ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Cybersecurity aspects in the development of a medical device

State of the Art and Challenges

Swiss Medtech SaMD Event, 25.03.2021

Matthias Steck, Senior Software Engineer

matthias.steck@iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Content

Basic Concepts

Regulatory Requirements

Standards and Standardization

Hints from our experience

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Disclaimer

The views and opinions expressed in the following presentation are those of the individual author.

Copyright

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Introduction

Basic Concepts

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Cybersecurity – Cybercrime

As usual: **someone has** something of value (assets) that **someone else wants**:

- **Processing** → crypto mining
- **Storage** → file dump (e.g. child porn, warez)
- **Information** → steal (espionage), hold hostage (ransomware), damage (vandalism, sabotage)
- **Bandwidth** → attack other targets
- **Services** → use for free, prevent use (denial of service)

Multiplication possible – automatically attack many targets – improved return on investment: with multiple attacks (e.g. ransomware) some are bound to succeed.

Note: Cybercrime is a billion dollar industry attracting a lot of professionals and state-sponsored actors

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Cybersecurity – Cyberwar

Political motivation, same basic principle; someone has, someone else wants:

- **Active warfare** (e.g. Israel – Iran, China – Rest of the world)
- **Preparation** (e.g. USA – "I hunt sysadmins", attain strike capability)
- **Clandestine operations** (pretty much everyone)
- **Economic warfare** (e.g. USA – China)

Mostly **state actors** (APT – Advanced Persistent Threat, usually "deniable assets").

Preparation for TAO (Tailored Access Operations), Sabotage, False flag operations, offensive and defensive capabilities.

Note: High level of skill, budget, infrastructure, persistence. Virtually impossible to defend against an active, targeted attack from an APT. Still, we can make their life harder and try to limit the impact.

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Cybersecurity – Medical Devices

Attacks on medical devices and healthcare providers used to be accidental / opportunistic; i.e. a medical device / system was just another networked computer.

Targeted attacks, specifically ransomware, **are becoming the norm**; the health sector is an easy target: security has been neglected for a long time (manufacturers, regulators, and operators), IT systems in use are complex and long-lived, higher willingness and ability to pay ransom.


INTERNATIONAL

Französisches Gesundheitswesen im Visier von Hackern

Radio SRF 4 News | 11.03.2021

Angriffe aufs Gesundheitswesen

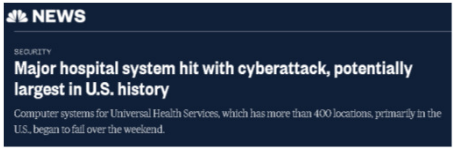
Frankreich ringt mit Pannen und Cyberangriffen auf Systeme von Gesundheitseinrichtungen. Nun will die Regierung handeln.

NEWS
RADIO SRF

Inhaltsart
Bericht

Sendung
Heute/Morgen

Region
International


NEWS

SECURITY

Major hospital system hit with cyberattack, potentially largest in U.S. history

Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend.


BBC
NEWS

Tech

Hackers threaten to leak plastic surgery pictures

By Joe Tidy
Cyber reporter

14 December 2020

Note: Cybersecurity is not a new thing, other industries have been targeted for decades. Healthcare is lagging behind while the (cyber-)world has become increasingly more dangerous.

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Cybersecurity – Basic Principles applied to Medical Devices

Integrity

The integrity of the medical device is protected; e.g. the software, configuration data, patient data are protected against accidental or malicious modification and corruption ➔ the device works correctly

Availability

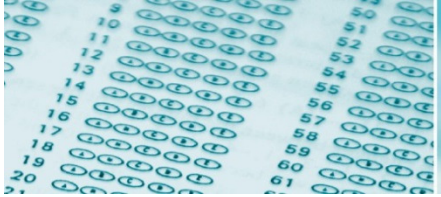
The medical device is available when needed

Confidentiality

The medical device or system protects information from unauthorized access; e.g. patient information and health records

Note: For medical devices, the priorities differ from normal InfoSec: a device that is available is of no use if it is unsafe because integrity has been lost, while confidentiality usually has the least impact on patient safety.

