global Harmonization Task Force

Essential principle

Chapter 1 General Requirements

Article 1（Design）

Article 2（Risk management）:

→ Reduce as far as reasonably practicable the remaining risks by taking adequate protection measures

JIS T 14971
(ISO 14971)

Article 3（Performance and function of medical devices）

Article 4（Term of validity or lifetime of the products）

Article 5（Transport and storage, etc.）

Article 6（Benefits of medical devices）:

→ All known and foreseeable risks should be minimized and be acceptable when weighed against the benefits

Chapter 2 Requirements for design and manufacture

Article 7（Chemical properties）

Article 8（Prevention of microbial contamination）

Article 9（Consideration of use environment ）

Article 10（Consideration of measuring or diagnostic function）

Article 11（Protection against radiation）

Article 12（Consideration of medical devices using software）

→ Ensure repeatability, reliability and performance based on intended use

→ Validation taking into account the development lifecycle

JIS T 2304
(IEC 62304)

Article 13（Consideration of active medical devices and medical devices connected to them）

Article 14（Consideration of mechanical risks）

Article 15（Consideration of medical devices supplying energy or substances）

Article 16（Consideration of medical devices intended to be used by lay persons）

Article 17（Information provision to users by package inserts, etc.）

Article 18（Performance evaluation and clinical studies）

独立行政法人 医薬品医療機器総合機構
Pharmaceuticals and Medical Devices Agency

Revised Essential Principle

- Cybersecurity requirements has been added to article 12 to reflect concepts in following documents；IMDRF/GRRP WG/N47 :2018, IMDRF/CYBER WG/N60 :2020 , Published cybersecurity notification in Japan

IMDRF/GRRP WG/N47 FINAL:2018

IMDRF International Medical Device Regulators Forum

Final Document

Title: Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices

Authoring Group: IMDRF Good Regulatory Review Practices Group

Date: 31 October 2018

Yuan Lin, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2018 by the International Medical Device Regulators Forum

IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

Article 12 Cluse 3

For medical devices using software that are used in connection with other devices and networks, etc., or that may be subject to external unauthorized access and attack, etc.,

Clarification for intended medical device

appropriate requirements shall be identified, taking into account the operating environment and network use environment of the medical device,

Identification of the minimum requirements (operating and usage environment) necessary for the software to operate as intended

← IMDRF N47 Clause 5.8.4, Japanese notification

the risk related to cybersecurity that may affect the function of the medical device or cause safety concerns shall be identified and evaluated, and risk management shall be conducted to reduce such cyber risks.

Design and manufacturing that appropriately reduces cyber risk（Identification and evaluation for cyber risks）

← IMDRF N47 Clause 5.5.6, Japanese notification

In addition, such medical devices shall be designed and manufactured based on a plan to ensure cybersecurity throughout the total product life cycle of the medical device.

Design, manufacture and maintenance that provides an appropriate level of cybersecurity throughout the total product life cycle

← IMDRF N47 Clause 5.8.5, IMDRF N60 Clause 4.2

Conformity to Revised Essential Principle

Article 12 Cluse 3

For medical devices using software that are used in connection with other devices and networks, etc., or that may be subject to external unauthorized access and attack, etc.,

appropriate requirements shall be identified, taking into account the operating environment and network use environment of the medical device,

the risk related to cybersecurity that may affect the function of the medical device or cause safety concerns shall be identified and evaluated, and risk management shall be conducted to reduce such cyber risks.

In addition, such medical devices shall be designed and manufactured based on a plan to ensure cybersecurity throughout the total product life cycle of the medical device.

Clarification for intended medical device

Conformity to a new clause with JIS T 81001-5-1:2023（IEC 81001-5-1:2021) and a part of published Japanese notification to align with this standard.

JIS T 81001-5-1:2023（IEC 81001-5-1:2021)

Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle

This standard defines the following requirements to increase the cybersecurity ;

- The certain activities through the product life cycle
- The development and maintenance on the basis of quality management system and risk management

In Japan, the software life cycle management (JIS T 2304) and risk management process (JIS T 14971) have been implemented in PMD Act.

JIS T 81001-5-1 and JIS T 2304

To improve cybersecurity, the activities to be performed during the product life cycle are described in the sequence of JIS T 2304 (IEC 62304).

