Shared Responsibility
The manufacturers view

COCIR Seminar - Cybersecurity in Healthcare

Online, 2020-06-30

Ben Kokx

Chair of the COCIR Cybersecurity Focus Group,
Director Product Security Philips

Security & Privacy, the bigger regulatory picture

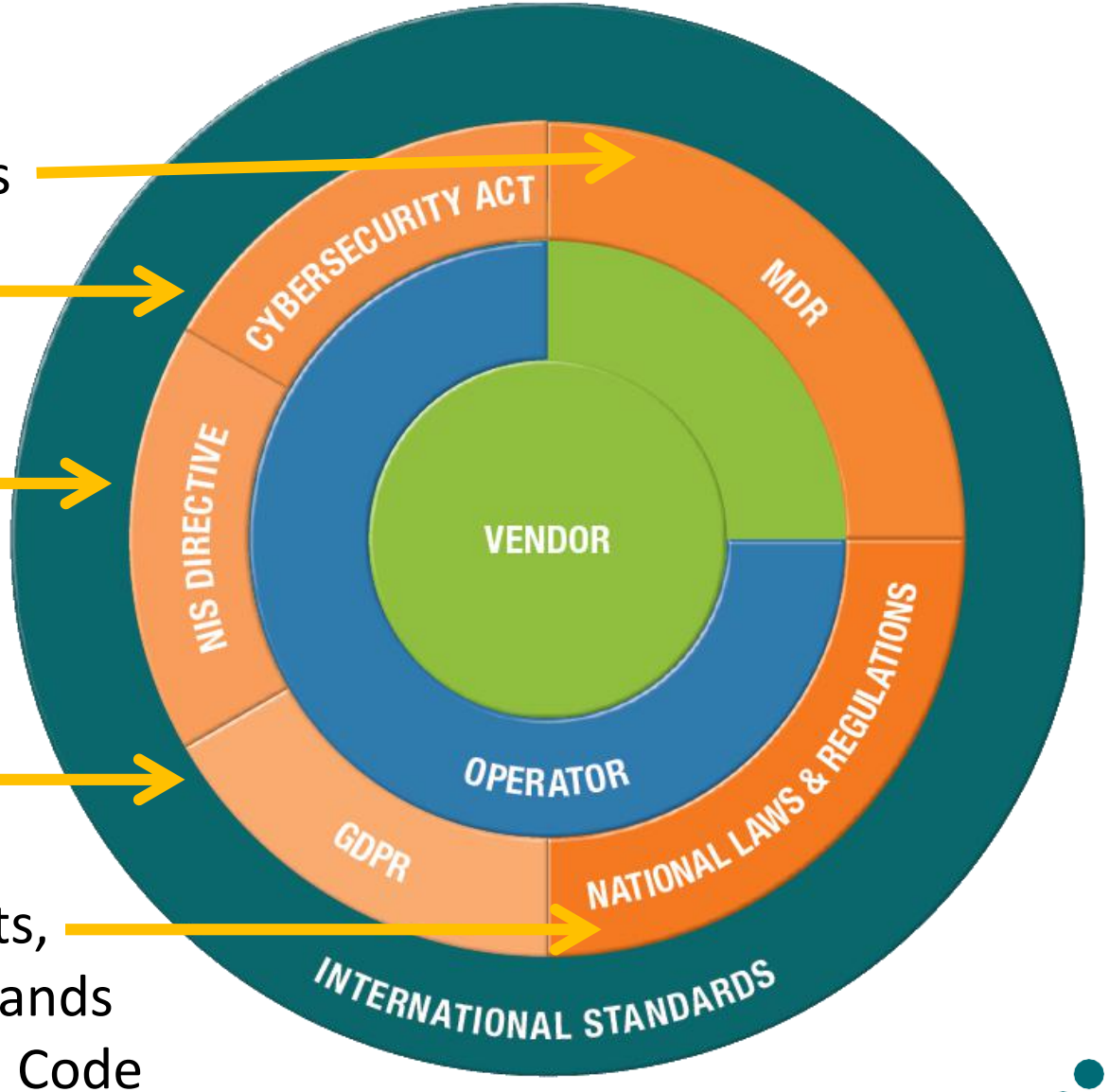
MDR focus on manufacturers

CSA and its schemes are still under development

Critical infrastructure requirements, e.g. BSI-KRITIS in Germany

GDPR requires appropriate security measures

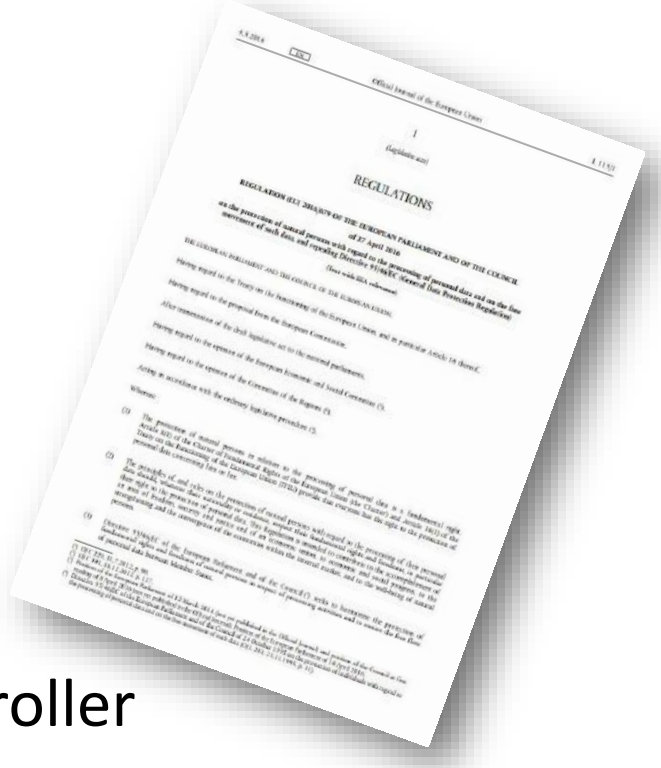
Country specific requirements, e.g. NEN 7510 in the Netherlands and the French Public Health Code



