EUROPEAN UNION AGENCY
FOR CYBERSECURITY

THE "SECURE BY PROCUREMENT" PERSPECTIVE IN HEALTHCARE CYBERSECURITY

Dr. Athanasios Drougkas
Cybersecurity Expert

PANACEA Research 3rd End-User Workshop

04 | 05 | 2021

ENISA GUIDELINES FOR PROCUREMENT IN HEALTHCARE

February 2020

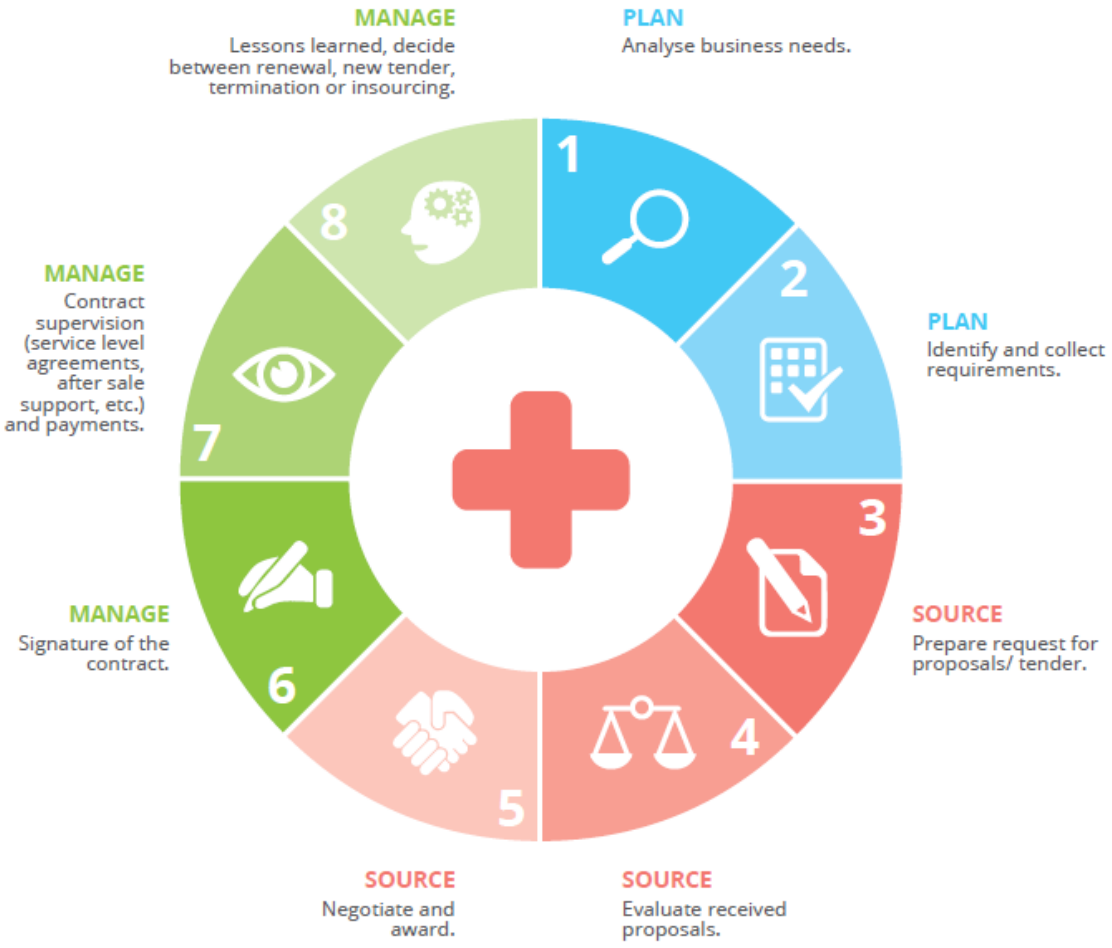
January 2021

April 2021

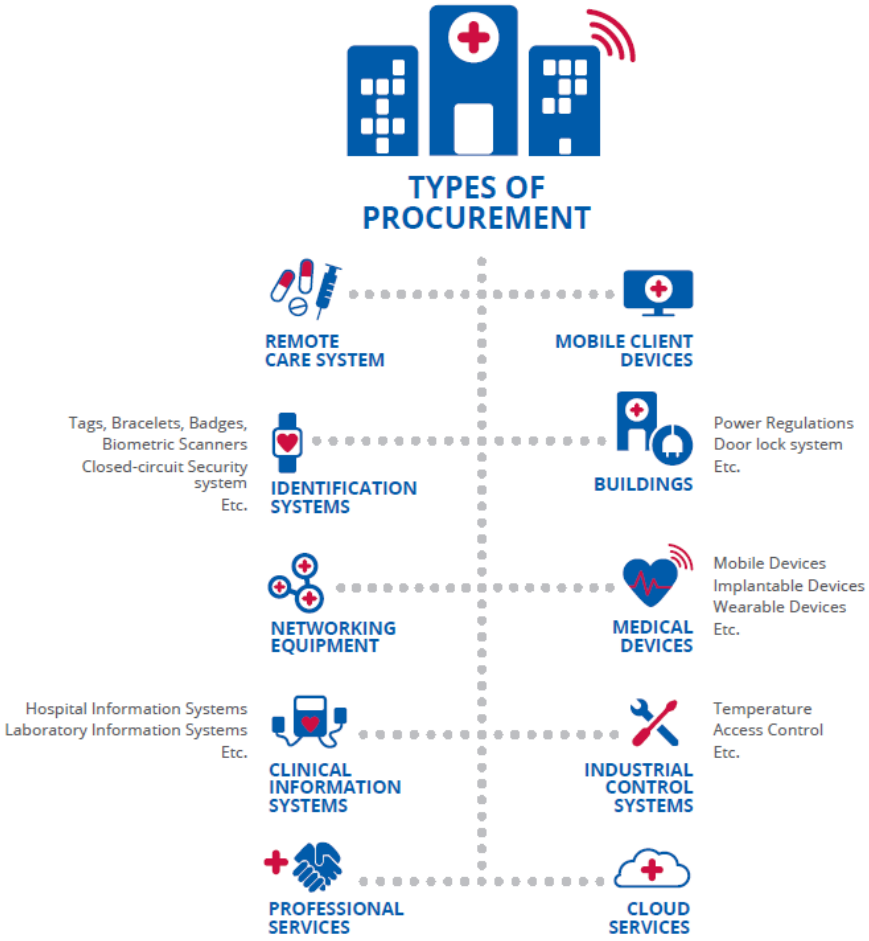
Online Tool

Translations in all EU languages

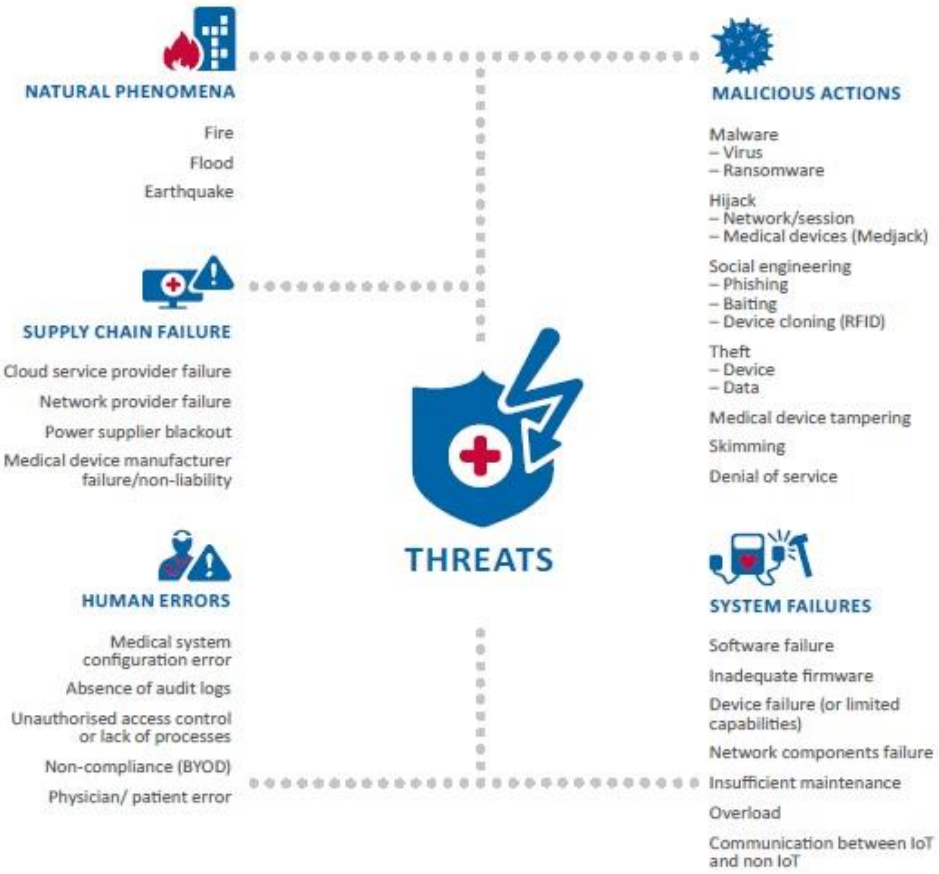
CYCLE OF PROCUREMENT



TYPES OF PROCUREMENT



THREAT TAXONOMY



GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

Organisational Practices

- Involve the IT department in procurement
- Asset inventory / configuration management
- Vulnerability identification and management
- Develop incident response plans
- Risk assessment as part of procurement
- Establish testing policies
- Threat identification for products/services
- Establish Business Continuity plans
- DPIA for new products/services
- Establish eligibility criteria for suppliers
- Raise cybersecurity awareness among staff
- Policy for hardware and software updates
- Provide training to staff / external consultants
- Plan network, HW and license requirements

GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

Technical Practices

Require cybersecurity certification	Allow auditing and logging
Determine network requirements	Schedule / monitor maintenance operations
Segregate your network	Involve supplier in incident management
Keep legacy systems/machines connected	Penetration testing frequently or after change
Take into account interoperability issues	Dedicated RFP for procuring Cloud Services
Access control for medical device facilities	Minimise / control remote access
Security controls for wireless communication	Encrypt sensitive data at rest / in transit
Enable testing of all components	Require patching for all components

PROCUREMENT GUIDELINES - RECOMMENDATIONS

- New **regulations, policies and standards** are setting the framework
- **Procurement goes beyond the RfP** when it comes to cybersecurity
- **Staff awareness/training** is key
- Cybersecurity is a consideration for the entire **lifecycle**
- Suppliers should be involved in **post-procurement** stages (e.g. incident response, patching, vulnerability disclosure)

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu