QAdvis

Introduction to ISO/IEC 80001-1

Application of Risk management for IT-networks incorporating Medical devices

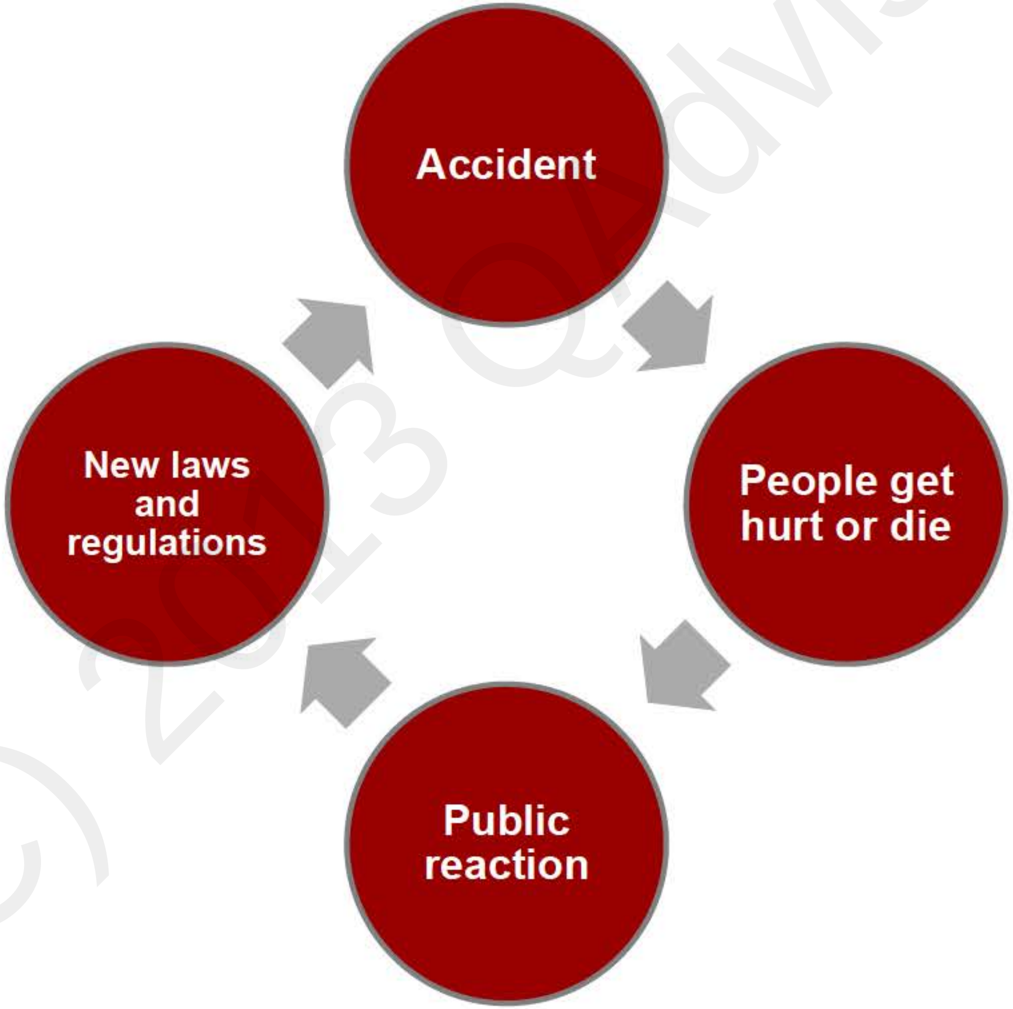
Why do we need another standard?

Introduction of Speakers

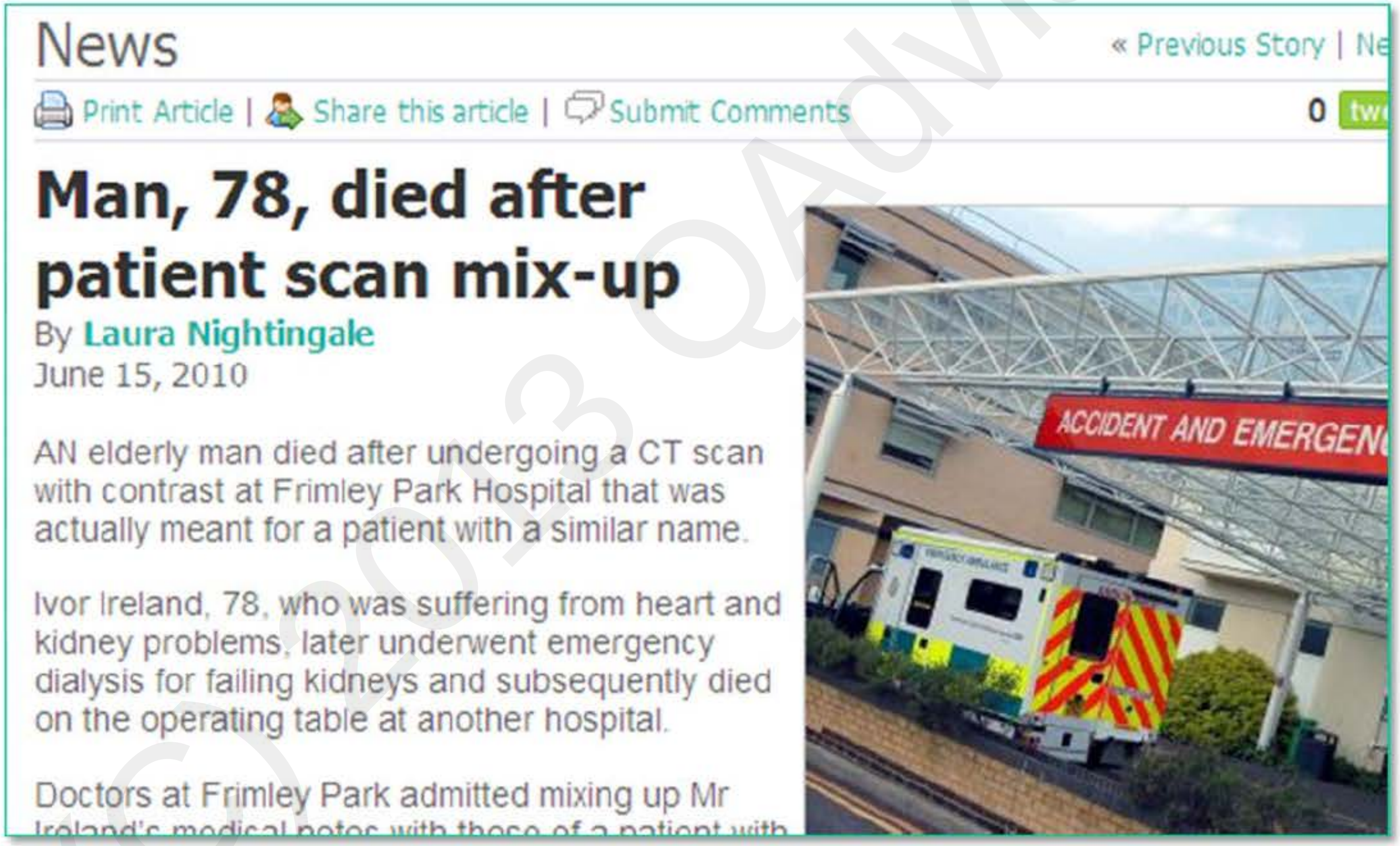
Robert.Ginsberg@QAdvis.com

- 26 years in software development
- 18 years in Medical Device software
- Participated in > 20 audits, FDA, MDD etc.
- Co-author of IEC/ISO 62304 (80001-1 and 80002-X)
- Working member of Cenelek TK-62 and JWG3

The bar is raised over time



Media report the mishaps, and we as the society don't accept as we mature



News

« Previous Story | Ne

Print Article | Share this article | Submit Comments

0 twe

Man, 78, died after patient scan mix-up

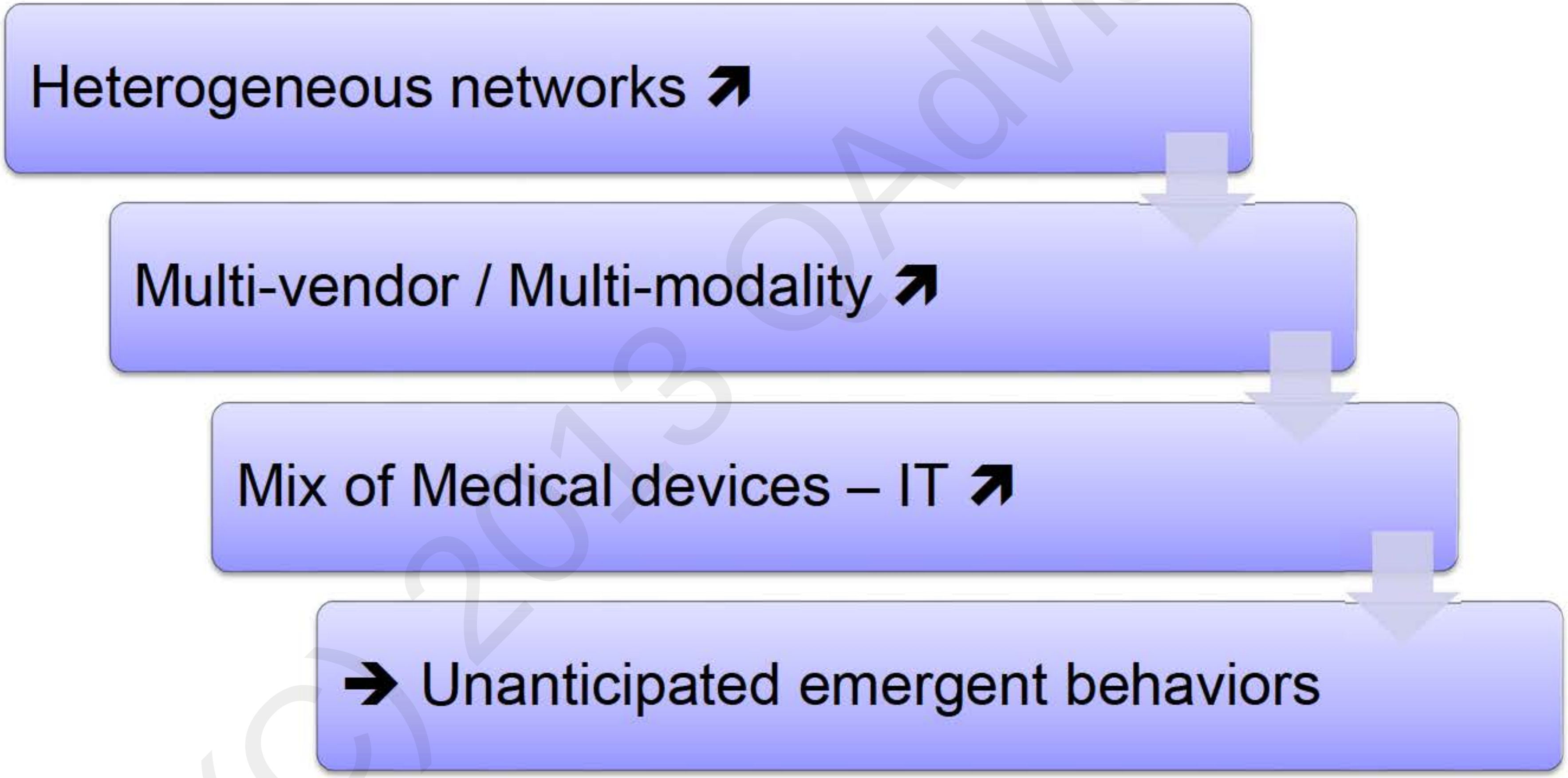
By Laura Nightingale
June 15, 2010

AN elderly man died after undergoing a CT scan with contrast at Frimley Park Hospital that was actually meant for a patient with a similar name.

Ivor Ireland, 78, who was suffering from heart and kidney problems, later underwent emergency dialysis for failing kidneys and subsequently died on the operating table at another hospital.

Doctors at Frimley Park admitted mixing up Mr Ireland's medical notes with those of a patient with

What is the problem we are facing with MedTech and IT?



