26th GHWP, Riyadh, Saudi-Arabia

CYBERSECURITY STANDARD DEVELOPMEN7

Michael Bothe, Feb., 13th, 2023, 5:05 p.m.

Brief Commercial

Speaker : Michael Bothe, Head of Notified Body, Active Medical Devices

- 1985 : M.S. Telecommunications
- Focus : R&D, QM, RA in CE, Automotive, Medical
- 35/24/14/4 yrs. Standardisation / Industry / NB / DQS-Med Experience
- Former Chairman of the Notified Body Recommendation Group

Company : DQS Medizinprodukte GmbH, Frankfurt, Germany

- Founded in 2008 as 100% subsidiary of DQS Holding a Global Cert. Body
- ~ 100 FTE‘s + ~ 300 Assessors serving ~ 1600 Clients
- Designated on Aug., 8th, 2020 for Reg. 2017/745

dqs

CE 0297

Agenda

01 **European Medical Device Regulation 2017/745**

Just a single word!

02 **Information Security**

What are the System Boundaries?

03 **State of the Art Standards**

Management System vs. Product specific

04 **Different Approach : Notified Body Consensus**

Keeping Pace with Sprints

MDR 2017/745

JUST A SINGLE WORD IN A 175 PG‘S REGULATION

01

MDR, Annex I, Chapter I, Clause 17.2

General Safety & Performance Requirements

Information security

For **devices that incorporate software or for software that are devices in themselves**, the 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 verification, validation and ...

MDR, Annex I, Chapter I, Clause 17
Standalone- / Embedded SW

- **Entire Software-Life-Cycle covering Design until Deinstallation**
- Risk Management incl. **Information Security**
- **Manufacturers** shall set out minimum requirements concerning
  - IT **networks characteristics**
  - **IT security measures**, including **protection against unauthorised access,** necessary to run the software as intended.

Simply leveraging Quality.

MDR 2017/745

INFORMATION SECURITY SYSTEM BOUNDARIES

02

System Boundaries

Product level

- Individual or networked products of **same type from identical Supplier**
- Networked products of **same type but from different Suppliers**
- Networked products of a **multiplicity of Devices from identical Supplier**
- Networked products from **a multiplicity of Devices from different Suppliers**

Picture Source : Meditronic-Journal 4/2017 OP 4.0, OR.NET e.V.

Simply leveraging Quality.

System Boundaries

Infrastructure level

- **Overall IT-Network** without segregation
- **Segregated, general** Medical IT-Network
- **Segregated, dedicated, Risk based** Medical IT-Network, e.g. OR, ER, etc.
- **Dynamicly segregated, redundant Risk based** Medical IT-Network

Simply leveraging Quality.

MDR 2017/745

STATE OF THE ART STANDARDS

03

State of the Art Standards

Infrastructure Level

- ISO/ IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- IEC 80001-1:2021 - IT Application of risk management for IT-networks incorporating medical devices - Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
- IT Baseline Protection of the German Federal Office for Information Security (BSI). BSI - IT-Grundschutz (bund.de)

Device Level

- IEC TR 60601-4-5:2021 Medical Electrical Equipment - Part 4-5: Guidance and Interpretation - Safety-Related Technical Security Specifications
- ISO/IEEE 11073-40102:2022 Health informatics — Device interoperability — Part 40102: Foundational — Cybersecurity — Capabilities for mitigation

Standards mostly did not yet reflect the entire speed of SW- Development which usually operates in Sprints rather than in consecutive design phases. As such it is a challenge, to maintain and adapt them accordingly.

MDR 2017/745

COMPLEMENTARY APPROACH : NOTIFIED BODY CONSENSUS

04

Concerted Effort

Notified Body Consensus

- Agreed **overriding Strictness Level** for Conformity Assessment
- **Editors : German Notified Bodies Alliance** for Medical Devices

IG·NB
Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland

Questionnaire "IT Security for Medical Devices“

(Version 5, 09.06.2022)

- Developed with stakeholder involvement and nondiscriminary consensus building
- **5 Revisions released** within a 2,5 yrs. Timeframe
- Meanwhile **de-facto standard** for all conformity assessments of or including SW

Microsoft Word - IG-NB - Questionnaire IT Security for Medical Devices - Version 5.docx

Life Cycle Approach

Installation is not the end

- **Product Design Phase**
  - Intended Use and Stakeholder-Requirements
  - System- / Software-Requirements/ -Architecture
  - Implementation and Design of Software
  - Assessment of Software-Units
  - System- and Software-Tests
  - Product Release
- **Postproduction Phase**
  - Production, Distribution, Installation
  - Post Market Surveillance
  - Incident Response Plan
  - Decommisioning

Simply leveraging Quality.