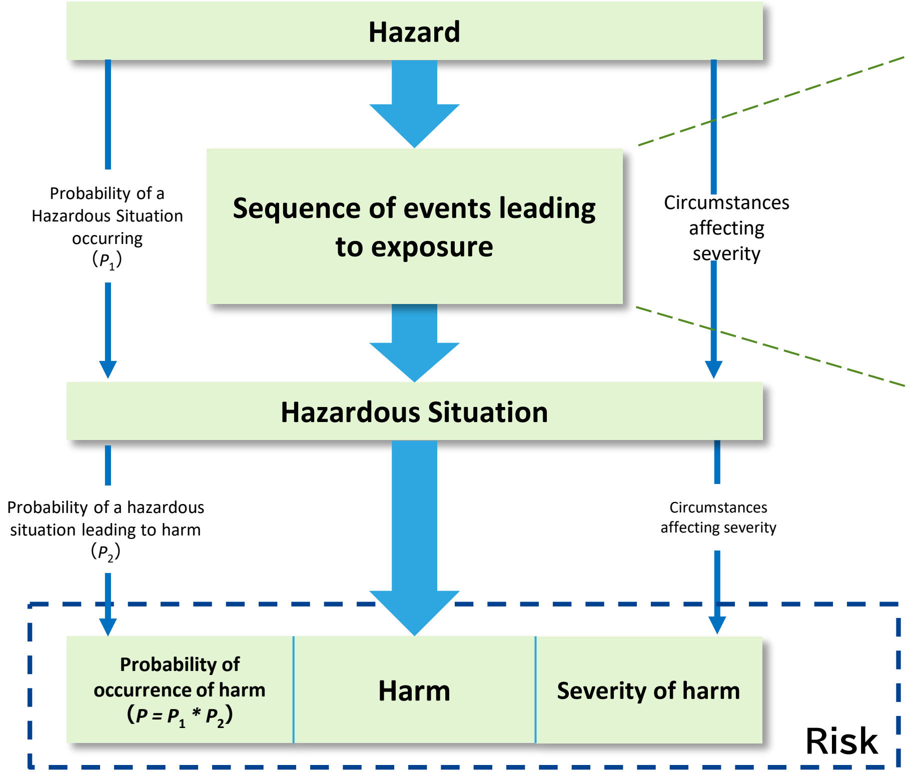
	JIS T 2304 (IEC 62304)
4	General requirements
5	Software development PROCESS
6	SOFTWARE MAINTENANCE PROCESS
7	RISK MANAGEMENT PROCESS
8	Software CONFIGURATION MANAGEMENT PROCESS
9	Software problem resolution PROCESS

↔

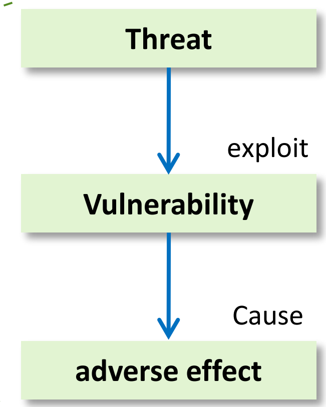
	JIS T 81001-5-1 (IEC 81001-5-1)
4	General requirements
5	Software development PROCESS
6	SOFTWARE MAINTENANCE PROCESS
7	SECURITY RISK MANAGEMENT PROCESS
8	Software CONFIGURATION MANAGEMENT PROCESS
9	Software problem resolution PROCESS

- IEC 81001-5-1 does not specify security lifecycle process individually.
- It specifies activities to be added to the framework of existing processes.

JIS T 81001-5-1 and JIS T 14971

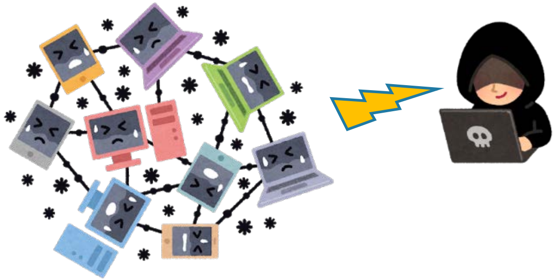

Hazard
Probability of a Hazardous Situation occurring (P_1)
Sequence of events leading to exposure
Circumstances affecting severity
Hazardous Situation
Probability of a hazardous situation leading to harm (P_2)
Circumstances affecting severity
Probability of occurrence of harm ($P = P_1 * P_2$)
Harm
Severity of harm
Risk

Reference： ISO 14971:2019 Figure C.1 Pictorial example of the relationship of hazard, sequence of events, hazardous situation and harm



Cybersecurity concerns in JIS 81001-5-1 can be mapped to risk management concepts in JIS T 14971.