Heterogeneous networks ↗

Multi-vendor / Multi-modality ↗

Mix of Medical devices – IT ↗

→ Unanticipated emergent behaviors

Integration of Medical devices is becoming a challenge

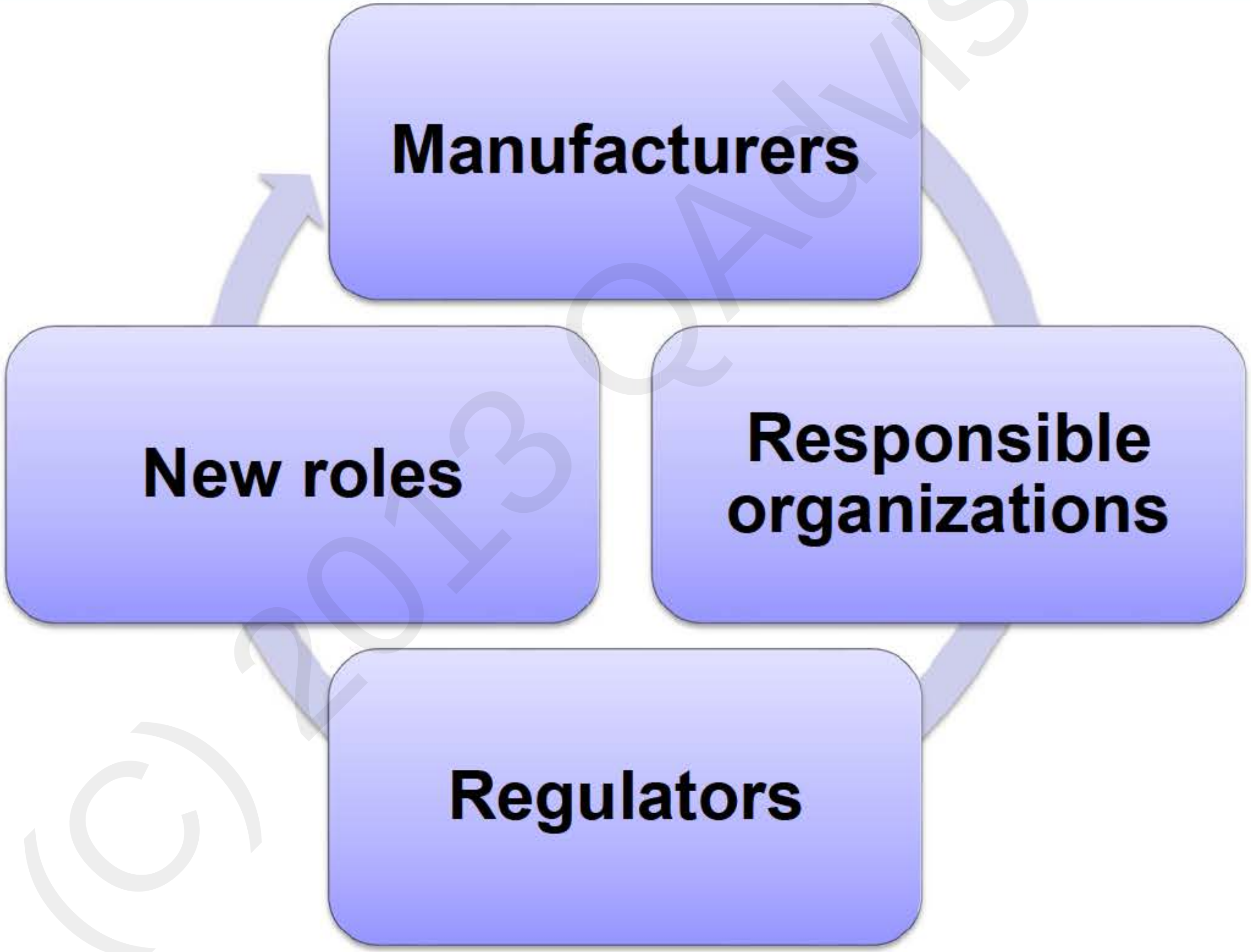
Manufacturers

Devices

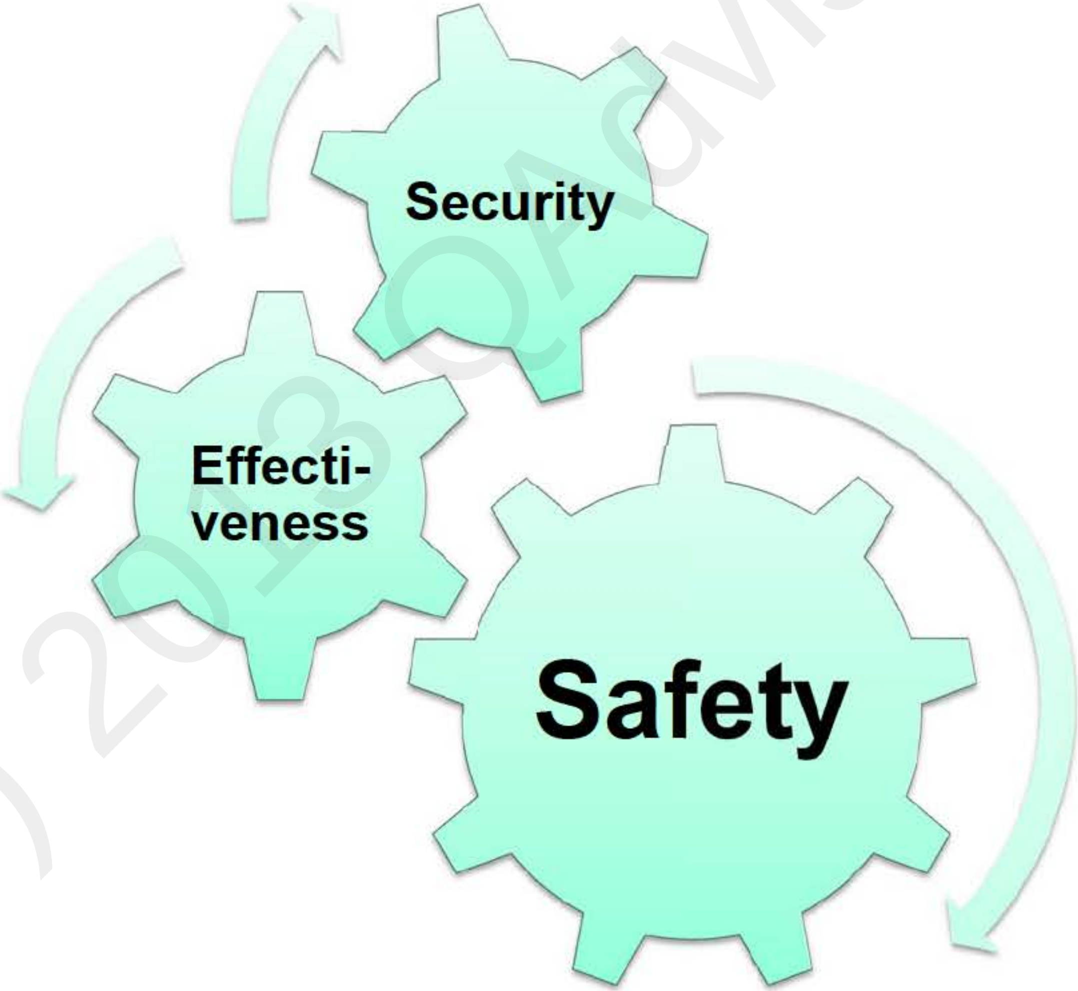
Involuntary Integrators

The complexity of the Information Technology is growing fast

Who needs to address the problem?



What properties need to be ensured?



IEC/ISO 80001 is made to resolve this problem

IEC - ISO

- Key stakeholder
  - Medical Device Manufacturers
  - Hospitals
  - FDA

Published in 2010

Risk management is the key activity in 80001

Responsible organization

- Accountable for the **use** and **maintenance** of an ME Equipment or an ME System