Both GDPR and MDR/IVDR set legislative requirements for shared responsibility

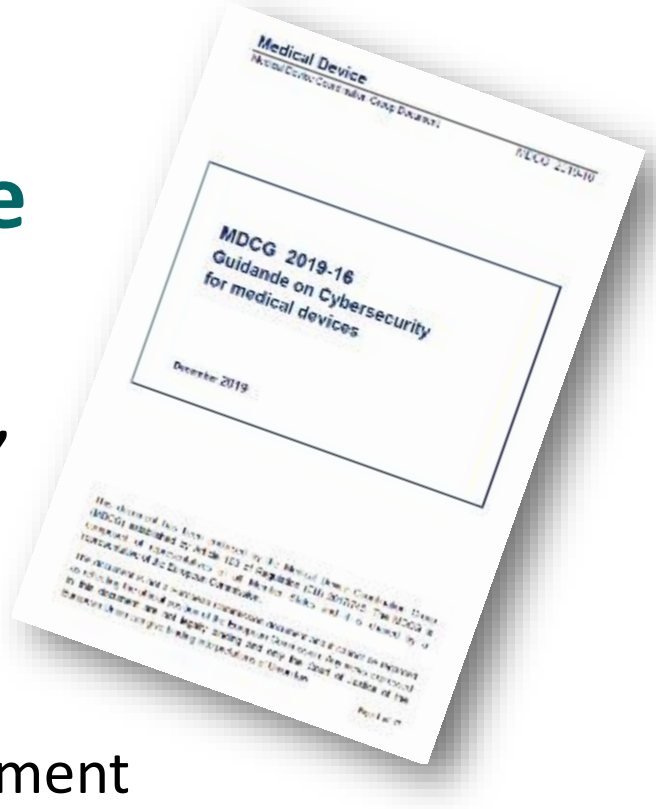
- General Data Protection Regulation (GDPR)
  - Controller and Processor roles
  - Data processing agreements to enforce requirements on processor
- MDR & IVDR (including the MDCG cybersecurity guidance)
  - MDR requirements make manufacturer responsible for security risk management and providing information to the operator on minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
  - Manufacturer, Integrator, Operator and Users (including healthcare & medical professionals, patients & consumers) roles
- NIS Directive
  - Only defines obligations for the operators

