DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

IMDRF International Medical Device Regulators Forum

IMDRF/DITTA Joint Virtual Workshop

Monday 21 Sept. 2020

Cybersecurity - Where are we today?

Latest developments in international standardization activities on cybersecurity in healthcare and medical devices

Ben Kokx

Chair of COCIR Cybersecurity FG

No single silver bullet

Security requirements must be:

- balanced against safety and performance;
- fit the intended use and intended operating environment
- fit the used technologies;
- address the entire life-cycle;
- be applied in all environments, e.g. the manufacturers development, manufacturing and enterprise as well in the end-user's infrastructure;
- Applied to people, products, services & organizations

As a result we have many different security standards developed by different TC's for specific purposes

Cybersecurity standards

There are currently over 600 security standards:

Convergence on a few base standard families:

- Information Technology (IT): *ISO/IEC 27000 family for Information security*
- Operational Technology (OT): *IEC 62443 family for Security of Industrial Automation and Control Systems*

ISO/IEC 15408 series; Information technology - Evaluation criteria for IT security
ISO/IEC 20000 series; Information technology - Service management

ISO/IEC 27000 series; Information technology - Security techniques:
- ISO/IEC 27000; Overview and vocabulary
- ISO/IEC 27001; Information security management systems
- ISO/IEC 27002; Code of practice for information security controls
- ISO/IEC 27003; Information security management system implementation guidance
- ISO/IEC 27004; Information security management - monitoring, measurement, analysis and evaluation
- ISO/IEC 27005; Information security risk management
- ISO/IEC 27007; Information security management systems - auditor guidelines
- ISO/IEC 27008; Guidelines for auditors on ISMS controls
- ISO/IEC 27017; Code of practice for information security controls for cloud services
- ISO/IEC 27018; Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27031; Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032; Guidelines for cybersecurity
- ISO/IEC 27033; Network security
- ISO/IEC 27034; Application security
- ISO/IEC 27035; Information security incident management
- ISO/IEC 27036; Information security for supplier relationships
- ISO/IEC 27043; Incident investigation
- ISO/IEC 27103; Cybersecurity and ISO and IEC Standards
- ISO/IEC 27799; Information security management in health using ISO/IEC 27002

System and Software engineering:
- ISO/IEC 12207; Software life cycle process
- ISO/IEC 15026; Systems and software assurance
- ISO/IEC 15288; System life cycle processes

Health Informatics:
- ISO/IEEE 11073; Personal health device communication - Many device parts...
- ISO/IEC 27799; Information security management in health using ISO/IEC 27002
- ISO 11633; Information security management for remote maintenance of medical devices and medical information systems
- ISO 13606; Electronic health record communication
- ISO 14441; Security and privacy requirements of EHR systems for use in conformity assessments
- ISO 22600; Privelege management and access control
- ISO 27789; Audit trails for electronic health records

IEC 62443 series; Industrial communication networks - Network and system security
- IEC 62443-2-4; Security program requirements for IACS service providers
- IEC 62443-3-3; System security requirements and security levels
- IEC 62443-4-1; Secure product development lifecycle requirements
- IEC 62443-4-2; Technical security requirements for IACS components

IEC 80001 series; Application of risk management for IT-networks incorporating MD
- ISO/IEC 80001-1; Roles, responsibilities and activities
- ISO/IEC 80001-2-1; Step-by-Step Risk Management
- ISO/IEC 80001-2-2; Guidance for the disclosure and communication of medical device security needs, risks and controls
- ISO/IEC 80001-2-3; Wireless Guidance
- ISO/IEC 80001-2-4; HDO Implementation Guidance
- ISO/IEC 80001-2-5; Distributed Alarm Systems
- ISO/IEC 80001-2-6; Responsibility Agreements
- ISO/IEC 80001-2-7; Conformance Self-assessmen
- ISO/IEC 80001-2-8; Guidance on standards for
identified in IEC TR 80001-2-2
- ISO/IEC 80001-2-9; Guidance for use of se

Several technical Information techno
- ISO/IEC 9796; Digital signature schem
- ISO/IEC 9797; Message Authenticati
- ISO/IEC 9798; Entity authenticatio
- ISO/IEC 10118; Hash-functions
- ISO/IEC 11770; Key manage
- ISO/IEC 11889; Trusted Pla
- ISO/IEC 14888; Digital si
- ISO/IEC 15443; Securit
- ISO/IEC 15446; Guid
- ISO/IEC 15946; Cr
- ISO/IEC 17825;
- ISO/IEC 1803
- ISO/IEC 180
- ISO/IEC 1
testing
- ISO/I
req
- ISO
- ISO

