The importance of STANDARDS to ensure ACCOUNTABILITY and GOVERNANCE in eHealth-ICT security processes

New targets for cyberattacks
New challenges for cybersecurity

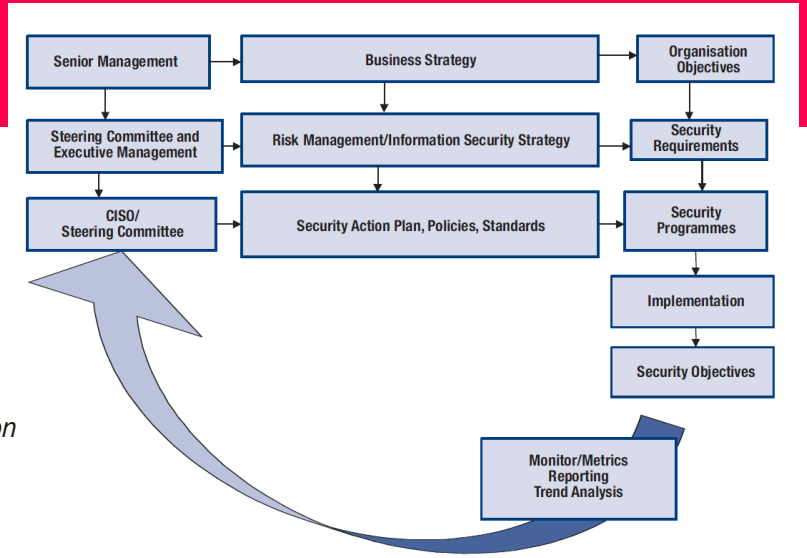
- not only money transaction and bank accounts
- personal information are the new target
- increased connectivity and enlarged attack surfaces

- a new approach to information security (security and privacy by design)
- design security of network attached devices
- consider new scenarios (ex: cyberattacks performed through a trusted supplier remotely connected)
- quickly develop awareness, tools and processes to improve the organization security posture

ACCOUNTABILITY E SECURITY GOVERNANCE

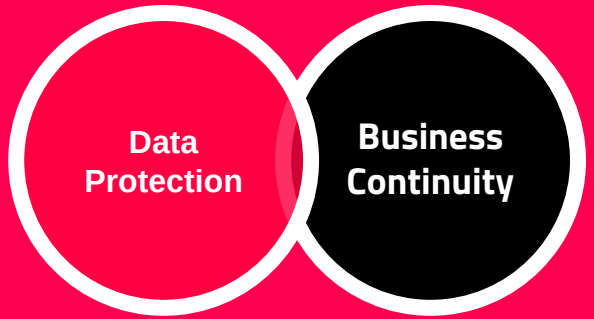
Impact of new laws, regulations (GDPR – NIS)

Governance is the set of responsibilities and practices exercised by the board to provide strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that resources are used responsibly