General Data Protection Regulation



- European hospitals are subject to the GDPR, and must have a written data processing agreement in place with all your data processors.
- The manufacturer is usually a data processor under the governance of the hospital as the controller
- “Data processing” essentially refers to anything you can possibly do with someone’s personal information, but the extend to which the provision of service / maintenance falls under ‘structural data processing’ might be a debate for products
- A data processor agreement is always needed where structural data processing takes place or where structural and uncontrolled access to personal data is possible, e.g. when providing services

MDR & IVDR cybersecurity guidance



- Developed by DG Grow, Joint Research Center, European regulators, ENISA, notified bodies, hospital and industry associations
- Details concepts around
  - Relation between safety and security risk management
  - Joint Responsibility
  - Security requirements for the operating environment
  - Documentation
  - Post market surveillance and vigilance
- Available via: https://ec.europa.eu/docsroom/documents/38924

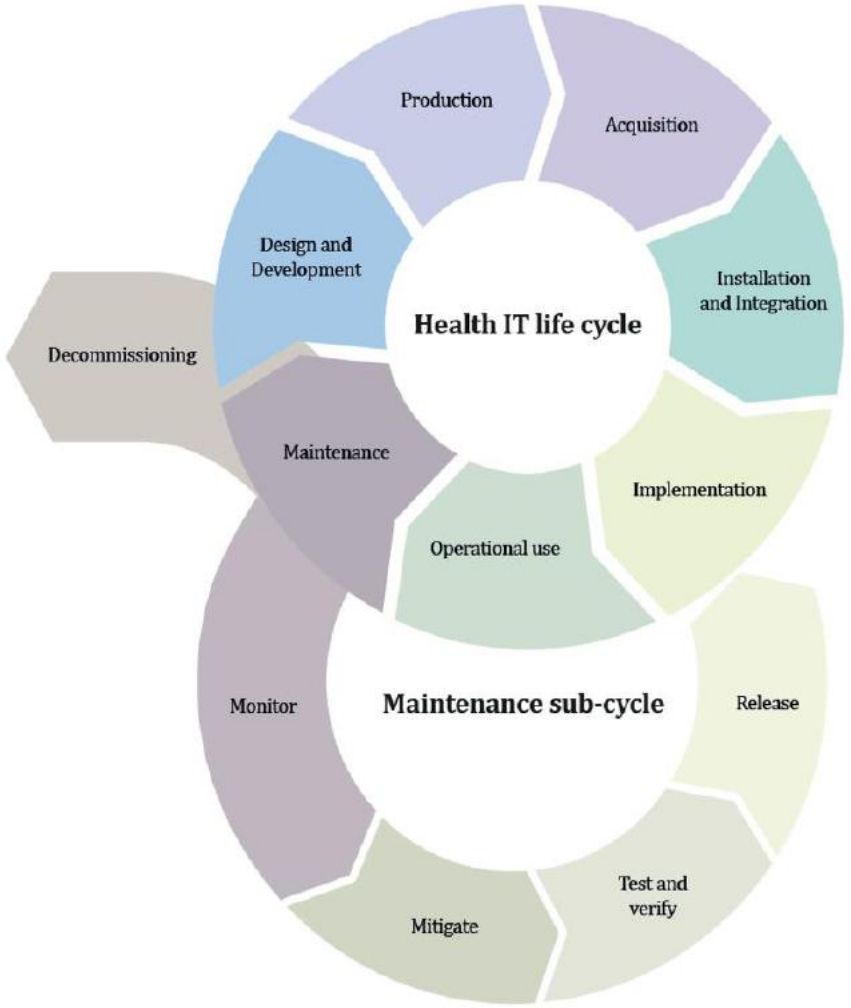
MDCG Guidance on Cybersecurity for medical devices (EU-MDR)

2.6. Joint Responsibility - Specific expectations from other stakeholders

While the MDR and the IVDR provide legal obligations only with regard to manufacturers, however it should be noted that for the provision of secured healthcare services, it is important to recognise the roles and expectations of all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators and regulators. All of these actors share responsibilities for ensuring a secured environment for the benefit of patients' safety.

EU-MDR MDCG Guidance on Cybersecurity
The Manufacturer role

- The manufacturer is responsible to address cybersecurity during the entire product life cycle.
- The expected intended operational environment of use has to be clearly documented (e.g. in the IfU).
- Newly identified threats and remediation scenarios have to be communicated.