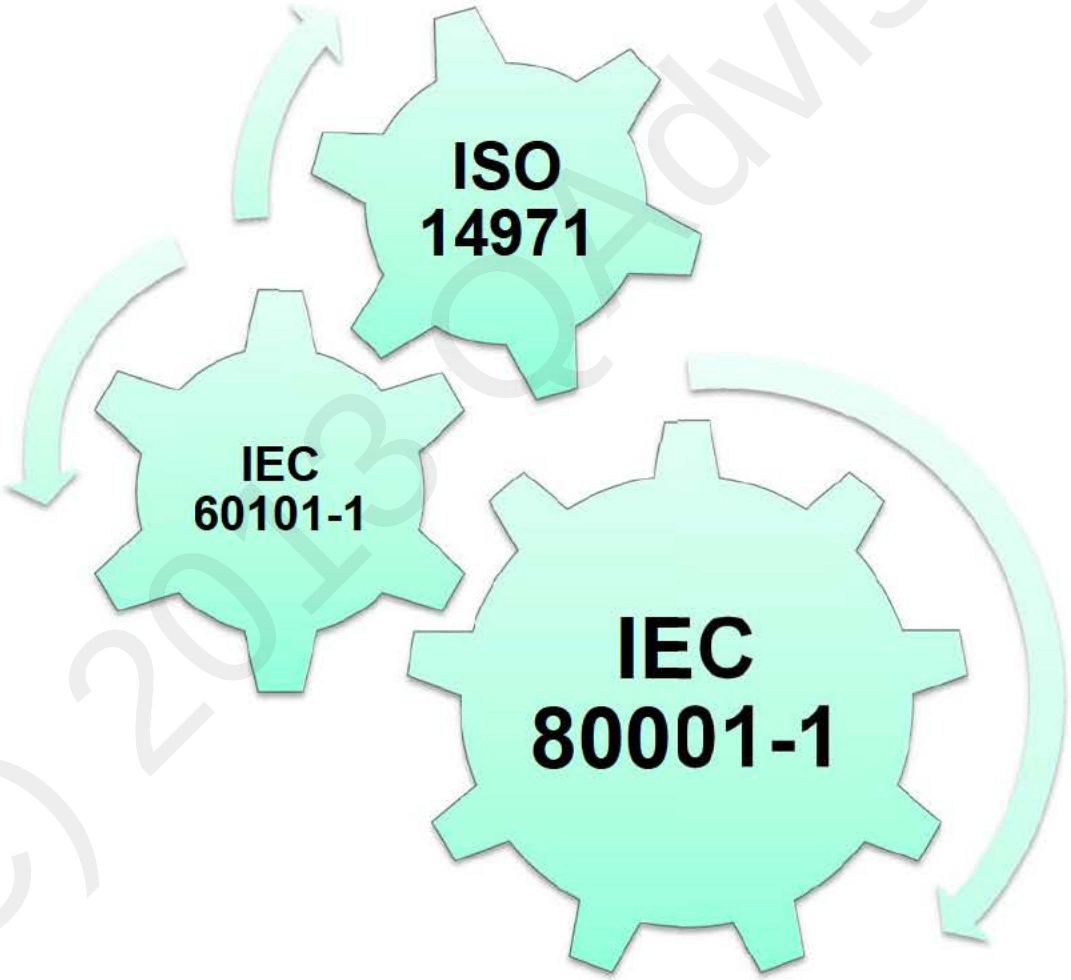
Hazards of Medical Devices in networks

- ISO 14971

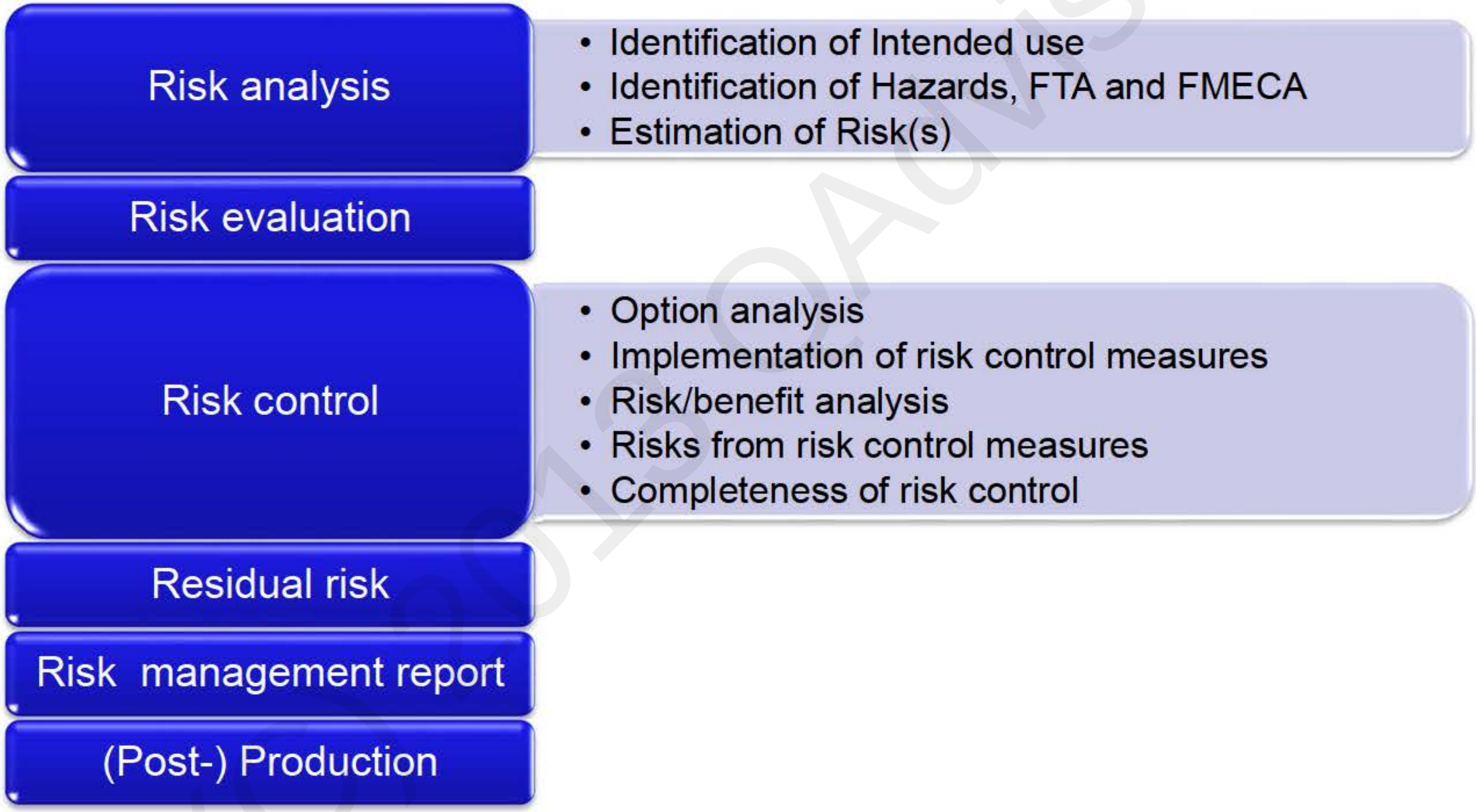
Residual risk

- Approval by appropriate person

There are three standards that are tightly interrelated



ISO 14971 is the established standard for Risk Management



Risk analysis

- Identification of Intended use
- Identification of Hazards, FTA and FMECA
- Estimation of Risk(s)

Risk evaluation

Risk control

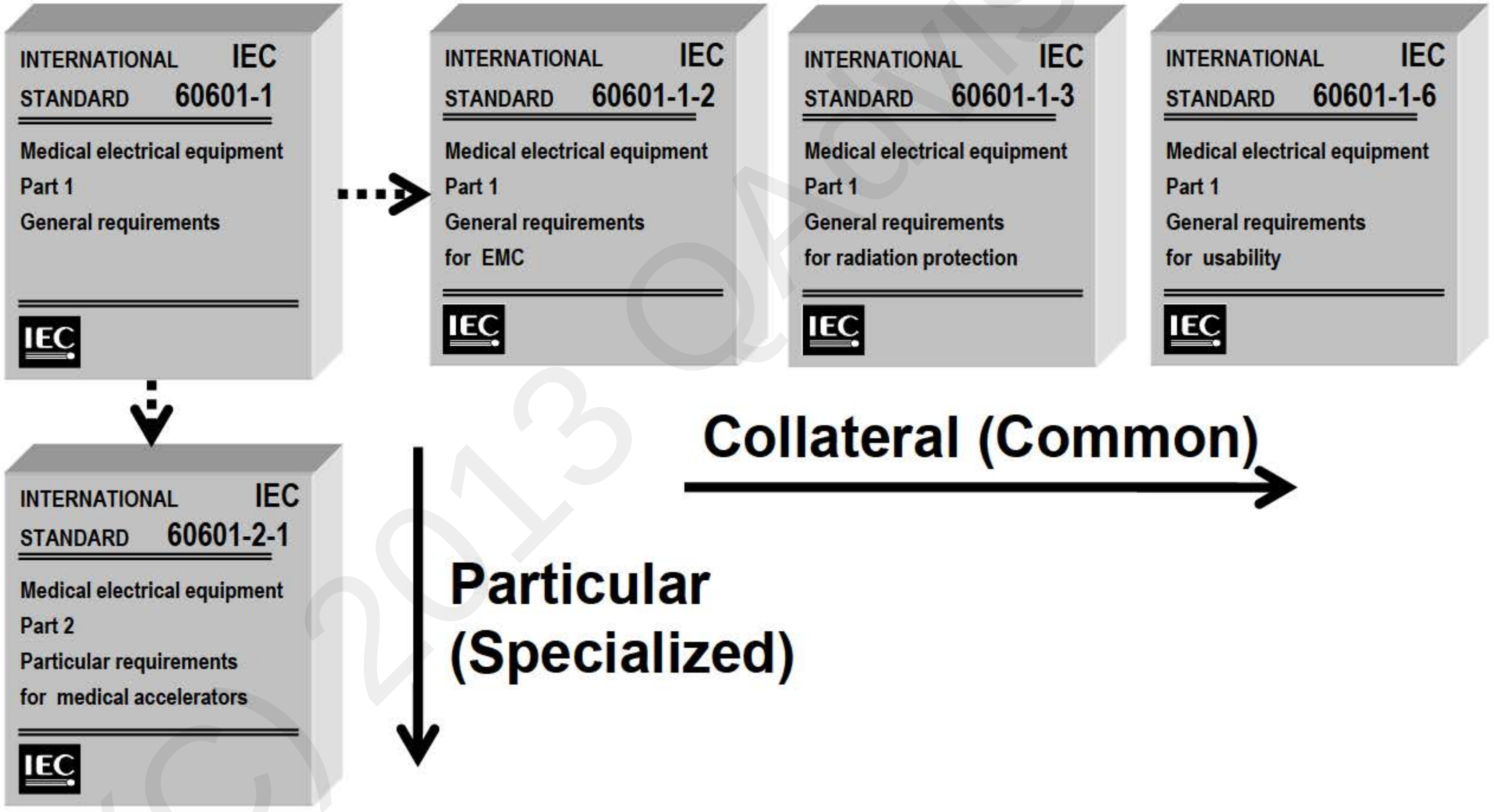
- Option analysis
- Implementation of risk control measures
- Risk/benefit analysis
- Risks from risk control measures
- Completeness of risk control

Residual risk

Risk management report

(Post-) Production

IEC 60601-series assure Basic Safety and Essential performance



INTERNATIONAL STANDARD IEC 60601-1

Medical electrical equipment
Part 1
General requirements

INTERNATIONAL STANDARD IEC 60601-1-2

Medical electrical equipment
Part 1
General requirements
for EMC

INTERNATIONAL STANDARD IEC 60601-1-3

Medical electrical equipment
Part 1
General requirements
for radiation protection

INTERNATIONAL STANDARD IEC 60601-1-6

Medical electrical equipment
Part 1
General requirements
for usability

INTERNATIONAL STANDARD IEC 60601-2-1

Medical electrical equipment
Part 2
Particular requirements
for medical accelerators

Collateral (Common)

Particular (Specialized)

New Hazards are arising from networks

- IEC 60601-1 3rd edition tries to address this
  - EU – 2012 -06-01
  - USA – 2013-06-30

- Targets the manufacturers

IEC 60601-1 3rd ed. Section 14.13

... the technical description shall **instruct the RESPONSIBLE ORGANIZATION** that:

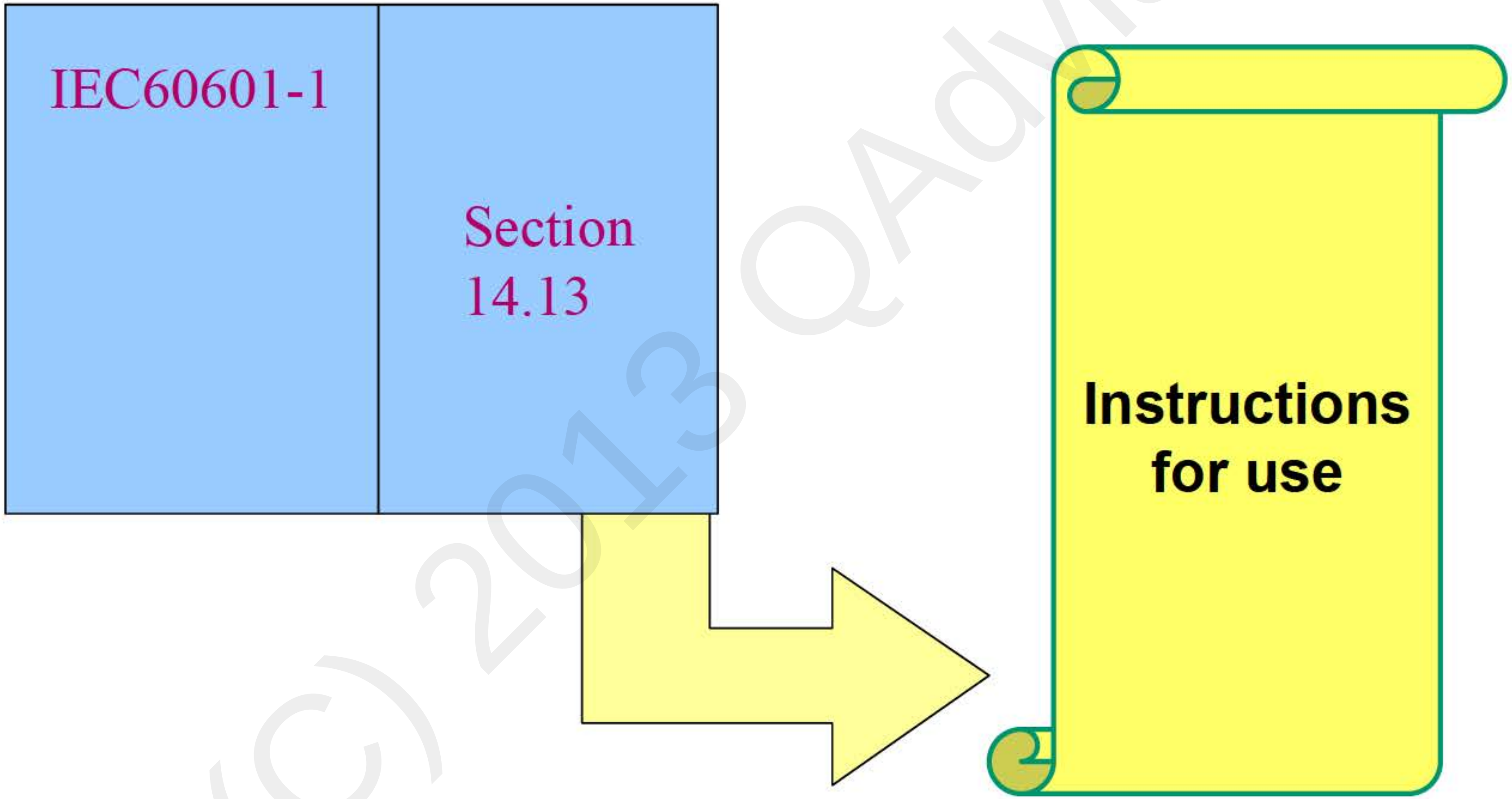
- connection of the PEMS to a NETWORK/DATA COUPLING that includes other equipment could **result in previously unidentified RISKS**
- the **RESPONSIBLE ORGANIZATION** should identify, analyze, evaluate and **control these RISKS**