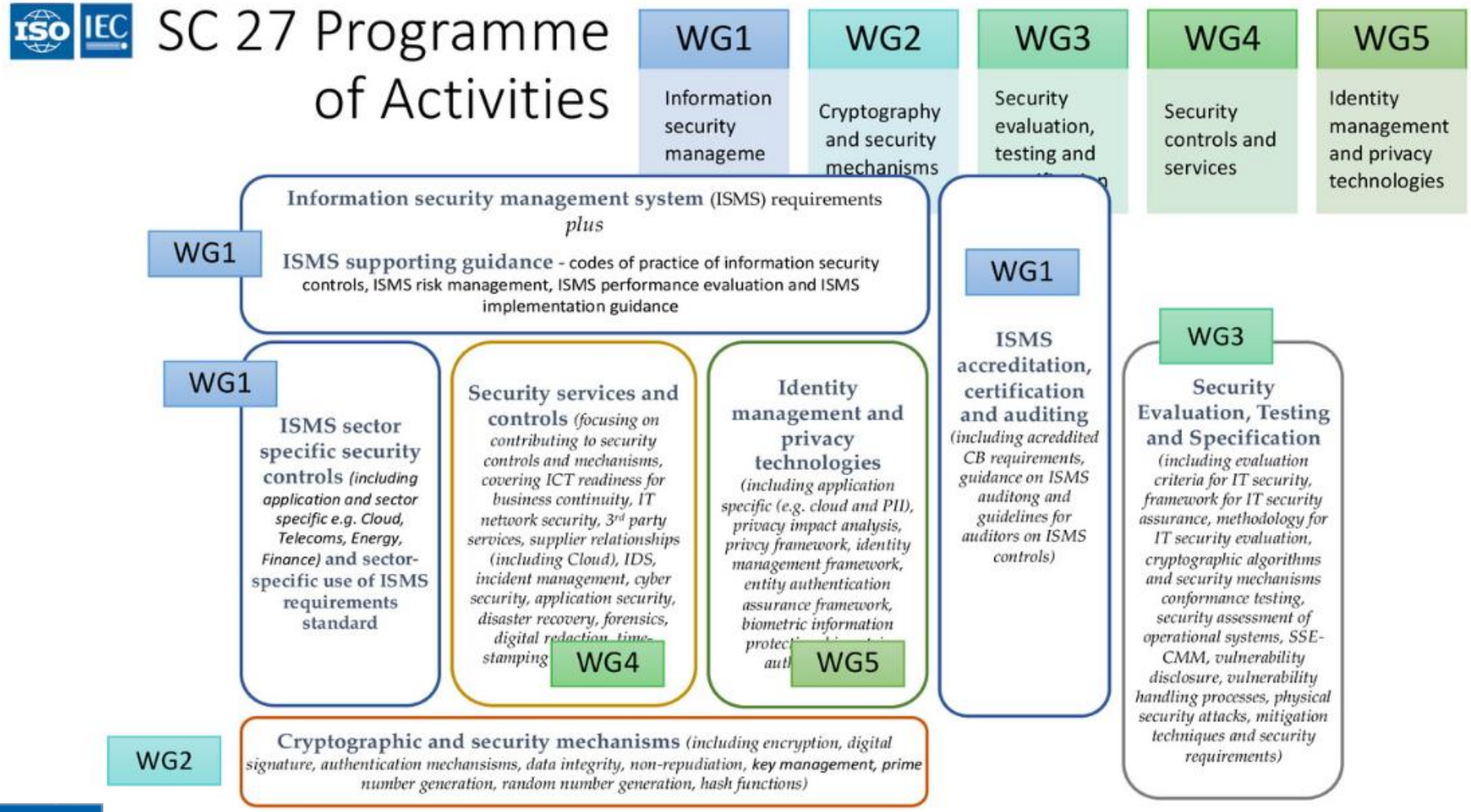
- ISO/IEC 19896; Competence requirements for information security testers and evaluators
- ISO/IEC 19989; Security evaluation of presentation attack detection for biometrics
- ISO/IEC 29115; Entity authentication assurance framework
- ISO/IEC 29128; Verification of cryptographic protocols

