Questionnaire "Cybersecurity for Medical Devices - Audit“

(Version 1, 21.03.2023)

Preliminary remarks

- This document was compiled by the German Notified Bodies Alliance (Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland - IG-NB) and is intended to serve as orientation for Notified Bodies, manufacturers and interested parties.
- This document is covering cybersecurity in regular scheduled MDR / IVDR audits.
- Created by Jan Küfner (TÜV SÜD), Dr. Abtin Rad (TÜV SÜD), Dr. Andreas Schwab (TÜV Rheinland), Volker Sudmann (mdc medical device certification), Markus Bianchi (DNV Medcert), Martin Tettke (Berlin Cert), Michael Bothe (DQS Med), Mark Küller (TÜV-Verband / IG-NB)
- This document, together with the questionnaire „Cybersecurity for Medical Devices – Technical Documentation“, replaces the questionnaire "IT security for Medical Devices“ (Version 5, 09.06.2022).
- Questions regarding the security risks of artificial intelligence can be found in latest version of IG-NB's "Questionnaire Artificial Intelligence (AI) in Medical Devices" (https://www.ig-nb.de/veroeffentlichungen).
- Not all requirements of MDR, IVDR and MDCG 2019-16 are covered in this document. Compliance to IEC 81001-5-1 is not expected prior end of its transition period. Compliance to IEC 81001-5-1 prior its transition period is however recommended.
- In the following tables IEC 81001-5-1 is mentioned only for complementary purposes. Questions for manufacturers are solely based on the current requirements (MDR, IVDR, MDCG 2019-16)
- Since cybersecurity evolves on a regulatory and technological level, this document is intended to reflect the current state of the art at the time of creation only.
- There are few cybersecurity experts today and it is likely that the situation will continue to be a similar in the foreseeable future. Therefore it is one goal of this paper to help making

conformity assessment(s) of cybersecurity aspects as efficient as possible without compromising quality.
- The terminology used in this document is derived from the terms and definitions within the referenced sources. E.g. cybersecurity as defined in ISO 81001-1:2021-12, cl. 3.30.
- Included in this document are references to paragraphs from the standards IEC 62034 and IEC 81001-5-1. These standards have different scopes (medical device software (IEC 62304) and healthcare software (IEC 81001-5-1)) and use different terms for similar subjects and processes. Specific terms and their use in the context of the respective standard are defined in clause 3 "Terms and Definitions" of the respective standard.
- The document makes no claim to completeness or mandatory application.

References

- REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (2017/745/EU) (MDR)
- REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (2017/746/EU) (IVDR)
- MDCG 2019-16 - Guidance on Cybersecurity for medical devices, Rev. 1, 2020-07
- ISO 13485:2016-03 Medical devices - Quality management systems - Requirements for regulatory purposes
- IEC 62304:2005-05 Medical device software - Software life cycle processes
- IEC 81001-5-1:2021-12 Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

Terms and Definitions

- In this document, the term medical device is frequently used. Whenever the term medical device is mentioned, both types are meant, medical devices and in vitro diagnostic medical devices.

Changes to last version

/

1 General

	Source	Requirements	Questions / Comments
1.	ISO 13485 cl. 5.5.1	– definition, documentation and communication of responsibilities and authorities by top management – documentation of interrelations – ensure independence and authority	Has the auditee defined responsibilities and authorities for cybersecurity? Has the auditee defined a person or persons responsible for cybersecurity within the company?
	IEC 81001-5-1 cl. 4.1.2	– designate and document organizational roles – designate and document personnel responsible for activities and processes	
2.	ISO 13485 cl. 6.2	– only competent personnel should be performing work affecting quality – basis: appropriate education, training, skills, experience	Has the personnel carrying out cybersecurity tasks appropriate education and/or work experience and/or training?
	IEC 81001-5-1 cl. 4.1.4	– established activities for identifying and providing security training and assessment programs – personnel should be assigned to the organizational roles and duties demonstrated security expertise – role descriptions, training profiles, training records	
3.	ISO 13485 cl. 7.4.1	– establish criteria for evaluation and selection of suppliers – basis: specific criteria (supplier - ability to provide product that meets requirements and performance of the supplier, effect of purchased product on quality, proportionate to the risk)	Are the suppliers (penetration testing laboratories, 3rd party component suppliers) appropriately qualified? Note 1: Penetration testing laboratories should be accredited where available. Note 2: Supplier evaluation of 3rd party components is not necessary when the quality of the code can fully be verified.

			Note 3: Auditing penetration testing laboratories seems to be not necessary. Other means for rating performance and ability of penetration-testing suppliers (e.g. penetration test report reviews, questionnaires) seem more plausible.