IEC 60601-1 3rd ed. Section 14.13

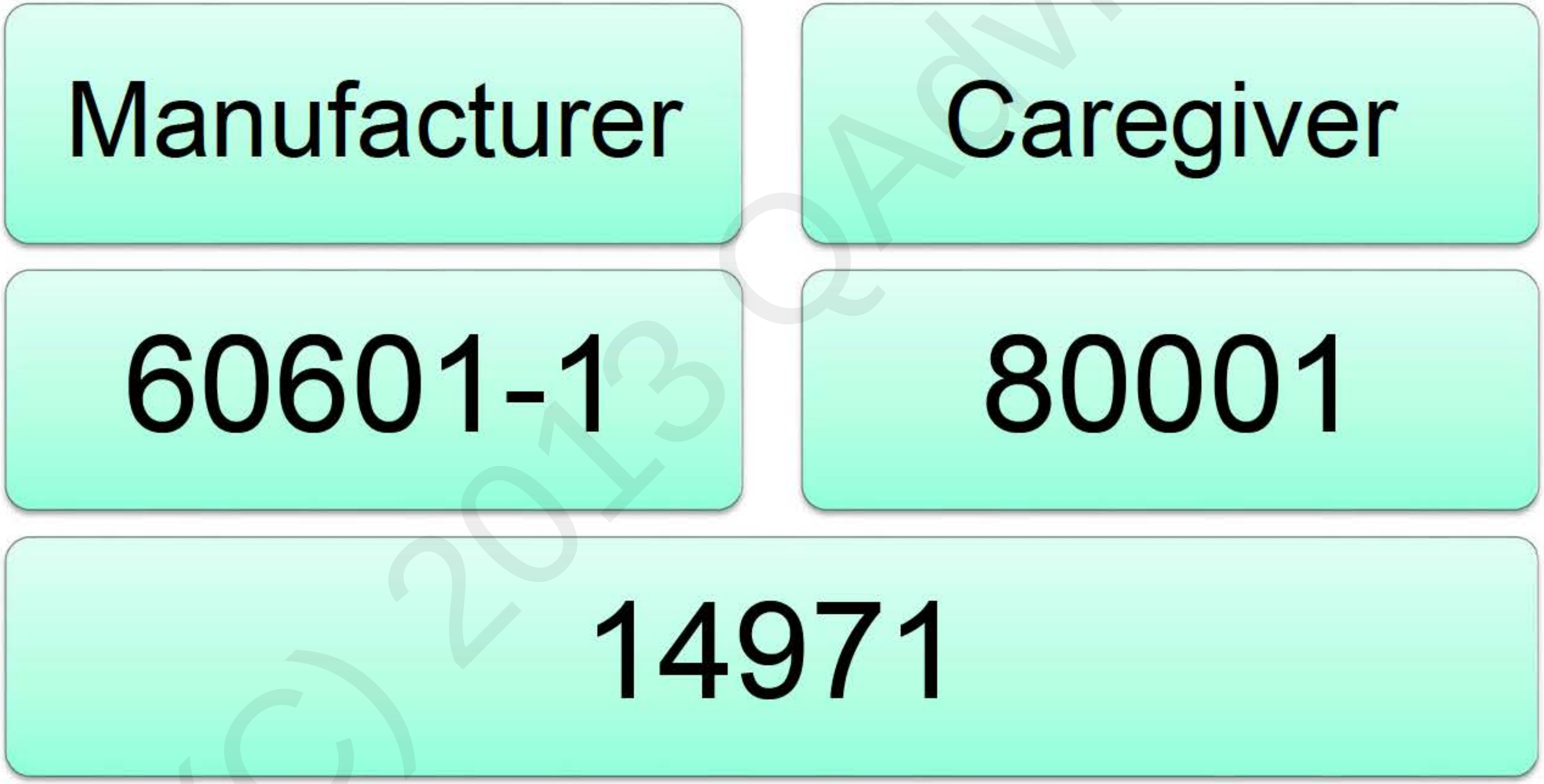
... the technical description shall **instruct the RESPONSIBLE ORGANIZATION** that:

- **changes** to the NETWORK/DATA COUPLING could introduce new RISKS and require additional analysis
- ...

The obvious solution is to extend the Instructions for use



ISO/IEC 80001 enables an interface between manufacturers and caregivers



Manufacturer

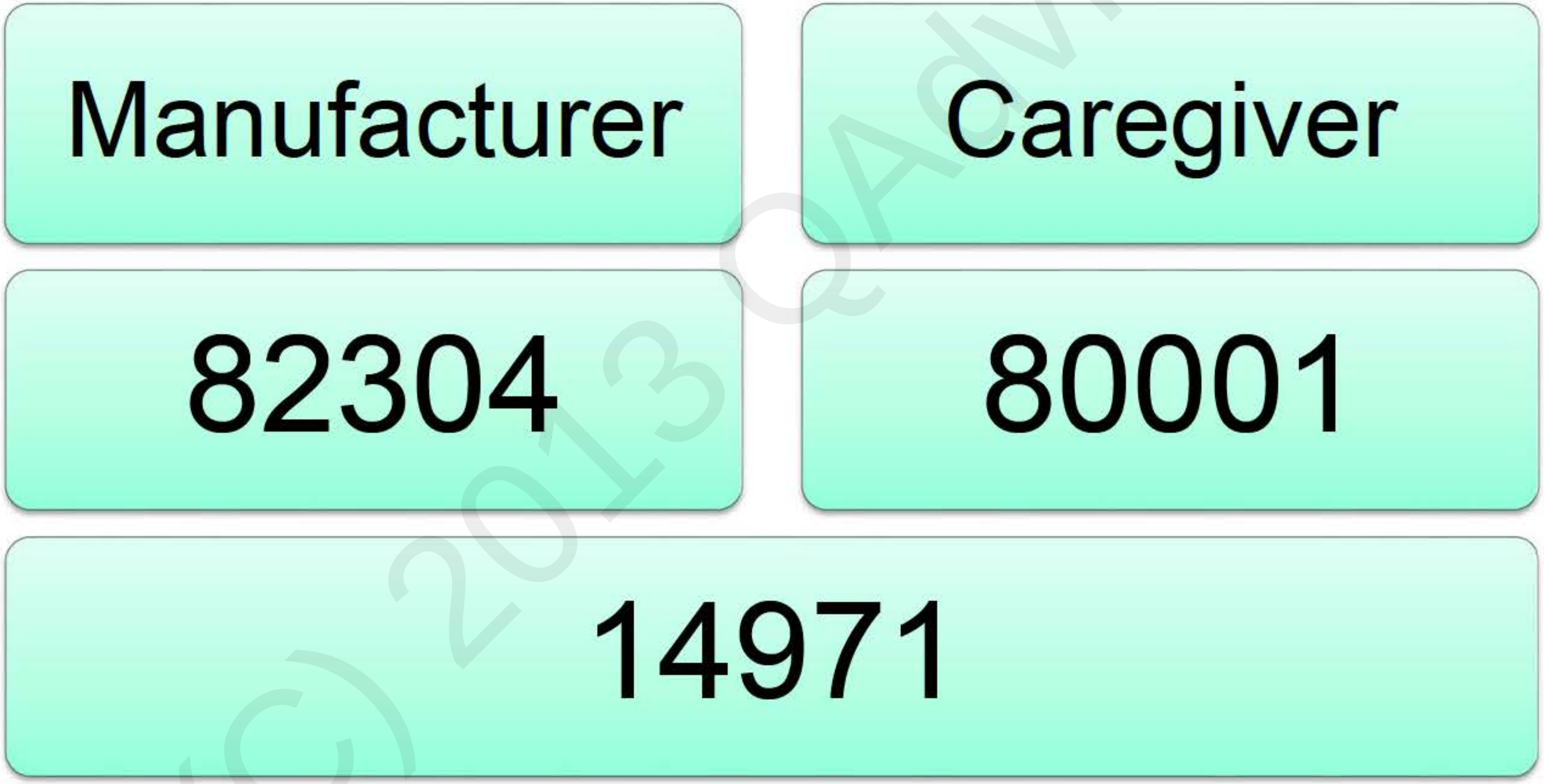
Caregiver

60601-1

80001

14971

The same interface will be valid for stand-alone software



Manufacturer

Caregiver

82304

80001

14971

Example of problems we need to address

The update problem from the **responsible organizations** point of view

If a medical device is connected to a network that has internet access, it may be vulnerable to viruses.

What should the responsible organization do when Microsoft announces an urgent update that applies to a medical device?

The update problem from the **manufacturers** point of view

If a medical device is connected to a network that has internet access, it may be vulnerable to viruses.

What should the manufacturer do when Microsoft announces an urgent update that applies to a medical device?

Proper Risk Management is part of the solution

Draft Part 2-x: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples:

- Risk management of the Update
- Actions based on the outcome
- Change permit
- Cooperation
- Validation by manufacturer

Who needs to do what?

- Manufacturers
- Responsible organizations
- Regulators
- New Roles

Who needs to do What?

- Manufacturers
- Responsible organizations
- Regulators
- New Roles

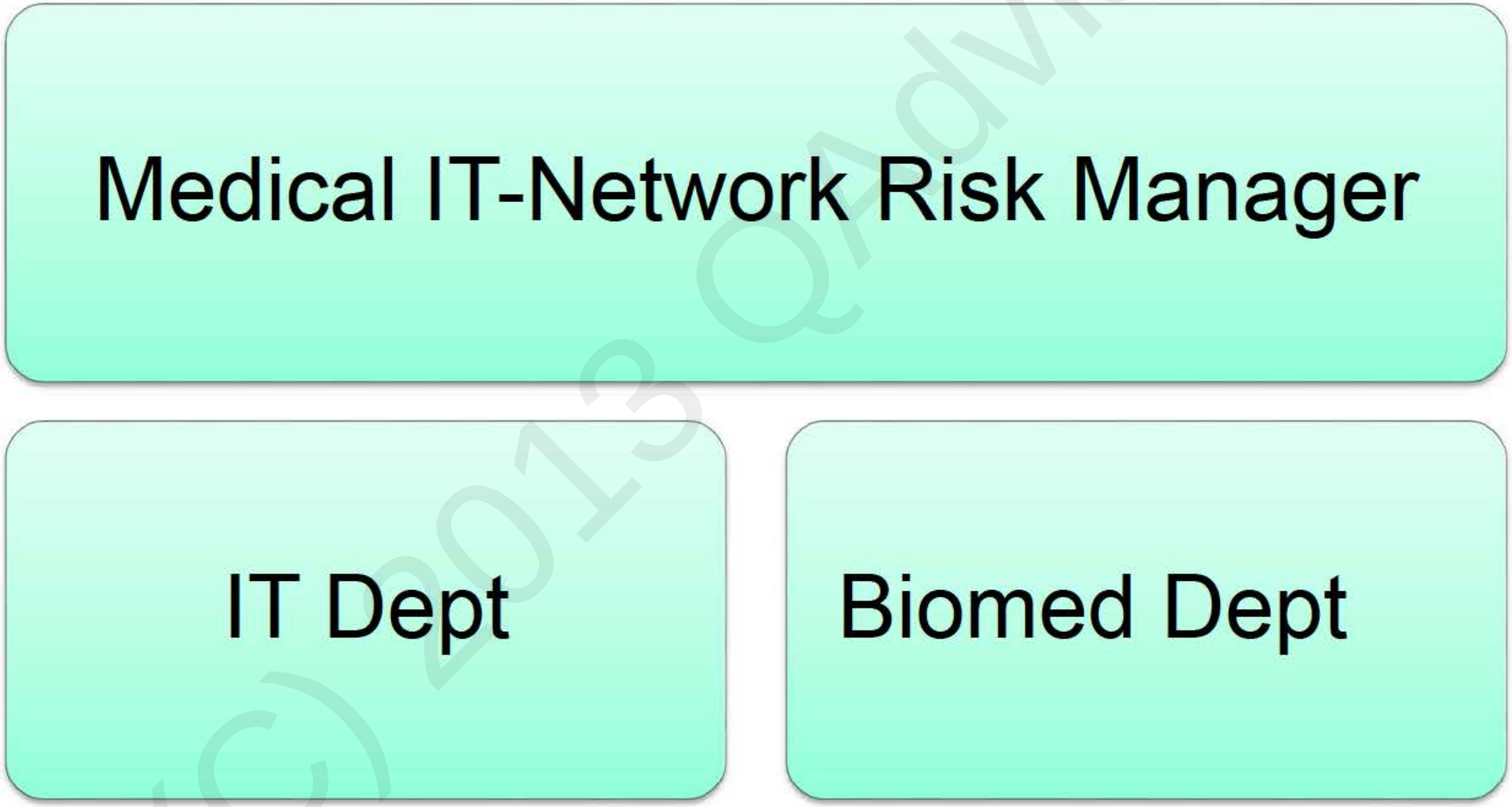
What manufacturers must do

- Design for networking
- State what the network connection is for
- Narrow the scope
- Inform about risks

Who needs to do What?