Cloud focus:
- ISO/IEC 17788; Cloud overview and vocabulary
- ISO/IEC 17789; Cloud reference architecture
- ISO/IEC 19086; Service level agreement (SLA) framework
- ISO/IEC 19941; Interoperability and portability
- ISO/IEC 19944; Cloud services and devices: Data flow, data categories and data use
- ISO/IEC 27017; Code of practice for information security controls for cloud services
- ISO/IEC 27018; Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 23167; Common technologies and techniques

Safety focus:
- ISO/IEC 14971; Application of risk management to medical devices
- ISO/IEC 60601; General requirements for basic safety and essential performance
- IEC 62304; Medical Device Software - Software life cycle processes
- C 80001; Application of risk management for IT-networks incorporating MD
- 82304; Health Software - General requirements for product safety

ersonal data protection focus:
- ; Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy
nagement — Requirements and guidelines
de of practice for protection of personally identifiable
public clouds acting as PII processors
framework
rchitecture framework
for privacy impact assessment
tice for personally identifiable information protection
irements for information security testers
gineering - Capability Maturity Model (SSE-
sses
ilities in programming languages

ISO/IEC JTC 1/SC 27



ISA99 & IEC TC 65/WG 10

TC 65

Industrial-process measurement, control and automation

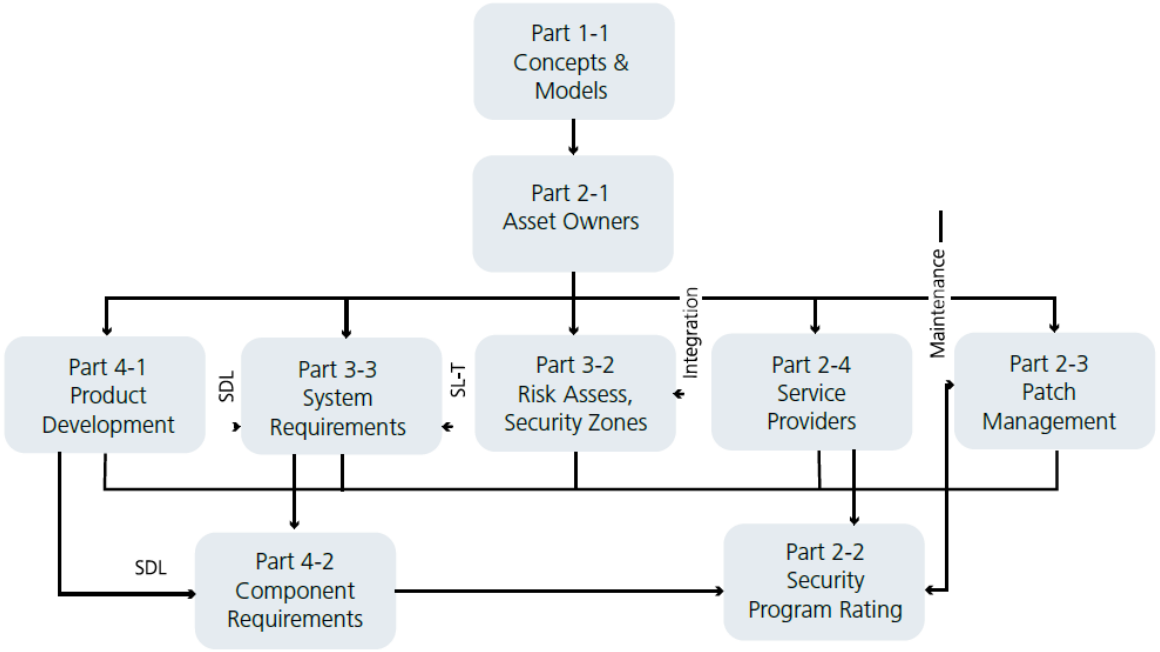
TC 65/WG 10

Security for industrial process measurement and control - Network and system security

TC 65/WG 20

Industrial-process measurement, control and automation– Framework to bridge the requirements for safety and security

IEC TR 63069 Framework for functional safety and security



ISA/IEC 62443 Standards - Hierarchical view

Healthcare scope

JWG 7 - ISO/TC 215 & IEC/SC 62A

Safe, effective and secure health software and health IT systems, including those incorporating medical devices

Standardization in the area of health informatics and electrical equipment in healthcare where ISO/TC 215 and IEC/SC 62A have identified a need for joint standards development.