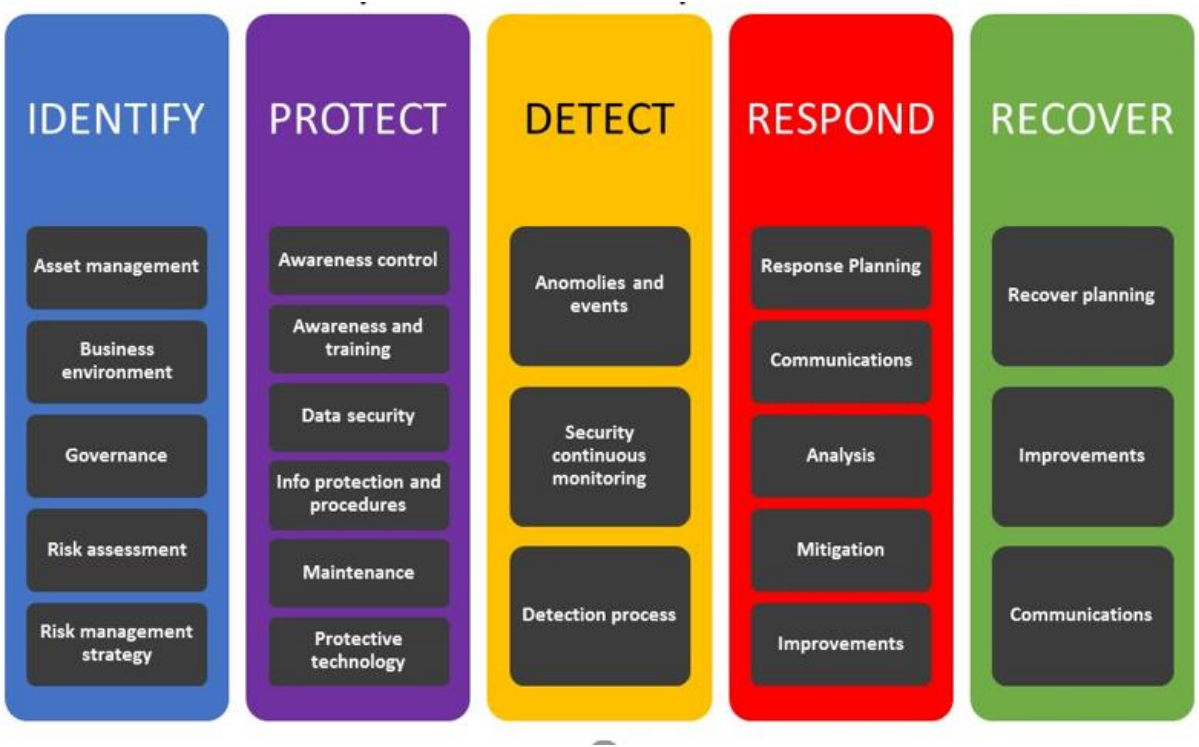
- *Development of security policies*
- *Assignment of roles, responsibilities, authority and accountability*
- *Security control framework (standards, measures, practices and procedures)*
- *Periodic assessments of risks and business impact analyses*
- *Classification and assignment of ownership of information assets*
- *Adequate, effective and tested controls for people, processes and technology*
- *Integration of security into all organisational processes*
- *Monitor security events and information security incident management*
- *Effective identity and access management processes for users and supplier of information*
- *Meaningful monitoring and metrics of security performance*
- *Education and awareness of all users*
- *Information security evaluations (audit) and performance reports*
- *Plan for remedial action to address information security deficiencies*
- *Training in the operation of security processes*
- *Development and testing of plans for continuing the business in case of interruption or disaster*

Standard and best practices GDPR compliance



NIST cybersecurity framework

Framework for Improving Critical Infrastructure Cybersecurity



Risk Management:
Consider cybersecurity risks as a part of overall operational risk management

Protective technologies:
Select appropriate and effective technical controls

Incident mangement and Data Breach Communication:
Develop an incident management procedure and prepare for mandatory external communications

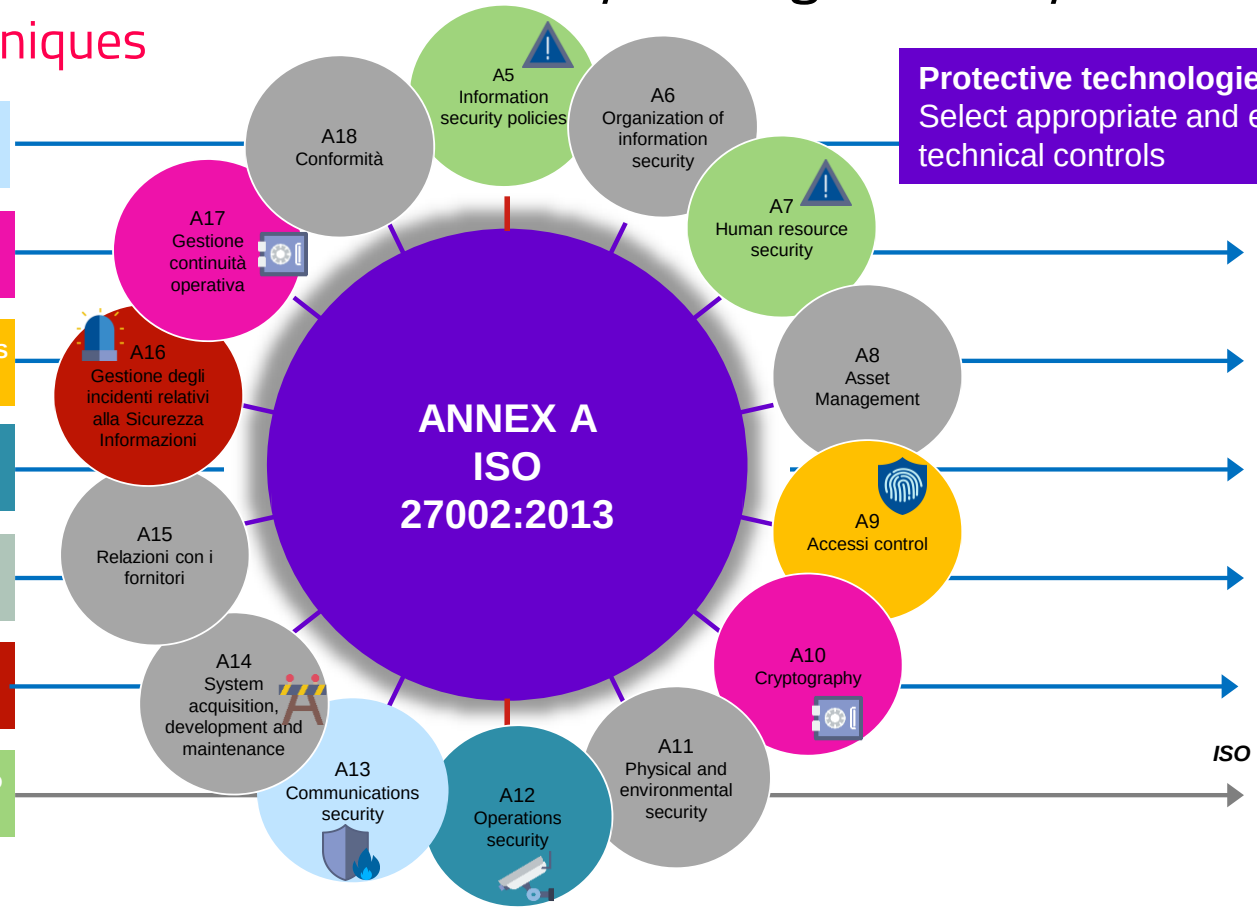
Recover Planning:
Design a recovery strategy
Develop business continuity and Disaster Recovery Plans
Test and exercise the Plans