- Manufacturers
- Responsible organizations
- Regulators
- New Roles

A new role has to be shaped out



Medical IT-Network Risk Manager

IT Dept

Biomed Dept

Who needs to do What?

- Manufacturers
- Responsible organizations
- Regulators
- New Roles

What the Regulator must do

IEC 80001-1 is not, and will probably not be, harmonized with the MDD.

There is no correspondance to CE-marking for care-givers.

So regulators (of healthcare organizations) have to find a way of introducing it.

Socialstyrelsen har lagt en bra grund för IEC/ISO 80001

SOCFS	Innehåll	Aspekt
2005:12, 7§	Ledningssystemet skall säkerställa ... Säker användning och hantering av produkter, försörjningssystem och informationssystem	Effectiveness Safety
2008:14, 3§	Vårdgivaren ska utse ... personer ... riskanalyser som har utförts avseende informationssäkerheten	Data and system security
2008:1, 4§	Vårdgivaren ... egentillverkade medicintekniska produkternas säkerhet ... CE-märkta produkter	Safety

Handbok för patientsäkerhetsarbete beskriver grunder för riskanalyser

Riskanalys & Händelseanalys

Handbok för patientsäkerhetsarbete

ANDRA REVIDERADE UPPLAGAN

Mallar

Definitioner

Arbetsbeskrivningar

Who needs to do What?

- Manufacturers
- Responsible organizations
- Regulators
- New Roles

A new role for the responsible organization is needed

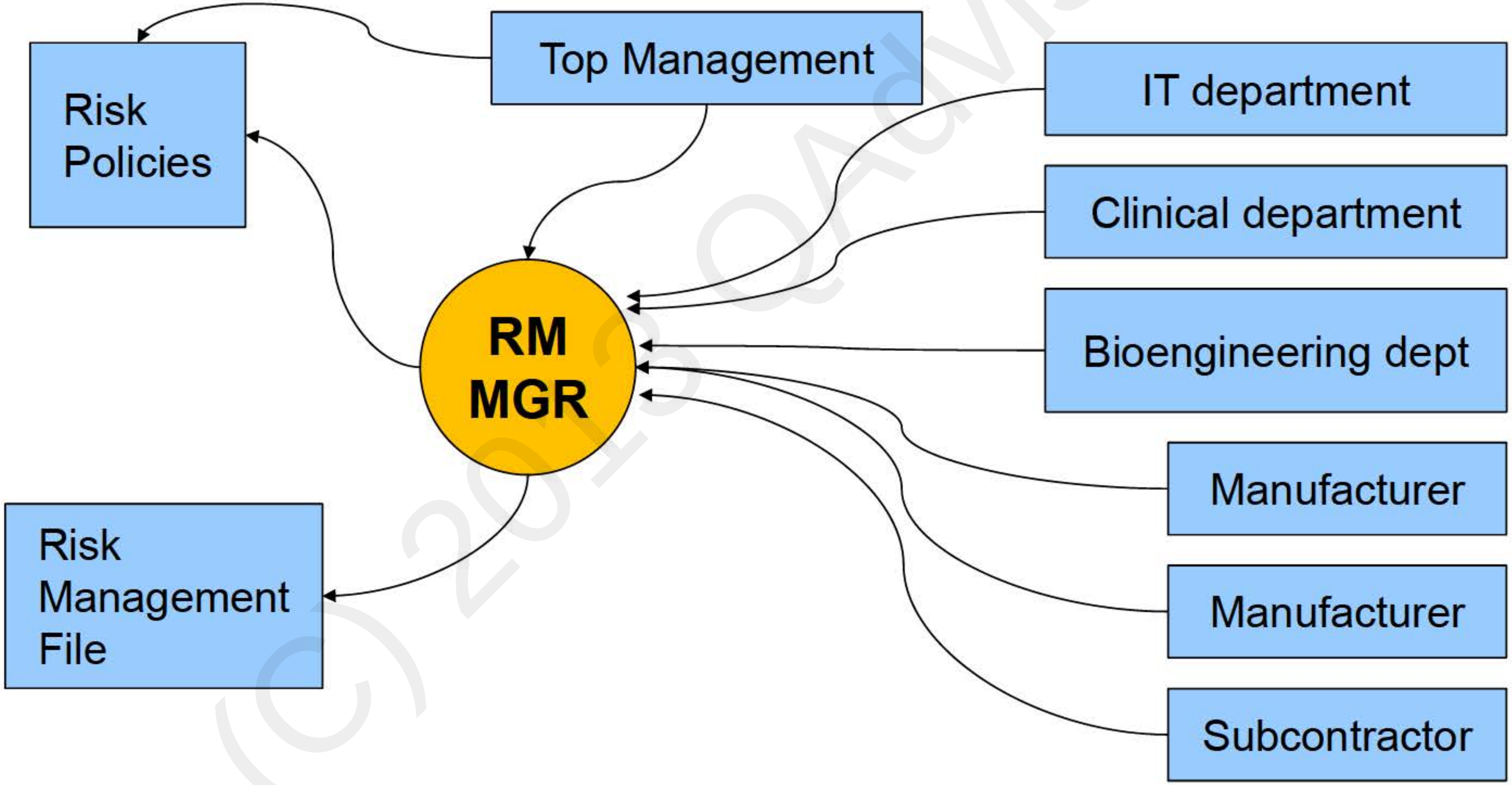
Standard IEC 80001-1 defines:

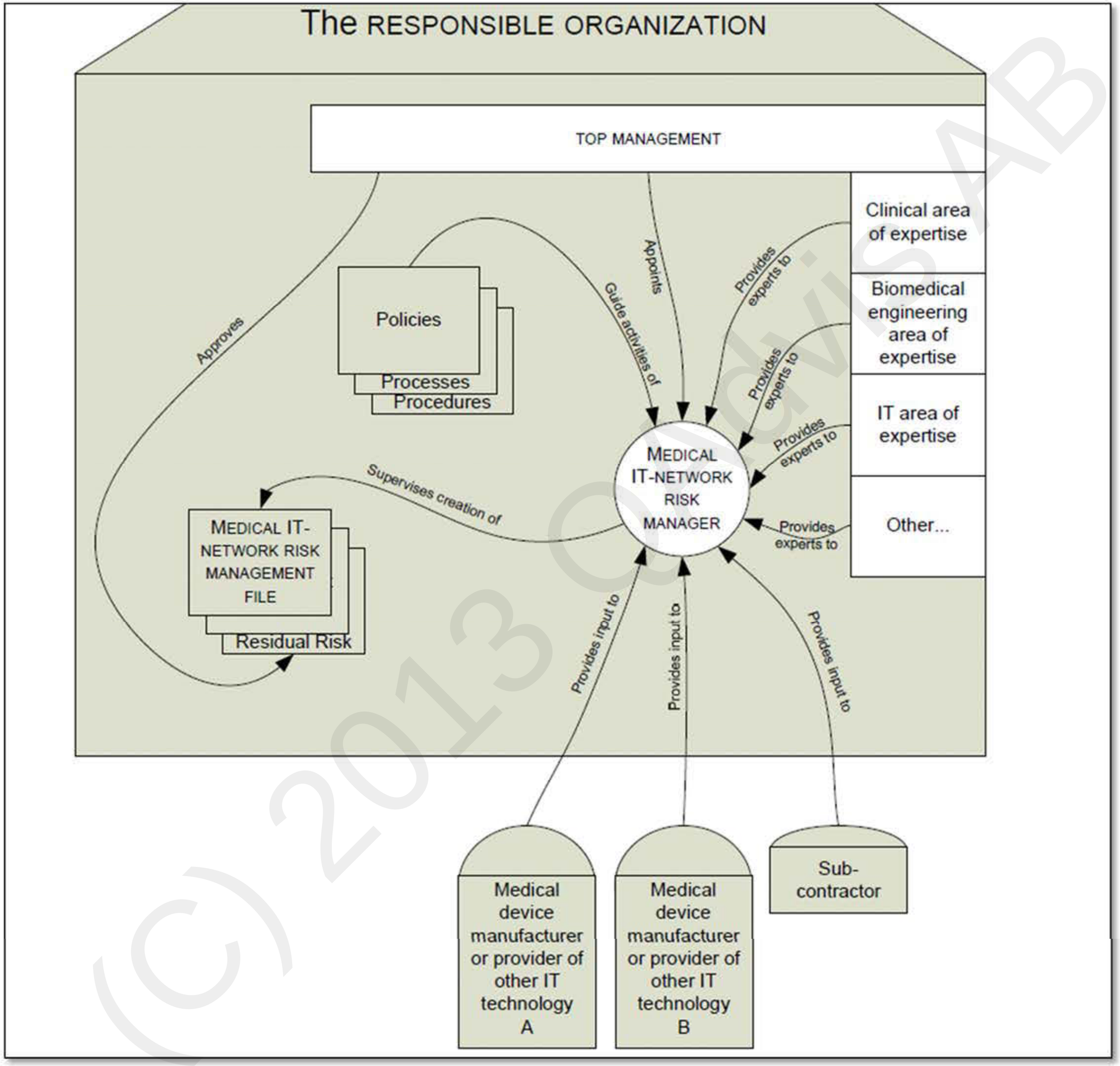
Medical IT-Network Risk Manager

A New Role with lots of responsibilities

- Management of RM process
- Reporting to Top Mgmt
- Communicating
- Collecting information
- Planning changes
- Authorizing changes
- Informing on risks
- Monitoring all IT projects

The role is to be a spider in the web




The RESPONSIBLE ORGANIZATION
TOP MANAGEMENT
Approves
Appoints
Guide activities of
Policies
Processes
Procedures
Clinical area of expertise
Biomedical engineering area of expertise
IT area of expertise
Other...
Provides experts to
Provides experts to
Provides experts to
Provides experts to
MEDICAL IT-NETWORK RISK MANAGER
Supervises creation of
MEDICAL IT-NETWORK RISK MANAGEMENT FILE
Residual Risk
Provides input to
Provides input to
Provides input to
Medical device manufacturer or provider of other IT technology A
Medical device manufacturer or provider of other IT technology B
Sub-contractor