- Focus on health software, health IT (expanded scope)
- The 'IT-network' is no longer perceived a closed network
- Developments in Cloud, ByoMD, patient/family portals
- Roles of supplier/developer, operator and users are mingled

Current MD security standards

- There are security related requirements embedded in several medical device standards (e.g. **IEC 60601-1 Ed 3.1 & 3.2**)
- **IEC/TR 80001-2-8** has a mapping of the 19 security capabilities defined in **IEC/TR 80001-2-2** to the requirements of several security standards
- Standards focusing on the Health Delivery Organizations, e.g.:
  - **ISO/IEC 80001 series** – Application of risk management for IT-networks incorporating medical devices
  - **ISO 27799** – Information security management in health using ISO/IEC 27002

ISO 14971:2019 Ed 3

Example of changes in this risk management standard related to cybersecurity:

- "It is explained that the process described in ISO 14971 can be used for managing risks associated with medical devices, including those related to data and systems security"
- "The process described in ISO 14971 can be applied to hazards and risks associated with the medical device. Risks related to data and systems security are specifically mentioned in the scope, to avoid any misunderstanding that a separate process would be needed to manage security risks related to medical devices. This does not preclude the possibility of developing specific standards, in which specific methods and requirements are provided for the assessment and control of security risks.
- "Breaches of data and systems security can lead to harm, e.g. through loss of data, uncontrolled access to data, corruption or loss of diagnostic information, or corruption of software leading to malfunction of the medical device.

Overview current security related work items of IEC SC62 and ISO TC 215/WG 4

ISO 17090 multiple parts
Health informatics — Public key infrastructure — Part 4: Digital signatures for healthcare documents

ISO 27799(:2021-7)
Health informatics — Information security management in health using ISO/IEC 27002

ISO/TS 21547 (:2020-09)
Health informatics — Security requirements for archiving of electronic health records — Principles

IEC TR 60601-4-5(:2020-12)
Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices

IEC 62304 Ed2 (:2021-11)
Health software - Software life cycle processes

IEC 80001-1 Ed2 (:2021-07)
Health informatics — Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 1: Application of risk management

ISO/IEC 81001-1 (:2021-06)
Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms

ISO/IEC 81001-5-1 (:2021-11)
Health informatics — Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5: Security – Sub-Part 5-1: Activities in the Product Lifecycle

ISO/IEC 82304-2 (:2021-04)
Health informatics —Quality and reliability criteria for health and wellness apps

draft ISO/IEC 81001-5-1

Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5: Security – Sub-Part 5-1: Security - Activities in the Product Lifecycle

This standard uses a well established and certifiable **secure by design process** standard from the Industrial Control Systems IEC 62443 series:

IEC 62443-4-1:2018 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

The language and definitions did not fully align to what we are used to in Healthcare standards, e.g. we changed Impact to Severity, Damage to Harm and Supplier to Manufacturer

As a heavily regulated sector we needed to add more clarity and explanations to several requirements especially for risk management and its relation to safety

To increase acceptability and ease of implementation ISO/IEC 81001-5-1 restructured IEC 62443-4-1 to follow the structure of IEC 62304 and the standard mainly talks about additional activities to be executed within the 62304 processes