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY



Take home message

- **Medical devices are targets**
  (even if it is just a means to an end)
- **Medical device manufacturers are targets**
  (supply chain attacks, industrial espionage)
- **Your customers are targets**

- **Attackers are many**

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Regulatory Requirements

An Overview

Two different perspectives to consider

MD

Manufacturers

Customers

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

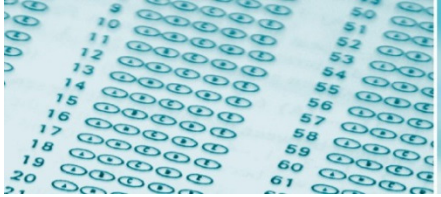
Legislation – Strategic Level

Legislation	Title	Applies to	Core Topics
NCS	National Cybersecurity Strategy	Switzerland	Critical Infrastructure
NIS Directive	Network Information Security Directive	European Member States	Critical Infrastructure
KRITIS / BSI-Gesetz	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz	Germany	Critical Infrastructure
2008/114/EG	Ermittlung und Ausweisung europäischer kritischer Infrastrukturen	European Member States	Critical Infrastructure

Note: Healthcare is critical infrastructure, where healthcare usually means healthcare delivery organizations (HDO) i.e. hospitals, doctors offices

Note: These directives and regulations have no or only very indirect impact on MD

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY



MD

Legislation – Industry Level

Legislation	Title	Applies to	Core Topics
MDR	Medical Device Regulation	Europe, Medical Devices	Risk Management, Information Basic Safety / Safety Lifecycle
MedDO	Medical Devices Ordinance	Switzerland, Medical Devices	Risk Management, Information Basic Safety / Safety Lifecycle
BSI Gesetz / B3S	Branchenspezifischer Sicherheitsstandard (B3S) für Krankenhäuser	Germany, Hospitals (HDO, Operators)	Risk Management, Cybersecurity
21CFR820.30	Quality System Regulation	USA, Medical Devices	Risk Management, Safety Lifecycle
GDPR	General Data Protection Regulation	Europe++, Personal information	Privacy

Note: These directives and regulations do have an impact on MD

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

MD

Medical Device Regulation (MDR)

In contrast to the MDD, the MDR directly addresses cybersecurity issues

General Safety and Performance Requirements:

17.2. …software shall be developed and manufactured in accordance with the **state of the art** taking into account the principles of development life cycle, risk management, including **information security** ...

17.4. Manufacturers shall **set out minimum requirements** concerning hardware, **IT networks characteristics** and **IT security measures**, including protection against unauthorized access, necessary to run the software as intended.

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Legislation in Switzerland – Outlook on the «MDR» Update

The new version of the MedDO (MepV) will place responsibility for cybersecurity on the health delivery organizations:

NEW

Art. 74 Cybersicherheit

«*Gesundheitseinrichtungen treffen alle technischen und organisatorischen Massnahmen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Produkten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen.*»

(will come into force on the 26th of May 2021)

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Where does that leave us?

MD

MDR / MedDO
NB
Standards

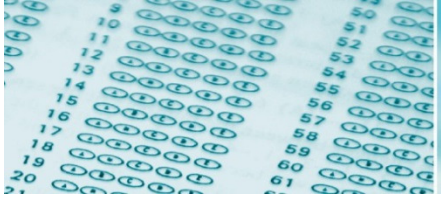
Manufacturer
- what is my responsibility?
- How to reduce effort?
- How to reduce risks?

Customer
- what is my responsibility?
- How to reduce effort?
- How to reduce risks?

KRITIS
MedDO
Own IT Policy

Usually, the customer is in a strong position, meaning <u>we</u> (industry) have to move

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY



Take home message

Direct and indirect requirements for your MD

Legislation revolves around (overlapping) core topics:

- Risk Management and Control
- Security Life Cycle
- Information from manufacturer to integrators, operators, and users
- Post Market Activities
- Vulnerability Disclosure

As usual: Legislation provides us with the «why» and «what», while standards and guidelines are supposed to provide us with the «how».