ISO 27001 - Information security management system

Security techniques

Appropriate technological meaures (GDPR)

- NETWORK AND SYSTEMS SECURITY
- DATA SECURITY & DATA AVAILABILITY
- IDENTITY AND ACCESS MANAGEMENT
- LOGGING AND MONITORING
- DATA PROTECTION BY DESIGN
- DATA BREACH NOTIFICATION
- ORGANIZATION AND HUMAN SECURITY



Protective technologies:
Select appropriate and effective technical controls

ISO 27002 controls

nist.sp.800-61r2

Incident Handling guide

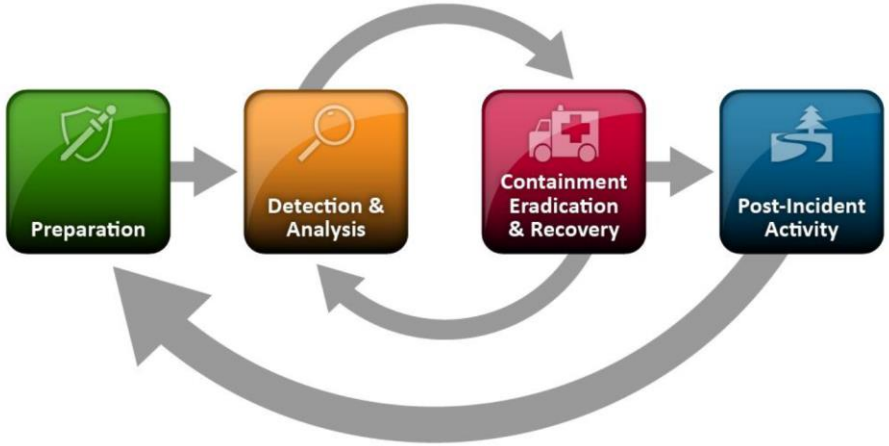
Incident mangement and Data Breach Communication:
Develop an incident management procedure and prepare for mandatory external communications

Preparation:
- Preventing Incidents

Detection and Analysis:
- Signs of an Incident
- Incident Analysis
- Incident Documentation
- Incident Prioritization
- Incident Notification-> DATA BREACH

Containment, Eradication, and Recovery:
- Choosing a Containment Strategy
- Evidence Gathering and Handling
- Eradication and Recovery