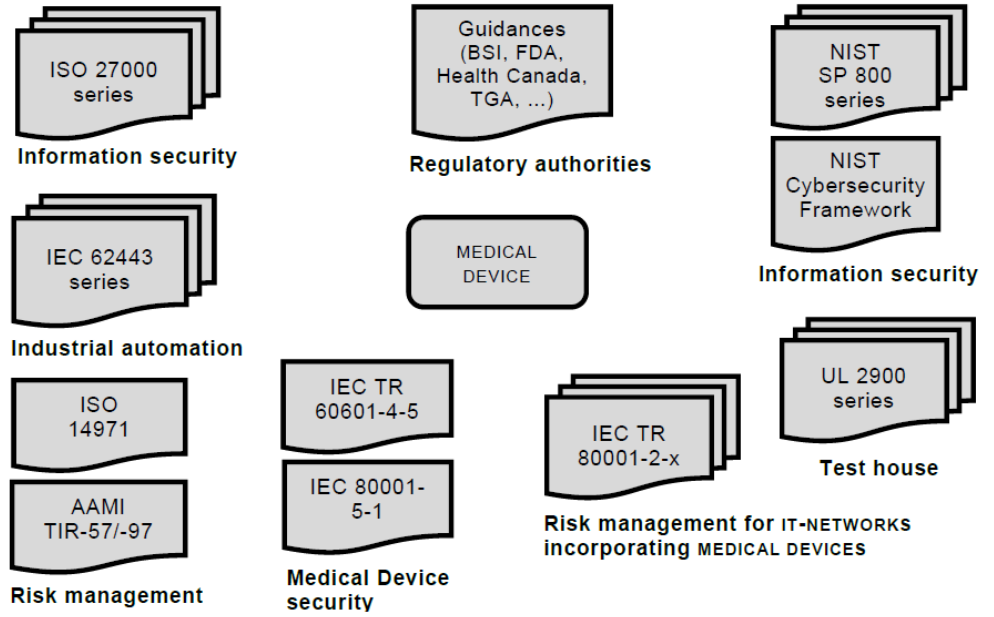
draft IEC TR 60601-4-5

Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices

➔Application of IEC 62443-4-2 (Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components) for medical devices

906 **A.4 Correlation to existing regulations, standards and technical specifications**

907 The sheer number of cybersecurity frameworks, standards and guidance documents may seem
908 overwhelming to the MEDICAL DEVICE MANUFACTURER. The following illustration shows an
909 overview of the most commonly used frameworks, standards and guidance used for MEDICAL
910 DEVICES.



911

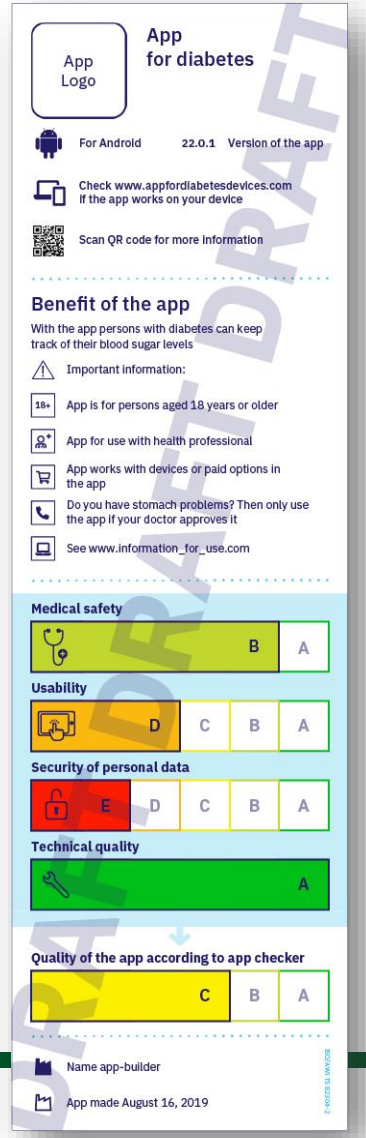
912 **Figure A.7 – Selection of IT security related documents**

draft ISO/IEC TS 82304-2

Health Software — Part 2: Quality and reliability criteria for health and wellness apps

Started as a CEN/TC 251 based on BSI PAS 277, has three main parts:

1. A walkthrough of relevant international Health Software product and process standards
2. defines the evidence that an app manufacturer should provide to show that their app conforms to the specification (Product information, Privacy, Safety and Security, Clinical Assurance, Usability (and Accessibility) and technical assurance
3. Annexes covering a range of topics such as a mapping between the product and process requirements, ethical considerations, relevant security and privacy considerations



Top 10 in current Guidance's

IEC	80001-1 *	Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities
IEC	TR 80001-2-2	Part 2.2: Guidance for the disclosure and communication of medical device security needs, risks and controls
IEC	TR 80001-2-8	Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
NEMA	MDS2	Manufacturer Disclosure Statement for Medical Device Security
AAMI	TIR57	Principles for medical device security - Risk management
ISO	27799	Health informatics — Information security management in health using ISO/IEC 27002
IEC	TR 80001-2-1 *	Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples
ISO	TR 80001-2-7 *	Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to selfassess their conformance with IEC 80001-1
NIST	CSF	Cybersecurity Framework (Framework Core requirements provide informative references to CIS SCS, COBIT 5, ISA 62443-2-1, ISA 62443-3-3, ISO/IEC 27001 and NIST SP 800-53)
ISO/IEC	29147	Information technology — Security techniques — Vulnerability disclosure
ISO/IEC	30111	Information technology — Security techniques — Vulnerability handling processes

*): These standards predominately focus on the Healthcare Delivery Organization

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

IMDRF International Medical Device Regulators Forum

Thank you!