The content of the standard 80001-1

1 Scope

2 Terms and Definitions

3 Roles and Responsibilites

4 Life Cycle RM in medical IT-networks

5 Document control

Higlights in Scope section

1 Scope

2 Terms and Definitions

3 Roles and responsibilites

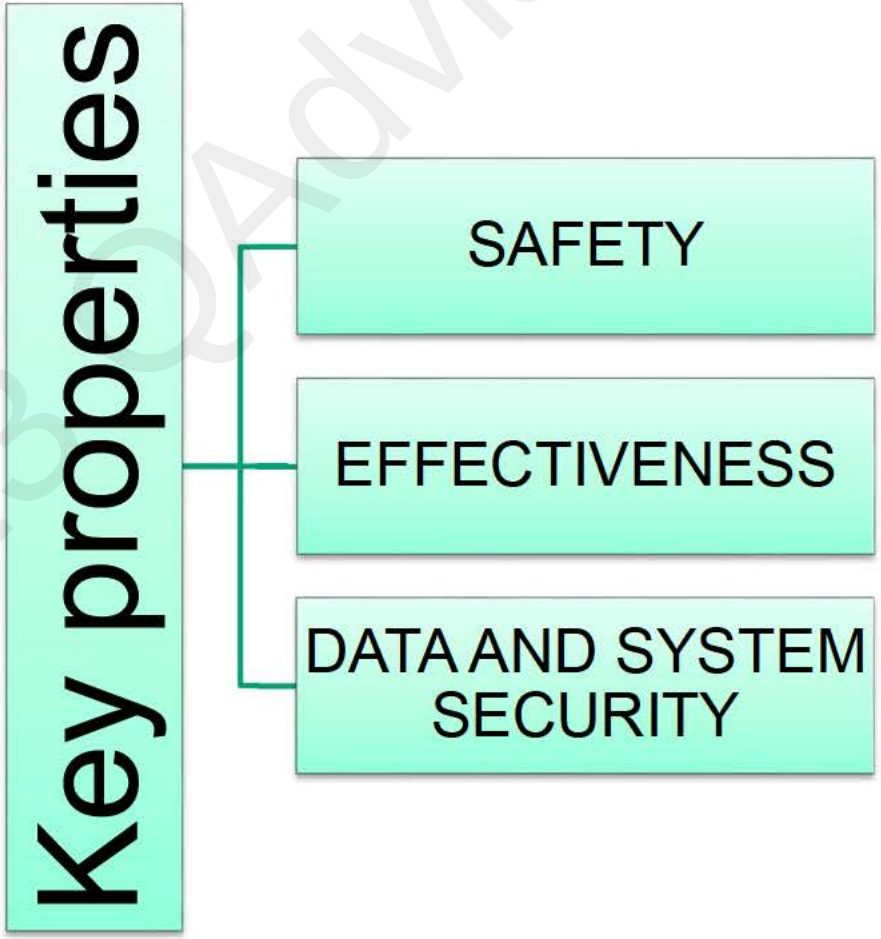
4 Life Cycle RM in medical IT-networks

5 Document control

The responsible organization is the primary target of the standard

- This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.
- To address
  - Safety
  - Effectiveness
  - Data and system security

80001 extends the definition of harm



Key properties

SAFETY

EFFECTIVENESS

DATA AND SYSTEM SECURITY

Higlights in Terms Section

1 Scope

2 Terms and Definitions

3 Roles and responsibilites

4 Life Cycle RM in medical IT-networks

5 Document control

2 Terms and definitions

IT-NETWORK - IT-NÄTVERK

- A system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

KEY PROPERTIES - NYCKELEGENSKAPER

- Three risk managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

2 Terms and definitions

RESPONSIBLE ORGANIZATION - VÅRDGIVARE[HFP]

- Entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

TOP MANAGEMENT - HÖGSTA LEDNINGEN

- Person or group of people who direct(s) and control(s) the RESPONSIBLE ORGANIZATION accountable for a MEDICAL IT-NETWORK at the highest level

2 Terms and definitions

HARM – SKADA [Vårdskada^{HFP}]

- Physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEM SECURITY

RISK - RISK^{HFP}

- Combination of the probability of occurrence of HARM and the severity of that HARM

RISK MANAGEMENT - RISKHANTERING^{HFP}

- Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

RISK MANAGEMENT FILE – RISKHANTERINGSDOKU-MENTATION

- Set of records and other documents that are produced by RISK MANAGEMENT

2 Terms and definitions

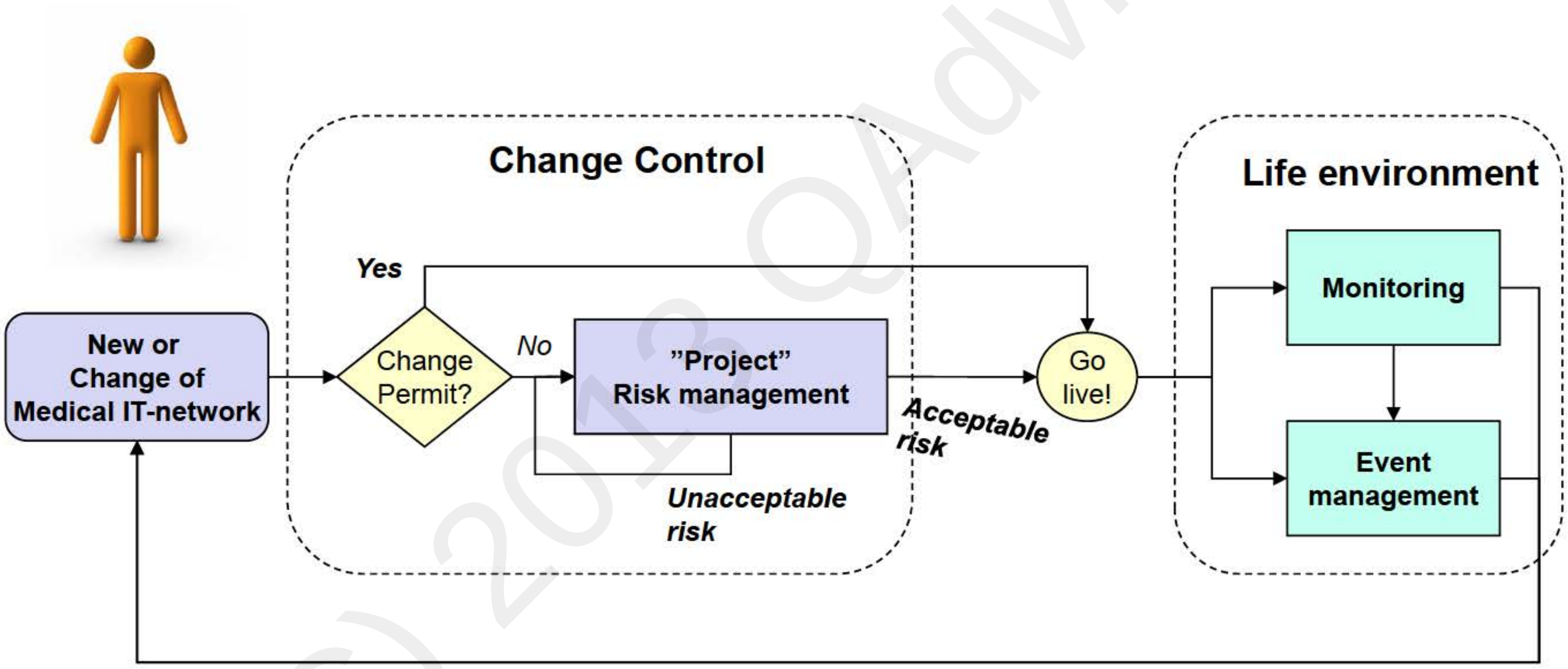
CHANGE PERMIT - Ändringsmedgivande

- An outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT Activities subject to specified constraints

EVENT MANAGEMENT – Händelshantering

- A PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner

IEC/ISO 80001-1 is a process standard



A CHANGE PERMIT can help you to make Risk Management efficient

CHANGE PERMIT:

an outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT Activities subject to specified constraints

A Change Permit is a way of reusing Risk Management work

Patient monitors type XXX may be added to or removed from the High-dependency ward's shielded wireless network subject to the following conditions:

- No more than 15 patient monitors may be connected to the network at any one time.
- An up-to-date record of the wireless devices in use in the ward is to be kept available for inspection at the nursing station.

If these conditions are not met, this permit is void and the full Risk Management process must be used.

Higlights in Roles and responsibilities section

1 Scope

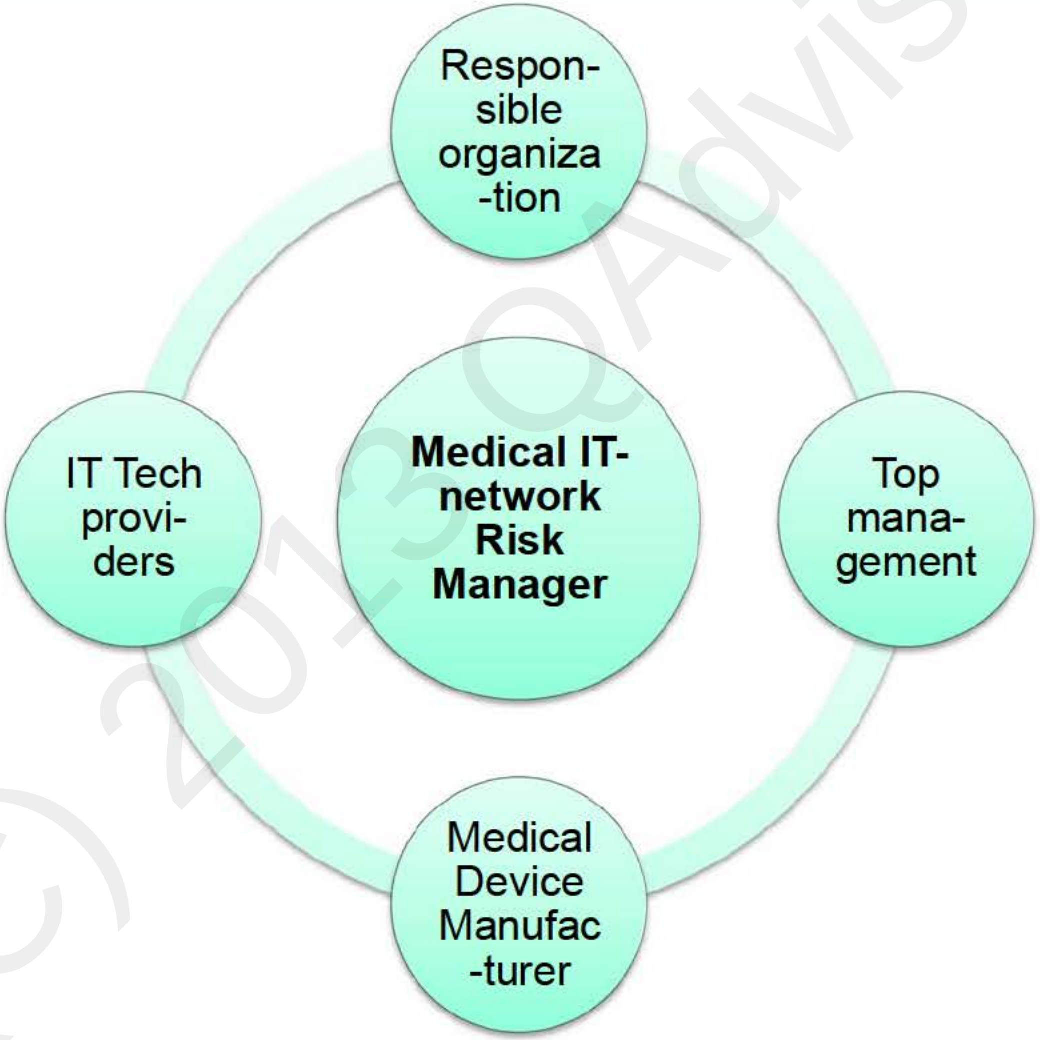
2 Terms and Definitions

3 Roles and responsibilites

4 Life Cycle RM in medical IT-networks

5 Document control

There are several ways of implementing the Risk Manager role


Respon-sible organiza-tion
IT Tech provi-ders
Medical IT-network Risk Manager
Top mana-gement
Medical Device Manufac-turer