ISO 81001-1

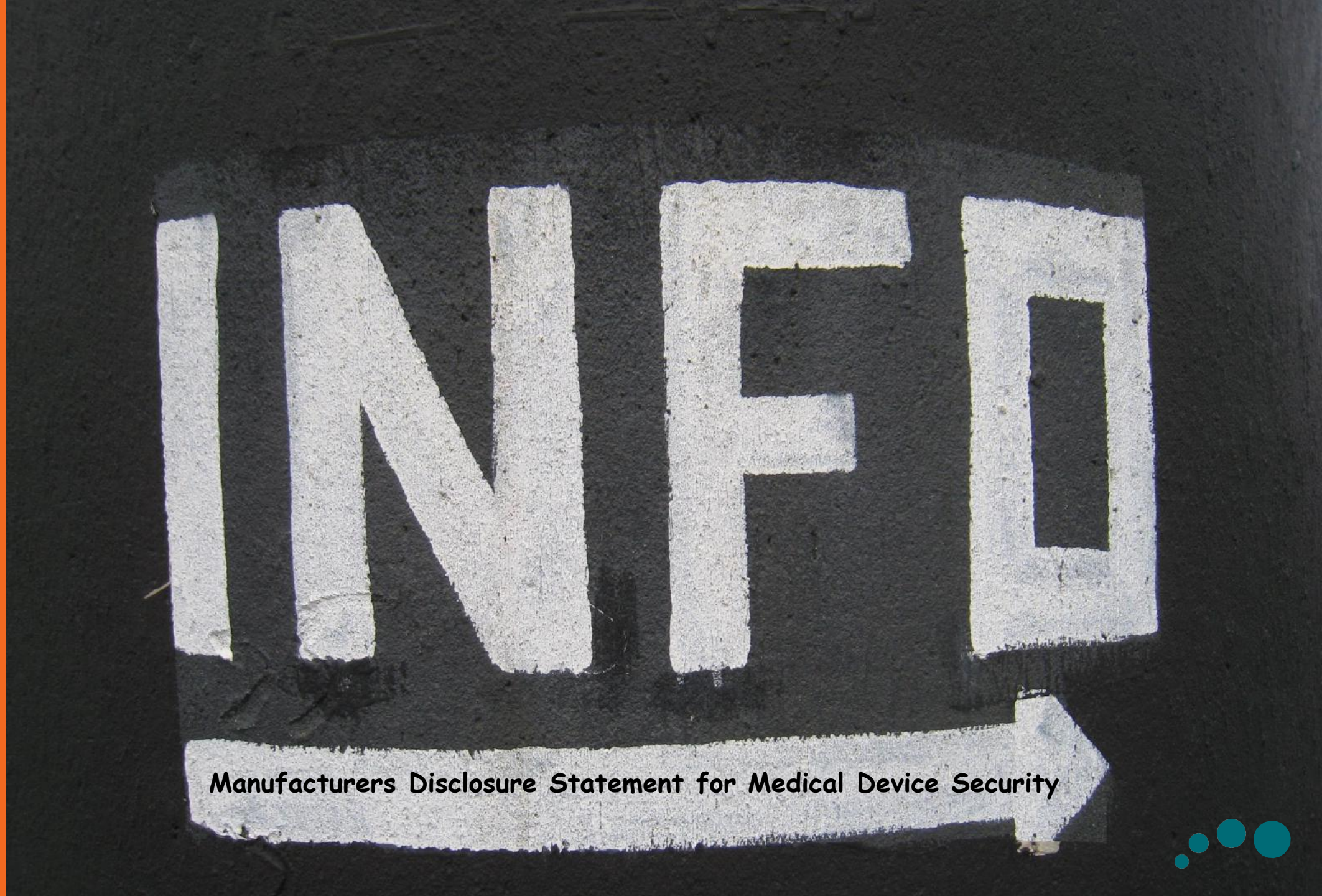
EU-MDR MDCG Guidance on Cybersecurity
The Operator role

- The operator is responsible for the procurement and should ensure that security is maintained during the operation and application of the system (medical device), and particularly not compromised by changes in the environment or by user interaction.
  - Ensure required level of security for operational environment (network, physical, …);
  - Provide required infrastructure (network, physical);
  - Ensure that personnel are properly trained and available in case of security issues;
  - Ensure that system is used as proscribed by manufacturer guidelines (e.g. no physical access by unauthorized users, password policies kept, network security measures);
  - Ensure that prescribed maintenance is done as required, including installation of security patches;
  - Notify the manufacturer without delay of any suspected security event.
- Annex I provides the mapping of IT security requirements to NIS Directive Cooperation Group measures

