Ai4HealthSec

2nd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop

29 April 2022

Standards and NIS compliance

CHATZOPOULOU Argyro

TÜV TRUST IT GmbH

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

AI4HealthSec H2020 Project

A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures* *(AI4HealthSec)

- **Call:** H2020-SU-DS-2019 (Digital Security)
- **Topic:** SU-DS05-2018-2019
- **Type of Action**: RIA
- **Project duration:** 36 Months
  - Started: 1/10/2020
  - End: 30/09/2023
- **Proposal overall cost:** 4,998,948.75 €
- **Project Coordinator:** CNR
- **Website**: https://www.ai4healthsec.eu/

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

The AI4HealthSec project

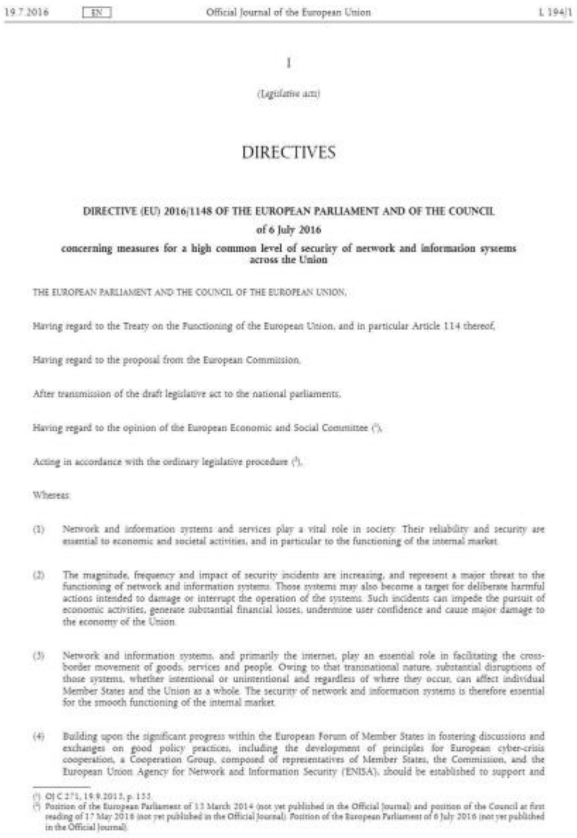
AI4HEALTHSEC proposes a state of the art solution that improves the detection and analysis of cyber-attacks and threats on HCIIs, and increases the knowledge on the current cyber security and privacy risks.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme, under Grant Agreement 883273

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

The NIS (1)

As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive. The NIS Directive (EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or 'transposes' the directive.



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA), should be established to support and

[1] OJ C 271, 19.9.2013, p. 133.
[2] Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 17 May 2016 (not yet published in the Official Journal). Position of the European Parliament of 6 July 2016 (not yet published in the Official Journal).

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

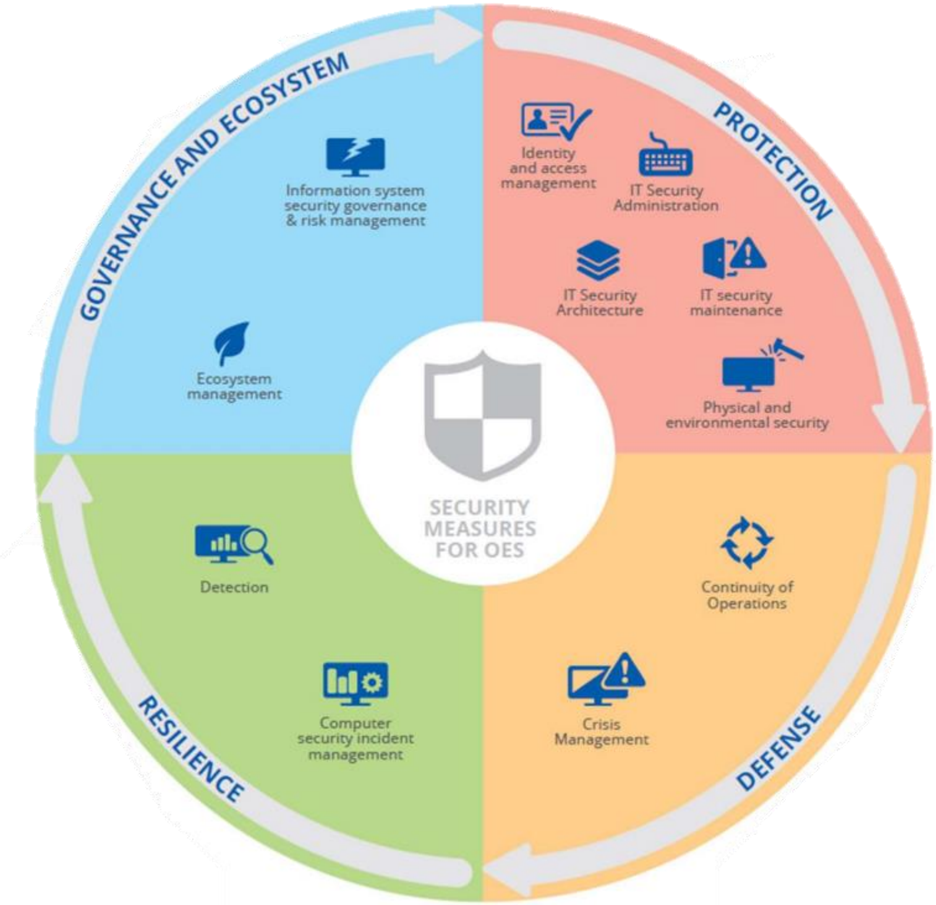
The NIS Cooperation Group

The Group's overall mission is to achieve a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. It facilitates strategic cooperation between the Member States regarding the security of network and information systems.