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Standards and Standardization

An Overview

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

The Challenge: The Current Situation

MDD

- **Harmonized Standards** → EN ISO 14971, EN 60601-1, EN 62304
- **Guidance (MEDDEV)** → -

MDR

- **Harmonized Standards** → -
- **Guidance (MDCG)** → MDCG 2019-16

FDA

- **Consensus Standards** → AAMI TIR 57, AAMI TIR 97, UL 2900-x, IEC TR 80001-x, :, IEC 62443-1/-2/3
- **Guidance** → Premarket, Postmarket, OTS Software

IMDRF

- **Guidance** → WG/N60FINAL:2020

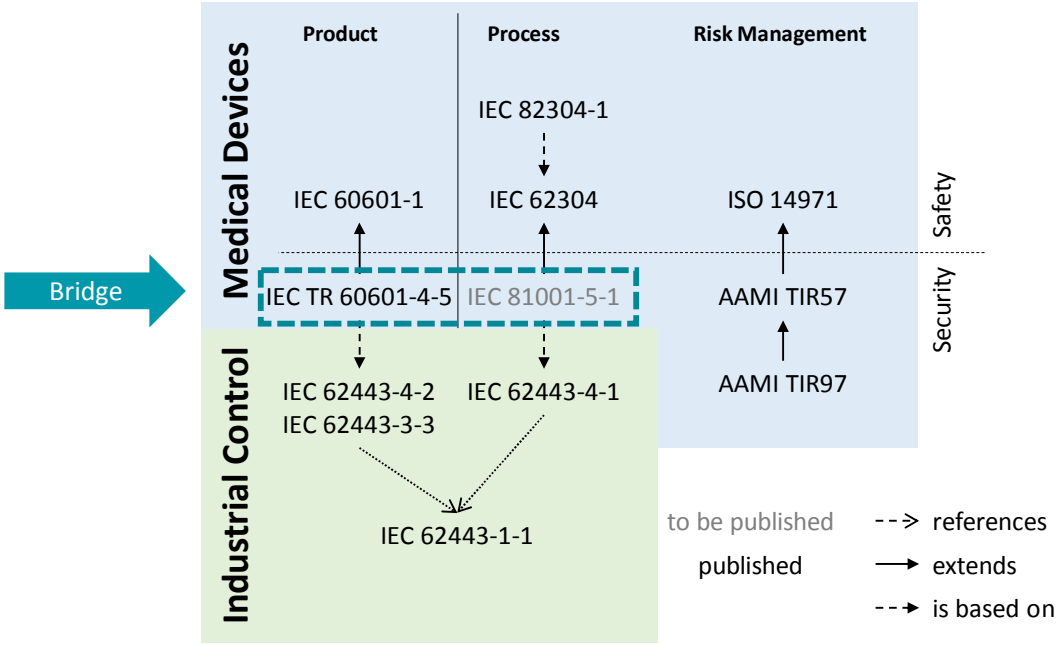
Consensus (state of the art)

IEC 62443-4-1
IEC 62443-4-2

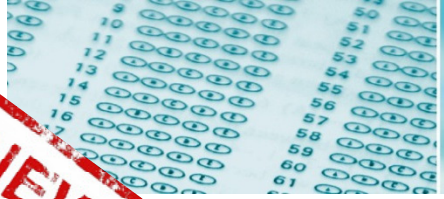
⚠ non-medical device standards

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

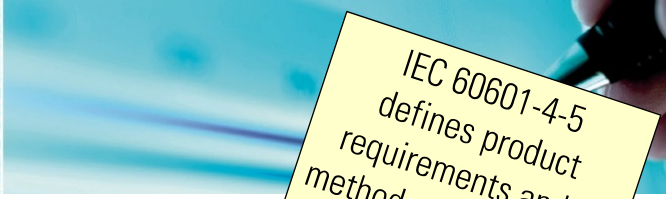
The Solution: Bridging the Gap



ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY



NEW



IEC 60601-4-5 defines product requirements and a method of cooperation

IEC TR 60601-4-5 – Security Specifications

Table 1 – Mapping of single requirements to capability security levels (SL-C)

Component requirements (CR) and requirement enhancements (RE)	SL-C 1	SL-C 2	SL-C 3	SL-C 4
FR 1 – Identification and AUTHENTICATION control (IAC)				
CR 1.1 – Human user identification and AUTHENTICATION	✓	✓	✓	✓
RE (1) Unique identification and AUTHENTICATION		✓	✓	✓
RE (2) Multifactor AUTHENTICATION for all interfaces			✓	✓
CR 1.2 – Software PROCESS and device identification and AUTHENTICATION		✓	✓	✓
RE (1) Unique identification and AUTHENTICATION [a]			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware SECURITY for authenticators			✓	✓