Sharing of information

- Information sharing must be bidirectional
- Security information through accompanying documentation such as but not limited to Instructions for Use, Instructions for Administrators and Network administrator guides
- Information published on the manufacturers website or part of procurement process:
  - Security and Privacy whitepapers
  - MDS2 documents
  - System security status / patch information
  - Security notifications
  - Other security relevant information

COCIR
Advancing Healthcare



Manufacturers Disclosure Statement for Medical Device Security

Manufacturers Disclosure Statement for Medical Device Security (MDS2)

- Developed by HIMSS, American College of Clinical Engineering (ACCE) and National Electrical Manufacturers Association (NEMA) to address the many hospital specific forms related to the new HIPAA regulation in the USA
- MDS2 form provides healthcare providers with an overview of the security related features of the medical device
- The MDS2 form can be used in an organization's risk assessment process, assessing vulnerabilities and risks associated with protecting the health information created, received, transmitted or maintained by medical devices
- Key benefits of using the standardized MDS2 form includes:
  - Providing a comprehensive set of medical device security questions developed through broad stakeholder participation and medical device vendor buy-in
  - Allowing for comparison of security features across different devices and manufacturers
  - Facilitating the review of the large volume of security-related information supplied by the manufacturers

MDS2 snippet

AUDT-2.9	Emergency access?	Yes	When the emergency access function is invoked a username is not requested. A default user name (emergency) is recorded in the AUDIT TRAIL along with the emergency access date, access time and a unique exam identifier.
AUDT-2.10	Other events (e.g., software updates)?	Yes	Events according IHE ATNA are recorded in the audit log. 1. Security Alert events such as a. Disabling of disk encryption or change of encryption settings b. Internal security integrity check failures (For example signature verification) c. Creation of new disk recovery Key d. Time sync events 2. User authentication events such as a. User Id locked event 3. New software available for installation event 4. Software installation started.
AUDT-2.11	Is the audit capability documented in more detail?	Yes	Philips internal design documentation contains all details. Any audit capability can be explained on requests.
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	—
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	AuditUserAuthenticationEvent : Name of the user AuditSecurityAlert : Name of the user, description AuditApplicationActivityEvent : Name of the user, AE Title AuditNetworkEntry : AE Title, Description AuditDicomdeleteStudy : AE Title, DiCOM instance AuditDICOMInstanceAccess : AE Title, DiCOM instance AuditConfigurationChange : Name of user, description of configuration change.
AUDT-4.1	Does the audit log record date/time?	Yes	—