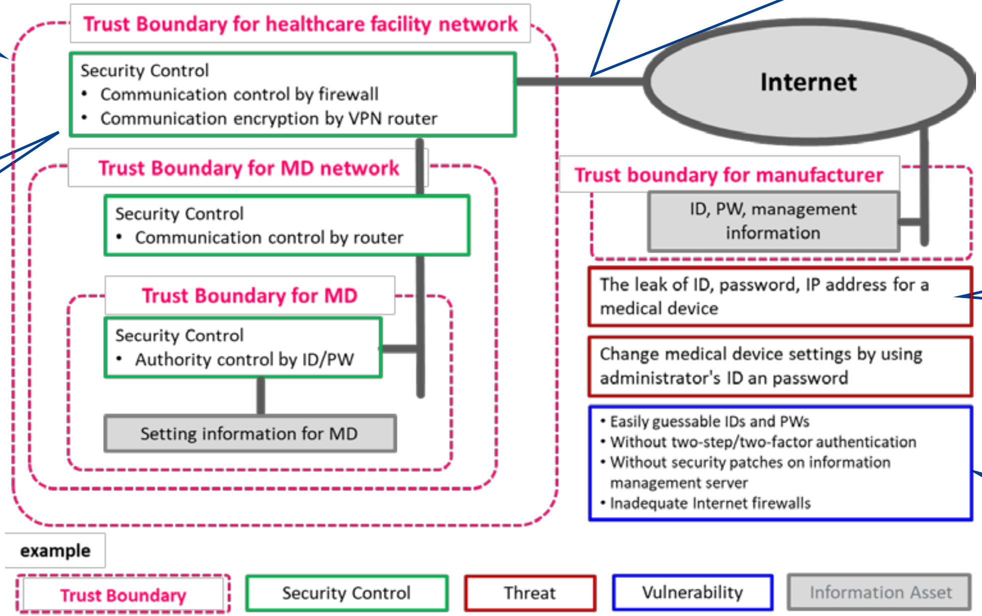
Clarify by Threat Modeling



Example of Threat Modeling

Clarify the intended use and environment of use

- Clarify the route (network configuration) by which the vulnerability can be exploited.
- Important to clarify "No I/F" for MDs without interface



Trust Boundary for healthcare facility network

Security Control
- Communication control by firewall
- Communication encryption by VPN router

Internet

Trust Boundary for MD network

Security Control
- Communication control by router

Trust Boundary for MD

Security Control
- Authority control by ID/PW

Setting information for MD

Trust boundary for manufacturer

ID, PW, management information

The leak of ID, password, IP address for a medical device

Change medical device settings by using administrator's ID an password

- Easily guessable IDs and PWs
- Without two-step/two-factor authentication
- Without security patches on information management server
- Inadequate Internet firewalls

example

Trust Boundary | Security Control | Threat | Vulnerability | Information Asset

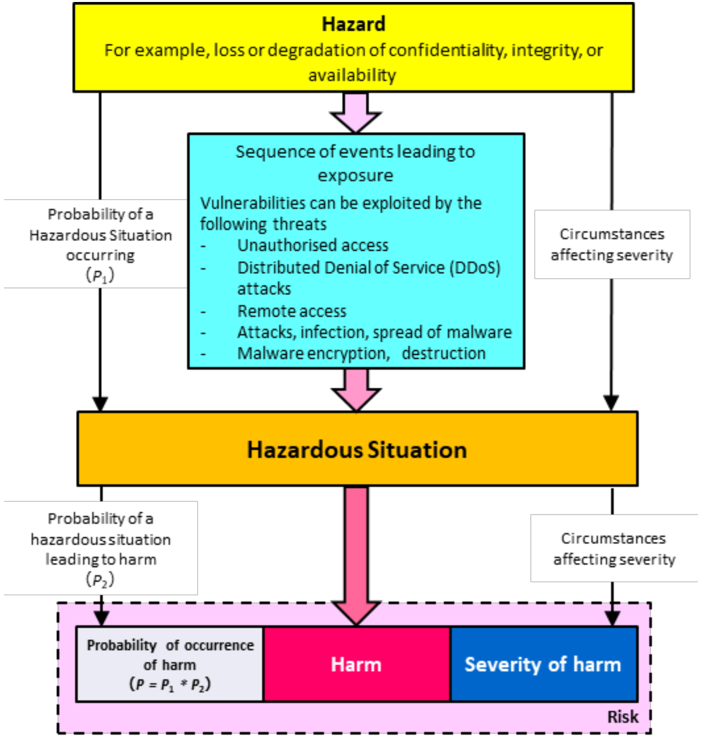
Clarify the Security Control for Healthcare facility