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

Source: IEC 60601-4-5:2021

INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

NEW

IEC 60601-4-5 defines product requirements and a method of cooperation

IEC TR 60601-4-5 – Security Specifications

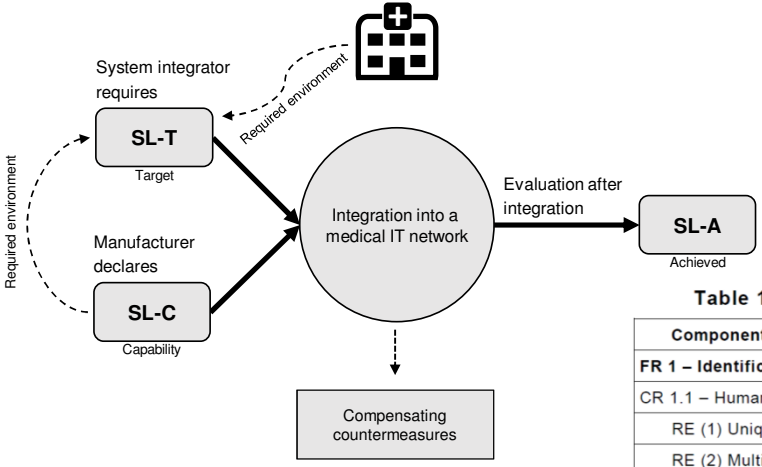


Table 1 – Mapping of single requirements to capability security levels (SL-C)

Component requirements (CR) and requirement enhancements (RE)	SL-C 1	SL-C 2	SL-C 3	SL-C 4
FR 1 – Identification and AUTHENTICATION control (IAC)				
CR 1.1 – Human user identification and AUTHENTICATION	✓	✓	✓	✓
RE (1) Unique identification and AUTHENTICATION		✓	✓	✓
RE (2) Multifactor AUTHENTICATION for all interfaces			✓	✓
CR 1.2 – Software PROCESS and device identification and AUTHENTICATION		✓	✓	✓
RE (1) Unique identification and AUTHENTICATION [a]			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware SECURITY for authenticators			✓	✓