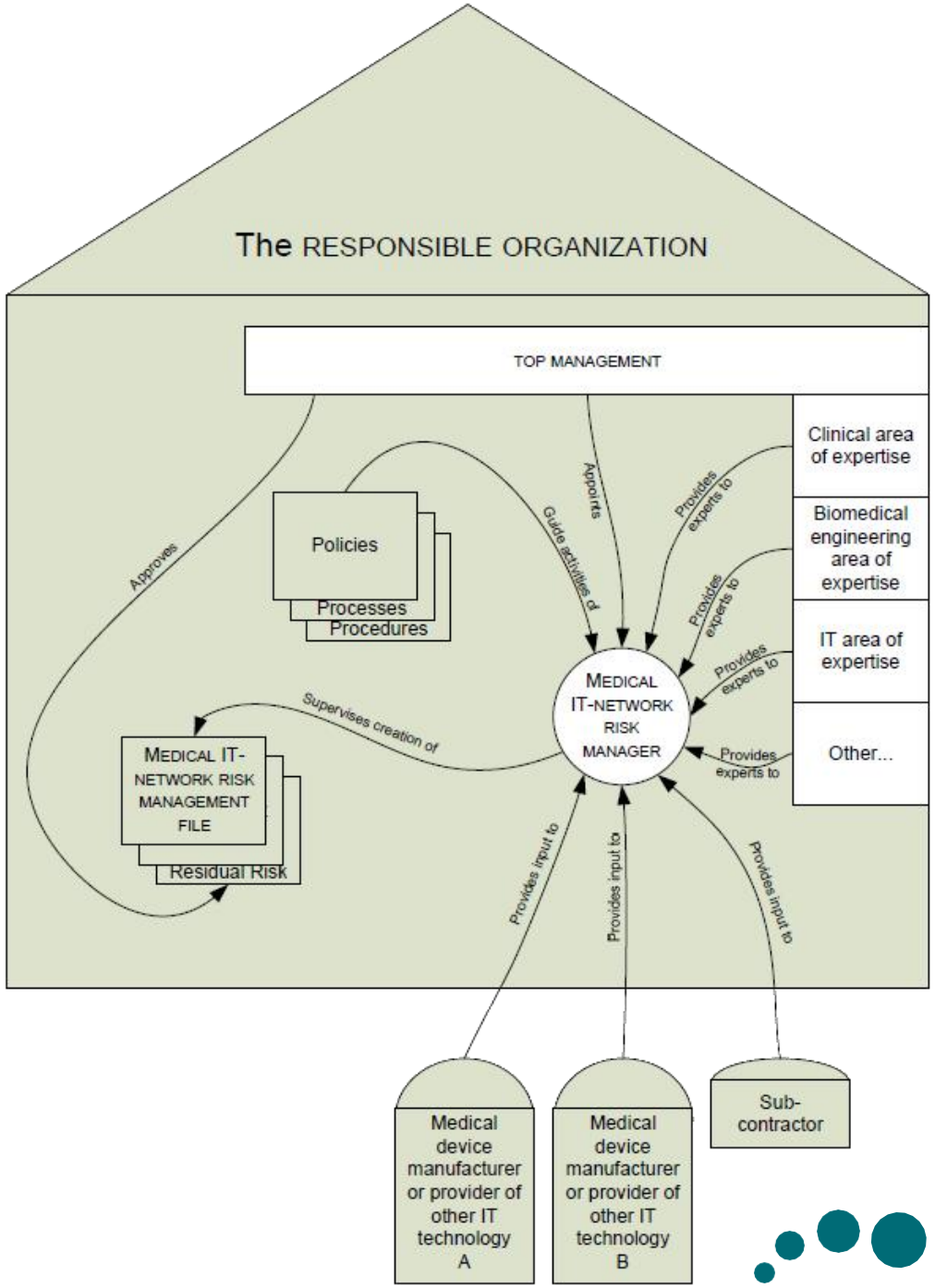
MDS2 mapping to ISO 27002 controls

AUDT-2.9	Emergency access?	Yes	When the emergency access function is invoked a username
AUDT-2.10	Other events		
AUDT-2.11	Is the audit c		
AUDT-3	Can the own are recorded		
AUDT-4	Is a list of dat audit log for		
AUDT-4.1	Does the audit log record date/time?	Yes	

AUDT-2.11	Is the audit capability documented in more detail?	
	☐ 12.4.1	Event logging
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	
	☐ 12.4.1	Event logging
	☑ 12.4.3	Administrator and operator logs
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	
	☐ 12.4.1	Event logging
	☐ 12.4.3	Administrator and operator logs
AUDT-4.1	Does the audit log record date/time?	
	☑ 12.4.1	Event logging
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	
	☑ 12.4.4	Clock synchronisation

ISO/IEC 80001

- The recognition that medical devices are integrated into IT networks which can lead to risk.
- This standard defines roles and responsibilities for the activities necessary for risk management of IT networks that contain medical devices.
- Addressing the key properties: safety, effectiveness and data & system security.



Global views on shared responsibility

FDA
Mitigating Cybersecurity Risks

Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place.

- **Medical device manufacturers (MDMs)** are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity.
- **Health care delivery organizations (HDOs)** should evaluate their network security and protect their hospital systems.
- **Both MDMs and HDOs** are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

IMDRF

Principles and Practices for Medical Device Cybersecurity

Introduction

.....

Stakeholders within the healthcare sector have a shared responsibility regarding medical device cybersecurity. This guidance intends to assist all stakeholders in gaining a better understanding of their role in support of proactive cybersecurity that helps protect and secure medical devices in anticipation of future attacks, problems, or events.

.....

Shared Responsibility

Medical device cybersecurity is a shared responsibility between stakeholders including the manufacturer, healthcare provider, users, regulator, and vulnerability finder. All stakeholders must understand their responsibilities and work closely with other stakeholders to continuously monitor, assess, mitigate, communicate, and respond to potential cybersecurity risks and threats throughout the life cycle of the medical device.

COCIR
Advancing Healthcare