2 Research and Development

	Source	Requirements	Questions / Comments
1.	MDR Annex I (17.2) IVDR Annex I (16.2)	'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 information security**, verification and validation.	Note 1: Cybersecurity risk assessment should be conducted prior to the finalization of specifications / cybersecurity risk management shall be conducted at the design input phase. (applicable for R&D projects that started after the release of MDCG 2019-16 in November 2019). Note 2: For legacy devices, the approach as defined in 81001-5-1 appendix F may be used. Note 3: It is not acceptable to add cybersecurity countermeasures (e.g. encryption) at the end of a development cycle project since this concept is following the outdated "penetrate and patch" approach.
	MDCG 2019-16 chapter 3	'Safety, **security** and effectiveness are critical aspects in the design of security mechanisms for in vitro diagnostic medical devices and medical devices. Therefore, there is a **clear requirement** that these aspects need to be considered by the manufacturers **from an early stage of development** and manufacturing process and throughout the entire life cycle.'	

	Source	Requirements	Questions / Comments
	MDCG 2019-16 chapter 3.2	'The security risk management process has the same elements as safety risk management process, all documented in a **security risk management plan**. The process elements are **security risk analysis**, **security risk evaluation**, **security risk control**, **evaluation of residual security risk** and **reporting**. When a security risk or control measure could have a **possible impact on safety** and effectiveness, then it **should be included in the safety risk assessment**. Similarly, any safety risk control or consideration that might have an impact on security should be included in the security risk analysis.'	Is a dedicated and plausible security risk assessment available for all MDR / IVDR certified devices?
2.	MDCG 2019-16 chapter 3.4	'**Threat Modelling techniques are a systematic approach** for analyzing the security of an item in a structural way such that vulnerabilities can be identified, enumerated, and prioritized, all from a hypothetical attacker's point of view. Risks related to data and systems security are specifically mentioned within the scope of the risk management process, **to avoid any misunderstanding that a separate process would be needed to manage security risks** related to medical devices. Specific methods (and requirements) are however used for security risks.'	Note 1: Threat modelling (e.g. STRIDE) should be used in security risk assessment. Note 2: Security risk assessment is assessed in depth during the Technical Documentation Assessment (TDA). During audit, it should be focused on identifying if non-sampled devices also have security risk management including threat modelling.
	IEC 81001-5-1 cl. 4.2	– establish process for managing risks associated with security – use threat modelling for identifying vulnerabilities – estimate, evaluate and control associated threats – monitor effectiveness of (security) risk control measures – intended use and use environment	

	Source	Requirements	Questions / Comments
3.	MDCG 2019-16 chapter 3.7	'The primary means of security verification and validation is testing. Methods can include security feature testing, fuzz testing, vulnerability scanning and **penetration testing**.'	Do all MDR / IVDR devices of the auditee have a recent penetration test? Note 1: Vulnerability scanning and penetration testing should be done for all medical devices. Note 2: Security test reports (including penetration test reports) are assessed in depth during Technical Documentation Assessment (TDA). During audit, it should be focused on identifying if non-sampled devices also have penetration test reports.
	IEC 81001-5-1 cl. 5.7.4	– establish activities to identify and characterize weaknesses – Establish tests that focus on discovering and exploiting security vulnerabilities	

3 Post Market Activities

	Source	Requirements	Questions / Comments
1.	MDCG 2019-16 chapter 3.8	'During the support lifetime of the device, the manufacturer should put in place a process to gather post-market information with respect to the security of the device (see also Chapter 6). This process should take into account: 1. Security incidents directly related to medical device software 2. Security Vulnerabilities that are related to the medical device hardware/software and the 3rd party hardware/software used with the medical device. 3. Changes in the threat landscape, including interoperability aspects'	Does the post-market surveillance system gather and evaluate: • security incidents directly related to the medical devices of the manufacturer? Note: These can be reported via complaint and feedback processes. • the cybersecurity threat landscape? Note 1: The auditee should be capable of using appropriate measures if a significant increase is detected / the auditee should have appropriate threat intelligence at his/her disposal. Note 2: Security vulnerabilities directly related to the medical devices of the manufacturer are discussed in the following.
	IEC 81001-5-1 cl. 6.2.1	– establish activities to collect and review relevant sources of information about vulnerabilities	
2.	IEC 81001-5-1 cl. 9.2	– establish activities that enable reporting of information regarding vulnerabilities (from an internal/external entity or via a complaint-handling system) – reception activity: receive and track closure reports on security related issues – including (minimum) sources as security verification/validation tester, suppliers of third-party components, product developers and testers, …	Does the auditee have an appropriate Vulnerability Disclosure Program in place? Note 1: The Vulnerability Disclosure Program shall make it possible for security researches etc. to submit vulnerabilities to the manufacturer securely. Information about possible vulnerabilities shall be assessed / triaged and mitigated appropriately with an appropriate timeline by the manufacturer. Bug bounties may or may not be provided to the security researchers.