Requirements and Risk Management

Adapted and regularly Updated Aspects

System-/Software-Requirements

- Authentification
- Communication and Storage
- Patches
- System-/Software-Architecture
- Accompanying Documents

Risk Management Aspects

- Product Release

Regular Penetration Tests challenging Security Level

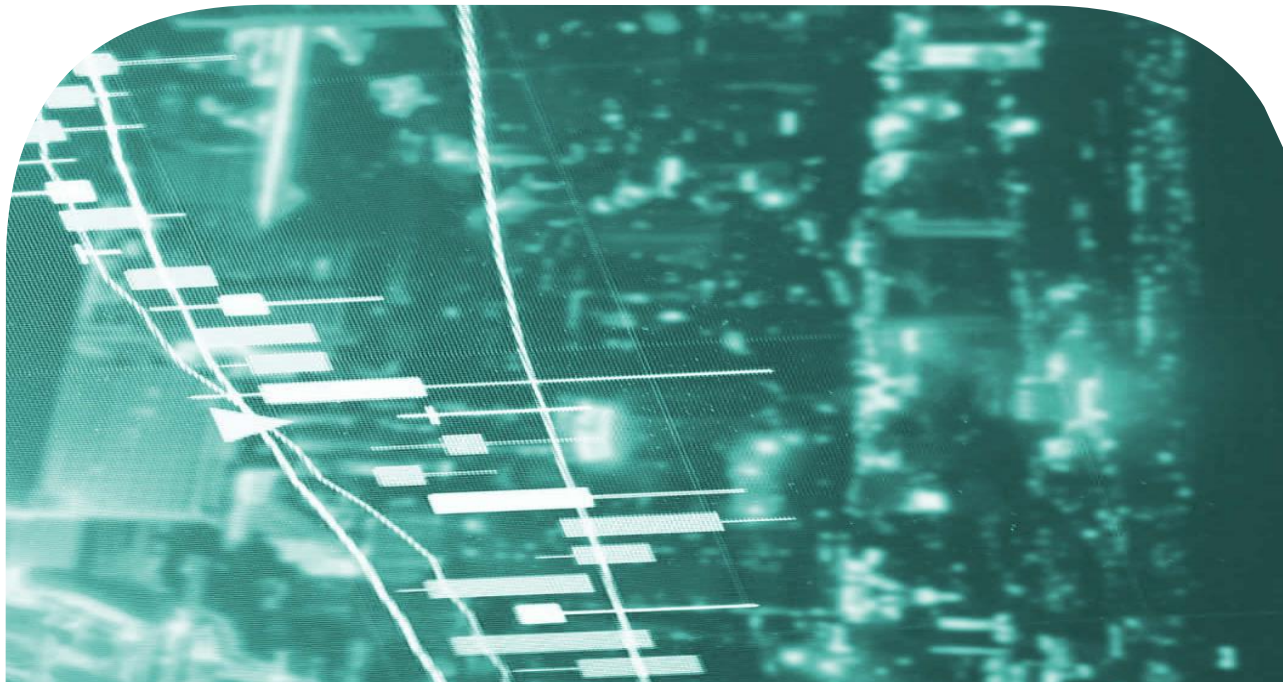
Established (global) Standardisation Bodies

Focus on overall harmonised, generic Quality Management Standards with relative low modification rate.

Summary : Best of both Worlds:

Specific (per jurisdiction) from new Interest Groups

Complementary Product specific de facto Standards with high modification rate and adaptiveness.



Thanks for your attention!

DQS Medizinprodukte GmbH

August-Schanz-Str. 21
60433 Frankfurt am Main
Germany

Phone: +49 69 95427-0
info@dqs.com
www.dqsglobal.com