Clarify the predictable threat

Clarify the predictable vulnerability

It's important to illustrate <u>which routes</u>, <u>which threat by which the vulnerabilities can be exploited,</u> <u>lead to a hazardous situation</u>, and which security controls are effective and which are not.

Threat Modeling and Risk Analysis



Hazard
For example, loss or degradation of confidentiality, integrity, or availability

Sequence of events leading to exposure
Vulnerabilities can be exploited by the following threats
- Unauthorised access
- Distributed Denial of Service (DDoS) attacks
- Remote access
- Attacks, infection, spread of malware
- Malware encryption, destruction

Probability of a Hazardous Situation occurring (P_1)

Circumstances affecting severity

Hazardous Situation

Probability of a hazardous situation leading to harm (P_2)

Circumstances affecting severity

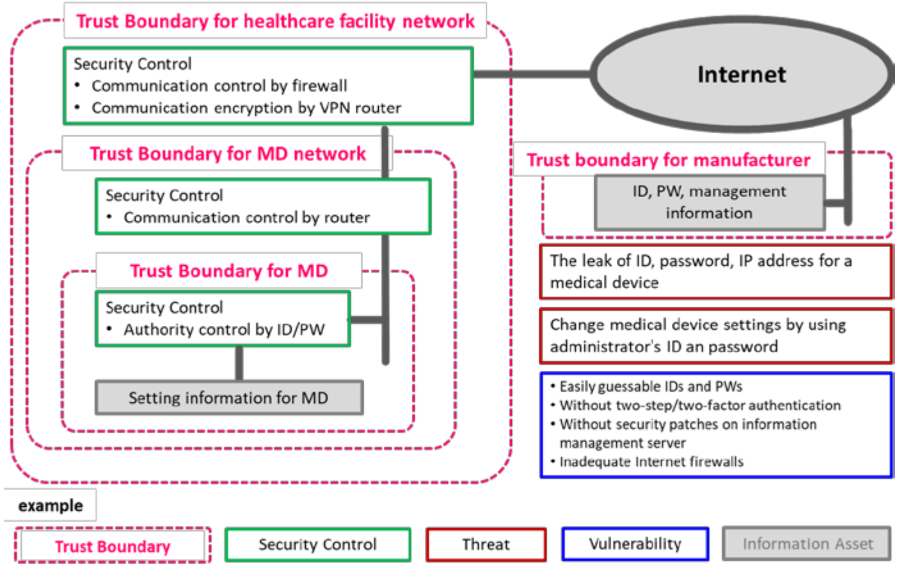
Probability of occurrence of harm ($P = P_1 * P_2$)

Harm

Severity of harm

Risk

Reference： ISO 14971:2019 Figure C.1 Pictorial example of the relationship of hazard, sequence of events, hazardous situation and harm



Trust Boundary for healthcare facility network

Security Control
- Communication control by firewall
- Communication encryption by VPN router

Internet

Trust Boundary for MD network

Security Control
- Communication control by router

Trust Boundary for MD

Security Control
- Authority control by ID/PW

Setting information for MD

Trust boundary for manufacturer

ID, PW, management information

The leak of ID, password, IP address for a medical device

Change medical device settings by using administrator's ID an password

- Easily guessable IDs and PWs
- Without two-step/two-factor authentication
- Without security patches on information management server
- Inadequate Internet firewalls

example

Trust Boundary | Security Control | Threat | Vulnerability | Information Asset

It's important to illustrate which routes, which threat, by which the vulnerabilities can be exploited, lead to a hazardous situation, and which security controls are effective and which are not.
Then explain how a sequence of events (threats) can lead to a hazardous situation or harm.