	Source	Requirements	Questions / Comments
			Note 2: The Vulnerability Disclosure Program can be governed by the feedback process. Note 3: Audit event logs shall be obtained and analysed timely and appropriately.
3.	IEC 62304 cl. 5.1.1	– establish software development plan/plans that address software configuration and change management – including SOUP configuration items	Do all medical devices have a list of software of unknown provenance (SOUP) components? Note: The list of SOUP-components can be part of SBOM / can be the SBOM (Software Bill of Materials).
	IEC 62304 cl .8.1.2	– document for each SOUP configuration item used (including standard libraries): title, manufacturer, unique SOUP designator	
4.	MDCG 2019-16 chapter 3.8	'The manufacturer should **evaluate** the information thus gathered, evaluate the associated security and safety risk and take **appropriate measures** that control the risk associated with such security incidents or vulnerabilities. Measures may include: • Information to operators of medical devices on the identified risk and possible mitigations in the operating environment. • Quick fixes, e.g. network **configuration changes**. • Medical device software updates. • 3rd party software **updates** or **patches**.	Does the auditee conduct proper security patch management? Note 1: Scanning / Checking SOUP components for vulnerabilities shall be conducted in intervals commensurate with the risk to patient safety and or data. Checks / Scans should be documented. Note 2: Any necessary corrective action (patching, firewall configuration updates, etc.) should be commensurate with the

	Source	Requirements	Questions / Comments
		The measures should be implemented at the operator site in a **time appropriate** to the security and safety risk determined by the manufacturer and operator.'	risk and implemented in a timely manner. Rationales for not conducting actions should be appropriate.
	IEC 81001-5-1 cl. 9.3	- establish activities that enable investigation of vulnerabilities in a timely manner to determine applicability - verifiability, related threats	
	IEC 81001-5-1 cl. 9.4	- establish activities for analysing vulnerabilities - identifying root cause of the issue - identifying impact on safety and effectiveness	
	IEC 81001-5-1 cl. 9.5	- establish activities to address security-related issues	
5.	IEC 81001-5-1 cl. 4.1.8	– establish activities for conducting periodic reviews of the software problem resolution process – periodic reviews of activities – examine (minimum) security-related issues managed through process (since last periodic review) – determine if management process was complete, efficient, led to resolution of security-related issues – periodic reviews at least annually or as part of monitoring, measurement, analysis	Does the auditee conduct at minimum an annual review of the security patch management process? Note 1: In case periodic review shows lack of performance of the software problem resolution process working appropriately, corrective measures need to be implemented. Note 2: An efficient measure to verify effectiveness of security patches implemented can be penetration testing.

4 Vigilance Reporting

	Source	Requirements	Questions / Comments
1.	MDCG 2019-16 chapter 5.2	• The reporting tools made available to the Manufacturer enable the **use of IMDRF codes** to index. • IMDRF Annex A codes on cybersecurity-related device problems: o Level 2: A1105 — Computer System Security Problem. o Level 3: A110501 — Application Security Problem. o Level 3: A110502 — Unauthorised Access to Computer System.	Do all Manufacturer Incident Report (MIR) forms have an IMDRF code?
	IEC 81001-5-1 cl. 4.1.7	– establish activities for informing regulatory authorities and users about vulnerabilities in a timely manner	
2.	MDR Article 88 (1) IVDR Article 83 (1)	'Manufacturers shall report, by means of the electronic system referred to in Article 92, any ***statistically significant increase*** in the frequency or severity of incidents that are not serious incidents or that are expected undesirable side-effects that could have a significant impact on the benefit-risk analysis referred to in Sections 1 and 8 of Annex I and which have led or may lead to risks to the health or safety of patients, users or other persons that are unacceptable when weighed against the intended benefits.'	Is the auditee able to report trends in cybersecurity-related incidents once the electronic system is available?

	Source	Requirements	Questions / Comments
	MDCG 2019-16 chapter 5.8	• 'Incidents that have **cybersecurity related incident root causes** are **subject to Trend Reporting** under the Medical Devices Regulations.' • 'Using IMDRF codes to index the cybersecurity medical root causes related to non-serious incidents is desirable and may be implemented into the Trend Report': o C1007 — Software Security Vulnerability	