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

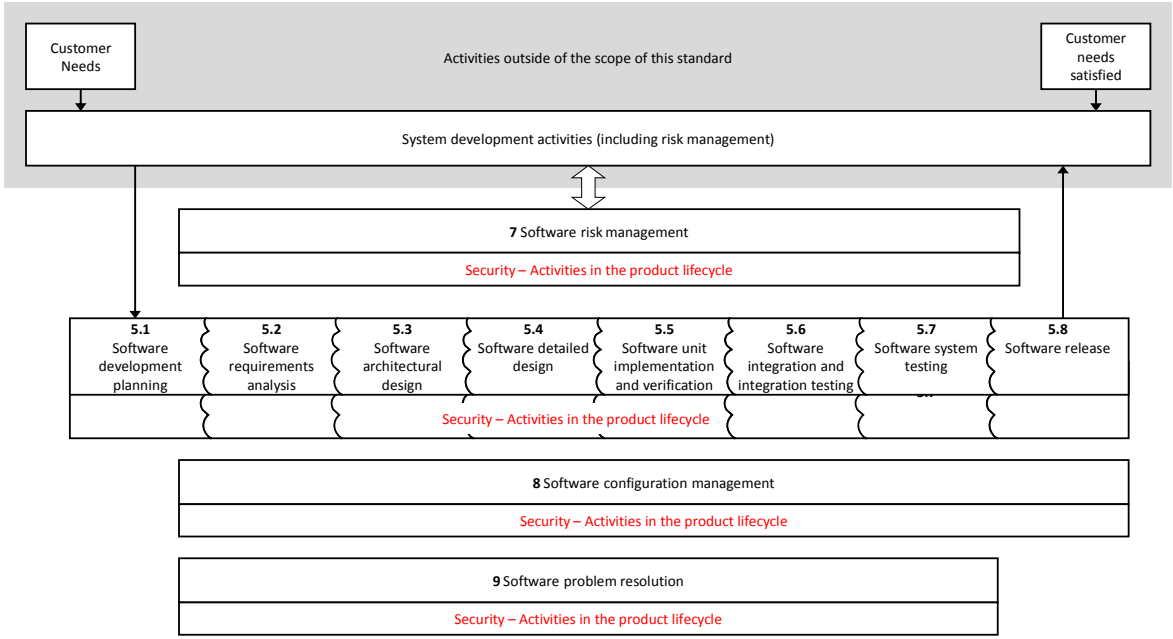
Source: IEC 60601-4-5:2021

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

NEW

IEC 80001-5-1 extends IEC 62304 lifecycle processes

IEC 81001-5-1 (draft) – Cybersecurity Lifecycle

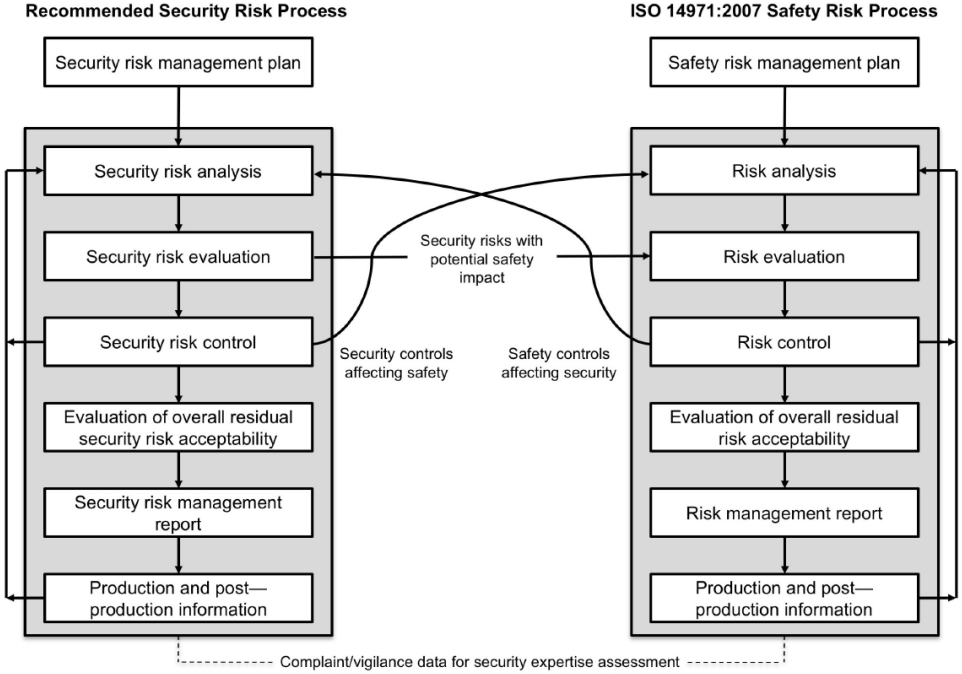


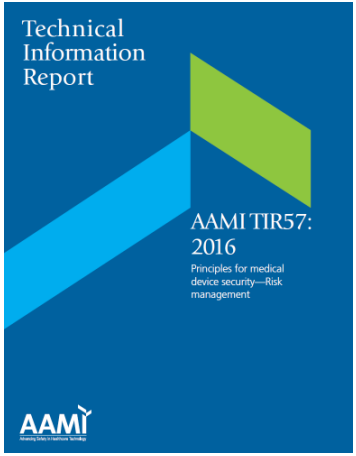
Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

Source: IEC/DIS 81001-5-1

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

AAMI TIR 57 – Security Risk Management





Source: AAMI TIR57:2016

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

In Practice

Hints from our experience

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Notified Bodies – What did they want to know?

Focused on MDR requirements

- **Risk management** documentation
- **Threat analysis** (assets, vulnerabilities, threats)
- Measures to **prevent unauthorized access**
- Measures to **ensure confidentiality** of personally identifiably information
- Measures to **ensure integrity** of data and systems
- Measures to **ensure availability** of data and systems
- Risk management of service and maintenance, including software updates
- Measures to ensure **detection**, **response**, and **recovery**
- Cybersecurity development process

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

What to do?

If you're not already doing it:

- **Perform threat analysis** (assets, vulnerabilities, impact)
- **Use risk management to:**
  - Identify and analyse security risks with impact to safety
  - Implement risk control measures and security controls
  - Make sure security controls don't negatively impact safety
- **Extend Post Market activities to cover SOUP (repeat it on a regular base)**
- **Provide information to integrators and users**
- **Be prepared for security vulnerabilities**
- **Work with authorities**

Ask us if you need support.

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch

ISS
INTEGRATED SCIENTIFIC SERVICES
A MEDTECH COMPANY

Questions

?

Robert-Walser-Platz 7 I CH-2503 Biel I +41 32 513 67 67 I info@iss-ag.ch I www.iss-ag.ch