Requirement for Pre-Market Application

- To introduce cybersecurity requirements into the pre-market application, the notification for Questions and Answers was published on Jul 20, 2023. (e.g., Requirements for documentation, Software Bill of Material (SBOM), and Marketed Medical Devices)
  - MAH needs to document for cybersecurity requirements
  - MAH identifies the documentation control number in Summary Technical Documentation (STED)※
- The more practical notification such as marketed medical devices will be published discussing with MAH.

<Contents for application form>

1 Category
2 Name
3 Intended Use and Indications
4 Shape, Structure, and Principle
5 Raw Materials
6 Standards for Performance and Safety
7 Usage Method
8 Storage Method and Expiration Date
9 Manufacturing Method
10 Manufacturing Site of Marketed Product
11 Remarks

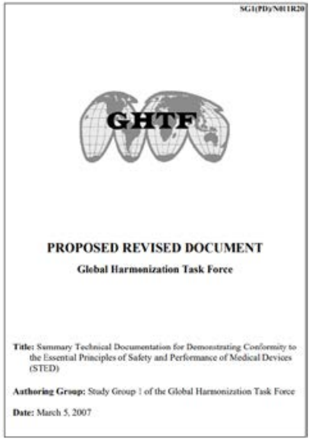
< Contents for STED※ >

1 Overview of Product
2 Conformity to Essential Principles
3 Device Description
4 Summary of Design Verification and Validation Documents
5 Package inserts (draft)
6 Risk Management
7 Information on Manufacturing

Clarify the applicability the Clause12.3

Clarify the documentation control number

※GHTF/SG1/SG1/N063:2011



SG1(PD)/N011R20

PROPOSED REVISED DOCUMENT

Global Harmonization Task Force

Title: Summary Technical Documentation for Demonstrating Conformity to the Essential Principles of Safety and Performance of Medical Devices (STED)

Authoring Group: Study Group 1 of the Global Harmonization Task Force

Date: March 5, 2007

Requirement for Pre-Market Application

<Example of cybersecurity requirements for documentation>

General Requirement	Implement activities to ensure cybersecurity on the basis of quality management system.
	Establish an activity to notify the vulnerabilities for regulatory authority and user.
	Clarify the security policy and the contact point for security, and define the procedure for disclosing vulnerability to customers on the basis of quality management system.
	Risk management should be conducted by considering the security vulnerability and threat, etc.
Software development process	Consider the security updates handling and development environment security in development planning.
	Specify the security requirements including security capabilities.
	Implement an architectural design for intended environment of use, trust boundary, and defense-in depth, etc.
	Clarify the intended environment of use as system configuration and network configuration, etc.
	Design and implementation should take into account the secure.
	Conduct software system testing to ensure that security requirements are met and that methods to address threats identified in the risk management process are implemented and effective in the design.

Requirement for Pre-Market Application

<Example of cybersecurity requirements for documentation>

Software maintenance process	Establish a policy for notifying security updates to user.
	Make a plan for product life cycle such as end of support, and conduct the plan for monitoring to the vulnerabilities, security updates, etc.,. Also, clarify a notifying policy to user for security updates as part of the established plan.
Security risk management process	Estimate and assess relevant threats identifying the relevant vulnerabilities by considering intended use and the environment of use, and control the threats by risk control measure and monitor the effectiveness.
Software configuration management process	Establish configuration management with change controls and change history for development, maintenance and support process.
	Establish the software bill of material (SBOM) as the results of the configuration management process.
Software problem resolution process	Establish the procedure for communicating and handling information on the security vulnerabilities, and handle security issues, including information disclosure in accordance with the procedures.

The following components need to be prepared;
1. Supplier Name, 2. Component Name,
3. Version of the Component, 4. Other Unique Identifiers,
5. Dependency Relationship, 6. Author of SBOM Data
7. Timestamp

独立行政法人 医薬品医療機器総合機構
Pharmaceuticals and Medical Devices Agency

Thank you for your attention.