Post-Incident Activity:
- Lessons Learned



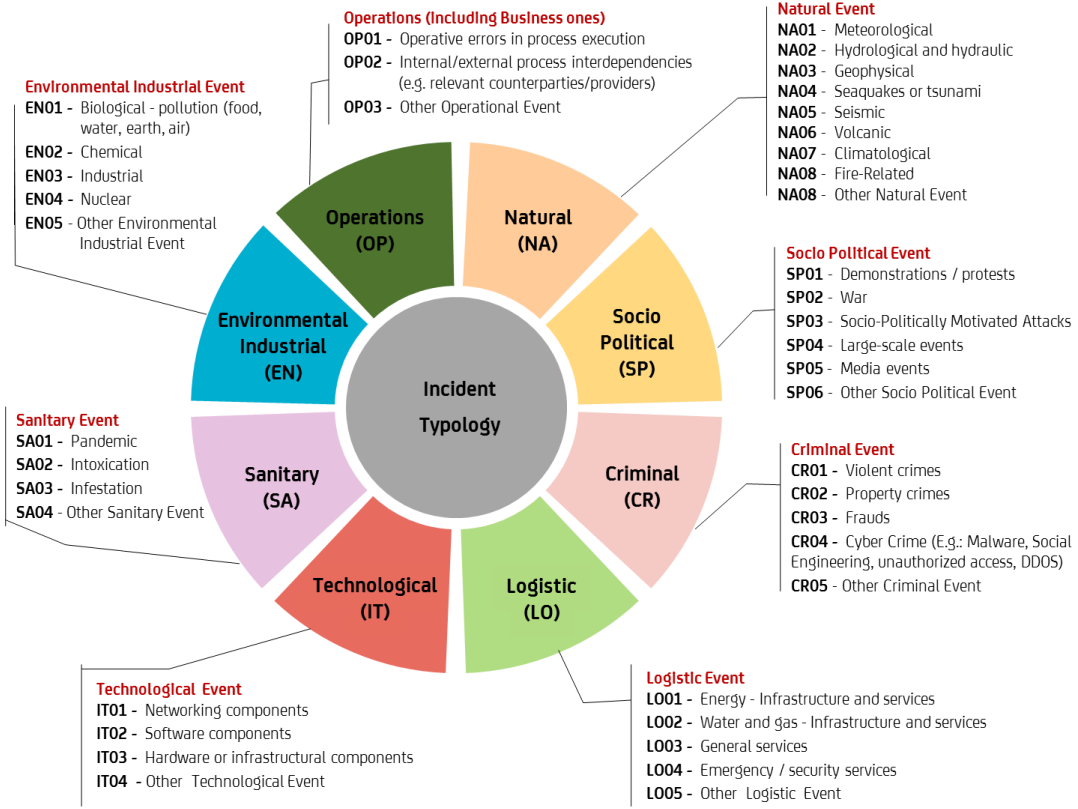
ISO 22301

Business Continuity Management

Business continuity is about having a plan to deal with difficult situations.

Processes and procedures must be implemented to ensure that mission-critical functions can continue during and after a disaster with as little disruption as possible

Recover Planning:
Design a recovery strategy
Develop business continuity and Disaster Recovery Plans
Test and exercise the Plans



Business Continuity Management process in 4 steps

1

Identifies the appropriate **Managerial level** to be engaged

2

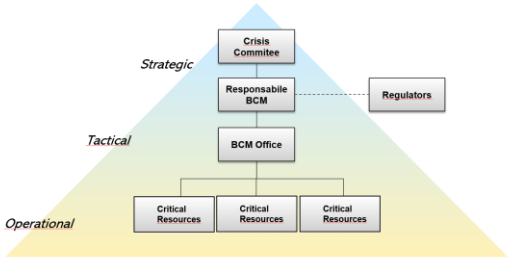
Conduct a **Business Impact Analysis**

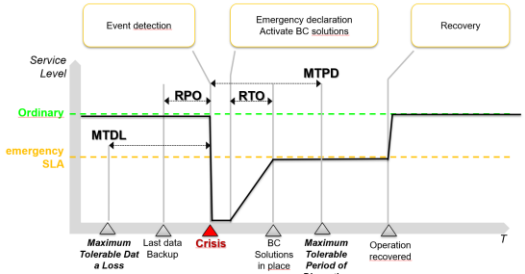
3

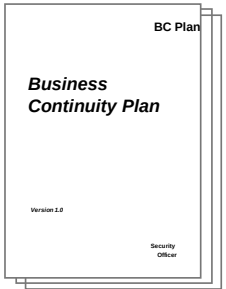
Prepare **BC emergency Plan** and **Disaster Recovery Plan**

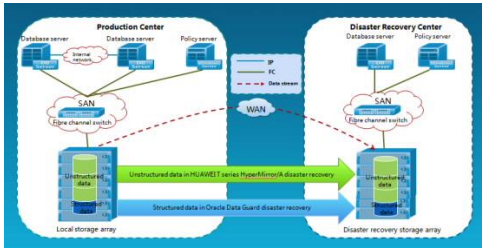
4

Test the Plan









To face new scenarios..

Remote maintenance on critical systems is provided by third parties

Obsolete and unpatched systems are connected to the network

IoT devices sends sensitive data in the cloud...

.. a new level of awareness is required

Thanks!

Any questions?

You can find me at
barbara.ceretti@gmail.com