Higlights in section on Lifecycle

1 Scope

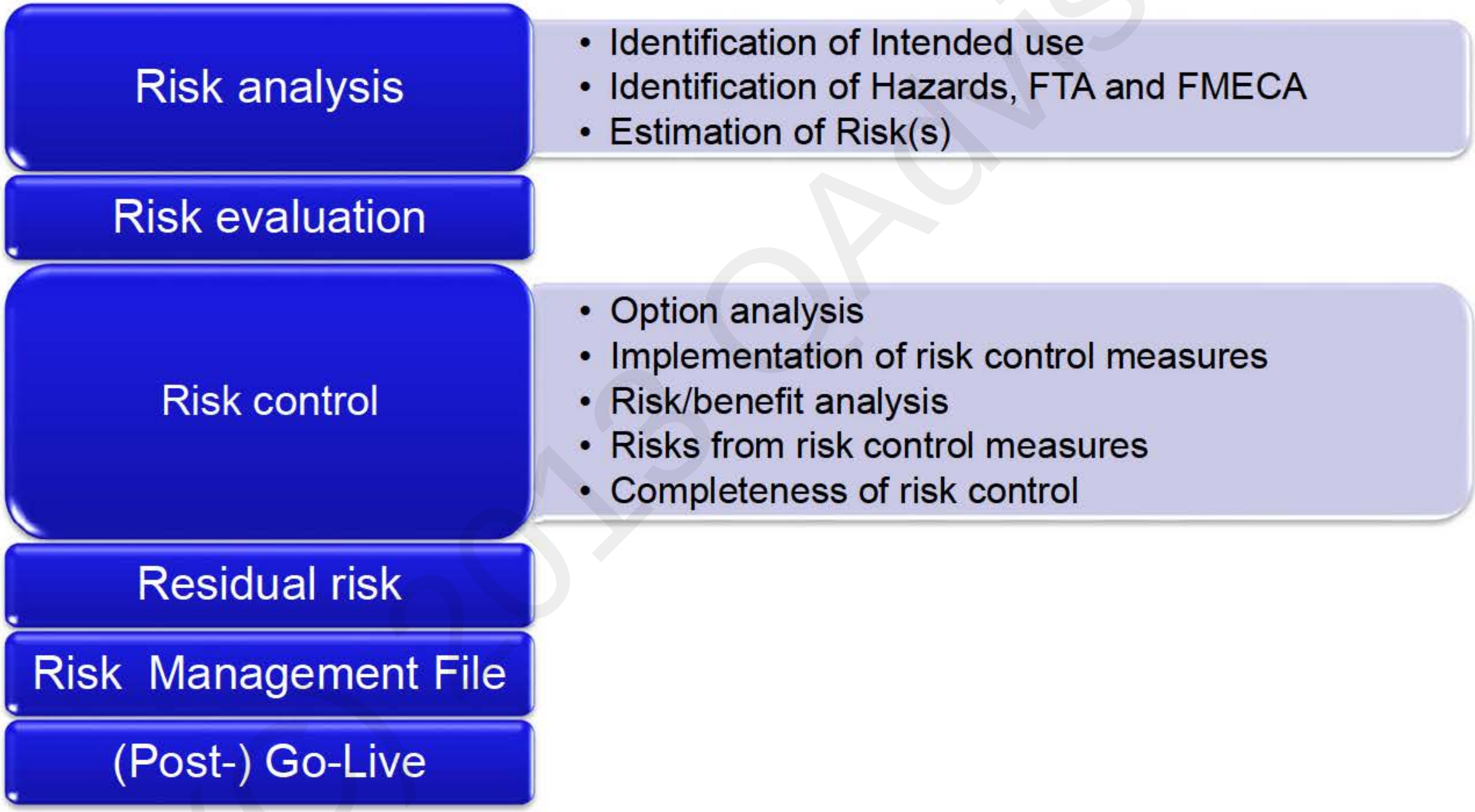
2 Terms and Definitions

3 Roles and responsibilites

4 Life Cycle RM in medical IT-networks

5 Document control

80001 is based on 14971, which is “the” standard for Risk Management



Risk analysis

- Identification of Intended use
- Identification of Hazards, FTA and FMECA
- Estimation of Risk(s)

Risk evaluation

Risk control

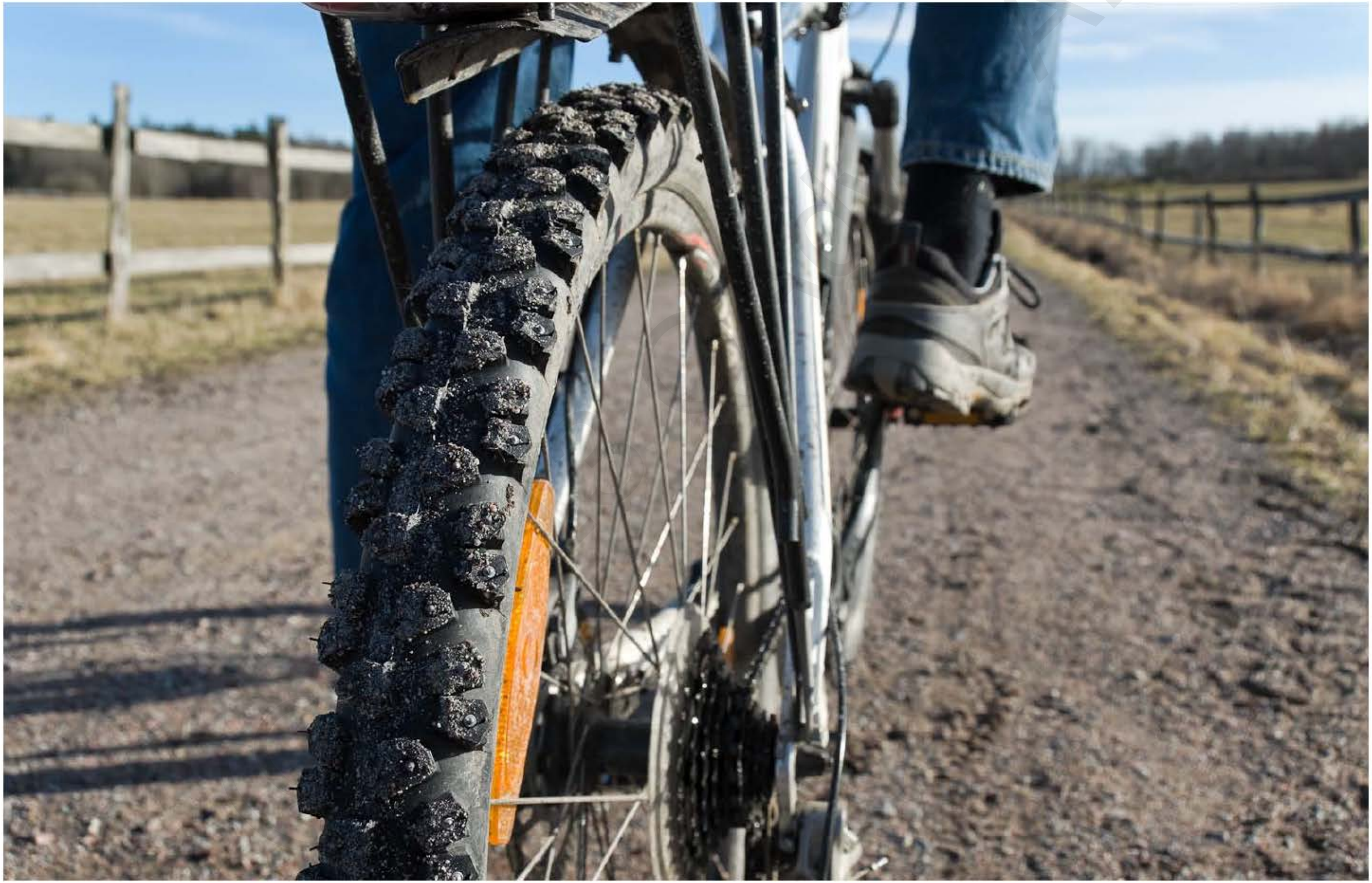
- Option analysis
- Implementation of risk control measures
- Risk/benefit analysis
- Risks from risk control measures
- Completeness of risk control

Residual risk

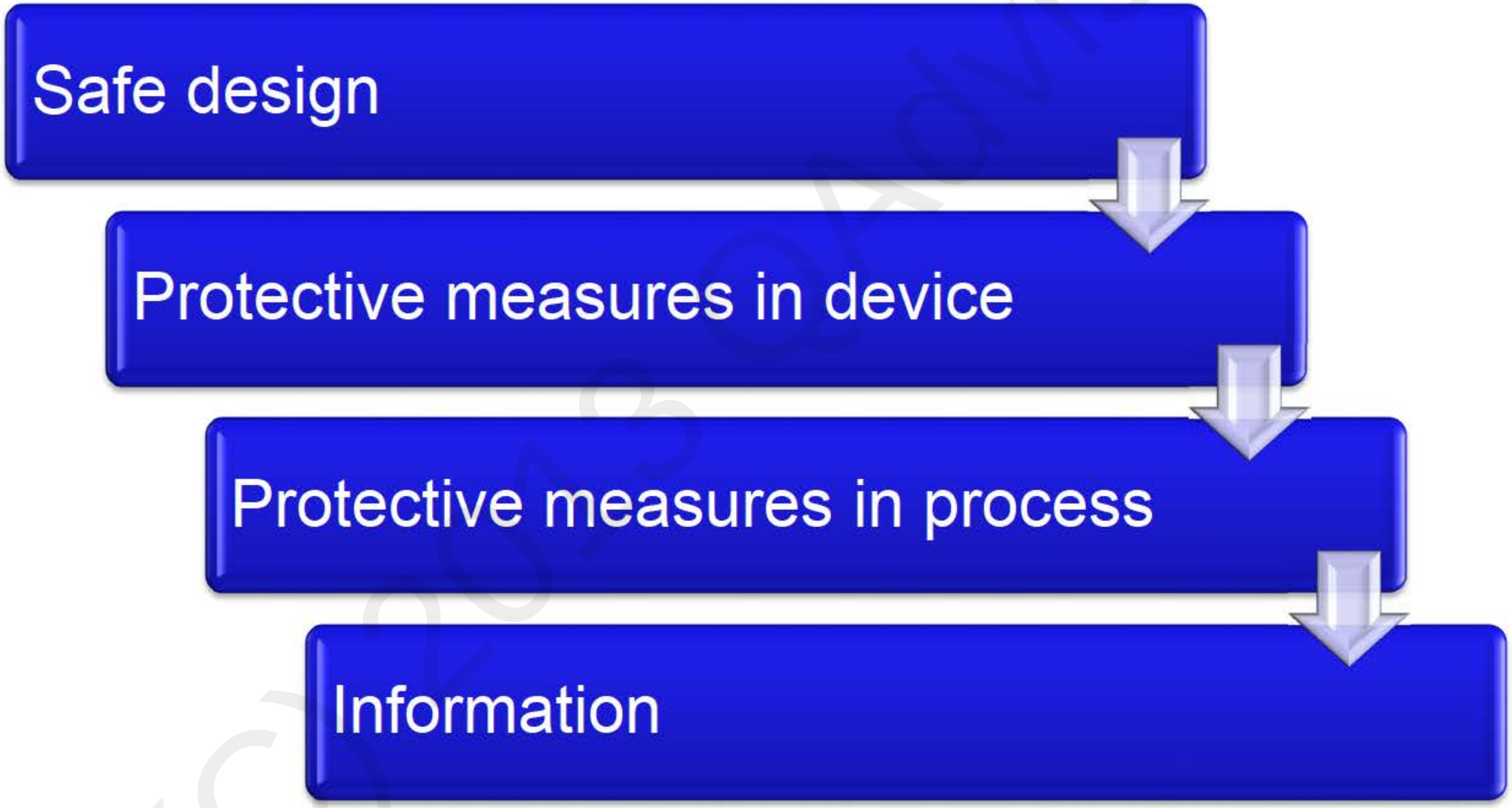
Risk Management File

(Post-) Go-Live

Example: hazard, harm, risk….

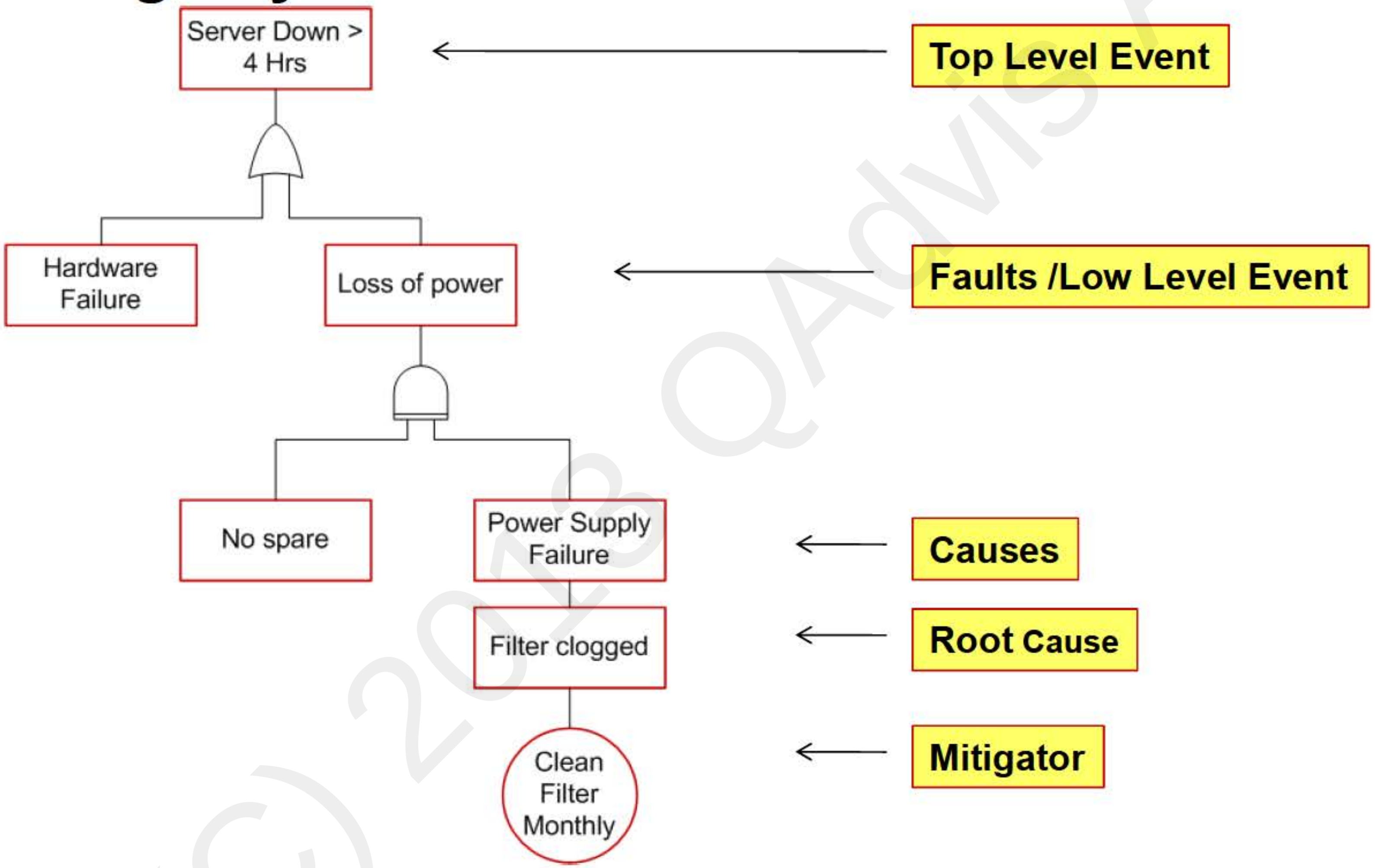


Safe design is the most desired Risk Control Option



Example of a Fault Tree Analysis for:

Image System Down



Top Level Event

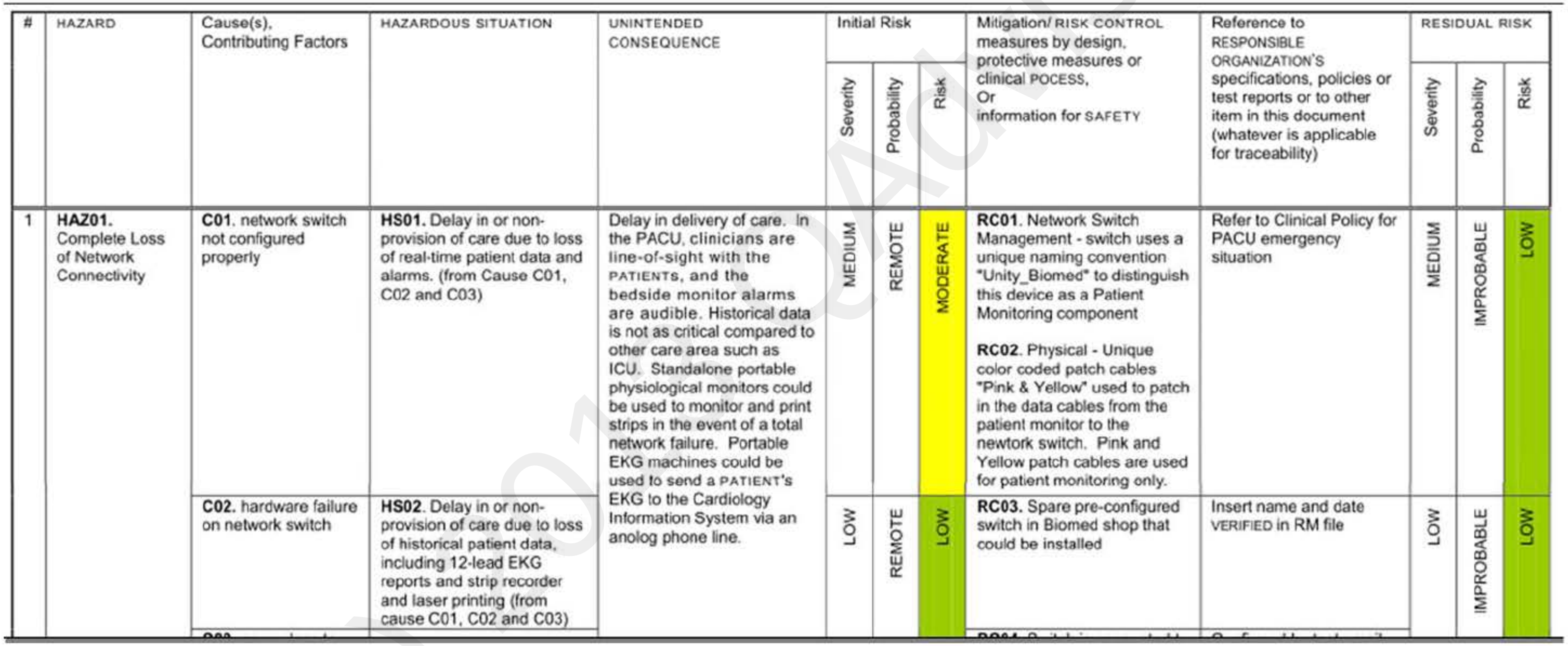
Faults /Low Level Event

Causes

Root Cause

Mitigator

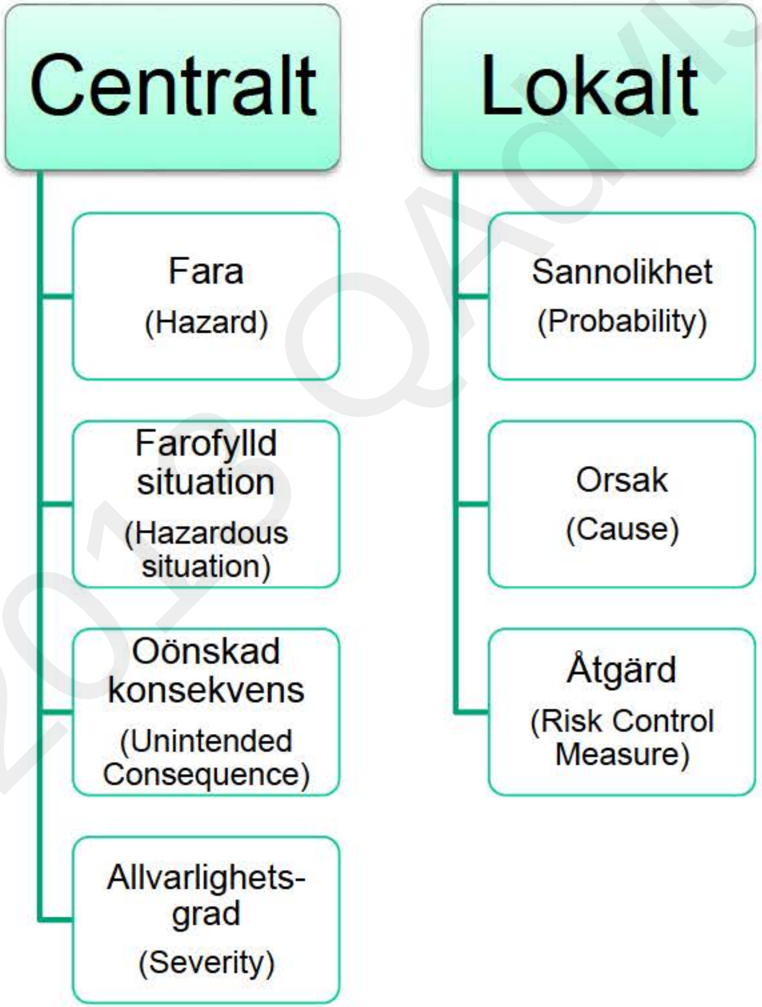
62A_719_NP has hands-on examples on how to do RM



#	HAZARD	Cause(s), Contributing Factors	HAZARDOUS SITUATION	UNINTENDED CONSEQUENCE	Initial Risk			Mitigation/ RISK CONTROL measures by design, protective measures or clinical POCESS, Or information for SAFETY	Reference to RESPONSIBLE ORGANIZATION'S specifications, policies or test reports or to other item in this document (whatever is applicable for traceability)	RESIDUAL RISK		
					Severity	Probability	Risk			Severity	Probability	Risk
1	**HAZ01.** Complete Loss of Network Connectivity	**C01**. network switch not configured properly	**HS01.** Delay in or non-provision of care due to loss of real-time patient data and alarms. (from Cause C01, C02 and C03)	Delay in delivery of care. In the PACU, clinicians are line-of-sight with the PATIENTS, and the bedside monitor alarms are audible. Historical data is not as critical compared to other care area such as ICU. Standalone portable physiological monitors could be used to monitor and print strips in the event of a total network failure. Portable EKG machines could be used to send a PATIENT's EKG to the Cardiology Information System via an anolog phone line.	MEDIUM	REMOTE	MODERATE	**RC01**. Network Switch Management - switch uses a unique naming convention "Unity_Biomed" to distinguish this device as a Patient Monitoring component **RC02**. Physical - Unique color coded patch cables "Pink & Yellow" used to patch in the data cables from the patient monitor to the newtork switch. Pink and Yellow patch cables are used for patient monitoring only.	Refer to Clinical Policy for PACU emergency situation	MEDIUM	IMPROBABLE	LOW
		C02. hardware failure on network switch	**HS02**. Delay in or non-provision of care due to loss of historical patient data, including 12-lead EKG reports and strip recorder and laser printing (from cause C01, C02 and C03)		LOW	REMOTE	LOW	**RC03.** Spare pre-configured switch in Biomed shop that could be installed	Insert name and date VERIFIED in RM file	LOW	IMPROBABLE	LOW

Sample Summary RISK ASSESSMENT Register

Effektiv upplägg har optimal balans Centralt - lokalt



Centralt

Fara (Hazard)

Farofylld situation (Hazardous situation)

Oönskad konsekvens (Unintended Consequence)

Allvarlighets-grad (Severity)

Lokalt

Sannolikhet (Probability)

Orsak (Cause)

Åtgärd (Risk Control Measure)

Higlights in Document Control section

1 Scope

2 Terms and Definitions

3 Roles and responsibilites

4 Life Cycle RM in medical IT-networks

5 Document control

The Medical IT-Network Risk Management File is the key document

Trace each identified Hazard to:

- Risk Analysis
- Risk Evaluation
- Implementation and Verification of the Risk Control Measures
- The assessment of the acceptability of any Residual Risk(s) with approval

There are three new work items on their way to clarify 80001

Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples

- Risk management hands-on

Guidance for the communication of medical device security needs, risks and controls

- IT Technology for security

Guidance for wireless network

- Hands-on networking

Summary

Care givers are facing a challenge

This will propagate to manufacturers

Manufacturers of stand-alone SW might have a large hurdle to pass

Building a solid Risk Management process can enable productivity

- ✓Synergus can contribute with
- ✓Auditing and reviews
- ✓Mentoring and training
- ✓Risk manager role
- ✓Risk management workshops
- ✓Process development and documentation
- ✓Risk management documentation

Q&A