⇨Reference document on security measures for Operators of Essential Services, CG Publication 01/2018

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

Security Measures for OES*


GOVERNANCE AND ECOSYSTEM
Information system security governance & risk management
Ecosystem management
PROTECTION
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
SECURITY MEASURES FOR OES
DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Detection
Computer security incident management

*Operators of Essential Services

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

European Commission

ROLLING PLAN FOR ICT STANDARDISATION

2021

2022

(B.) REQUESTED ACTIONS

Action 1 *SDOs to develop standards for critical infrastructure protection and thus in support of and responding to the requirements laid down in the NIS Directive. Foster the application of EN 62443 series (base on IEC 62443 series) for the firm establishment of EU regulatory requirement operational technology (OT) security including critical infrastructures.”*

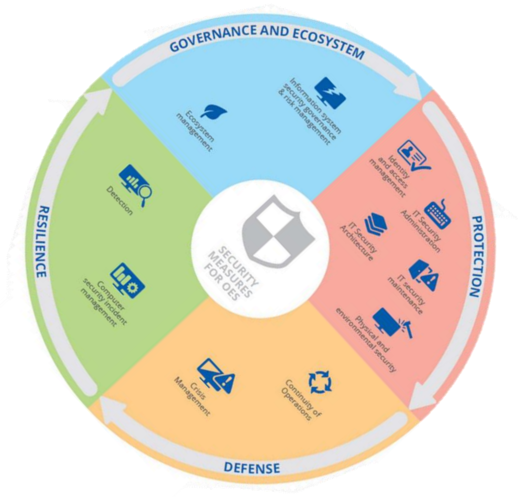
Action 5 *SDOs to investigate the availability of standards as regards to the security and incident notification requirements for digital service providers as defined in the NIS Directive and in support of possible other pieces of EU law.*

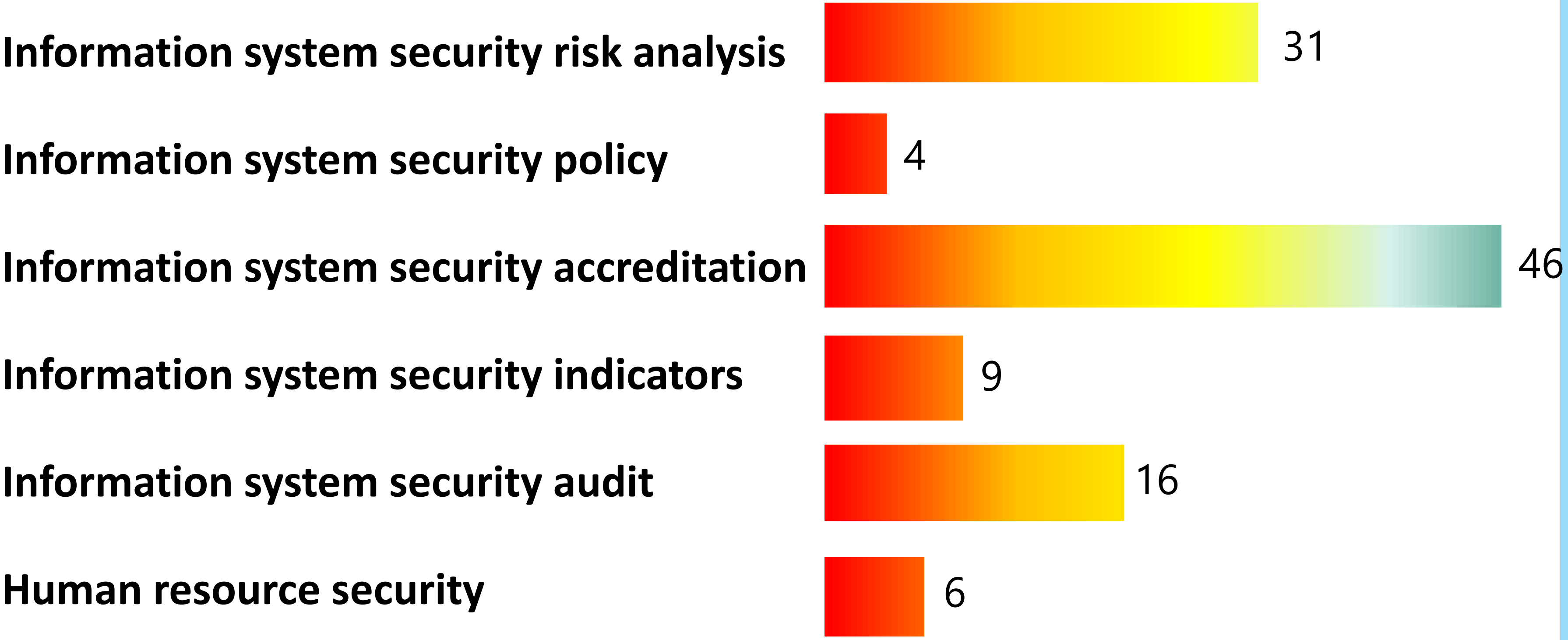
Action 6 *SDOs to develop a “guided” version of ISO/IEC 270xx series (information security management systems including specific activity domains) specifically addressed to SMEs, possibly coordinating with ISO/IEC JTC1 SC27/WG1 to extend the existing guidance laid out in ISO/IEC 27003. This guidance should be 100% compatible with ISO/IEC 270xx and help SMEs to practically apply it, including in scarce resource and competence scenarios.*

The work described in this document has been conducted within the project AI4HEALTH ion’s Horizon 2020
research and innovation programme under grant ag

GOVERNANCE AND ECOSYSTEM

Information System Security Governance & Risk Management

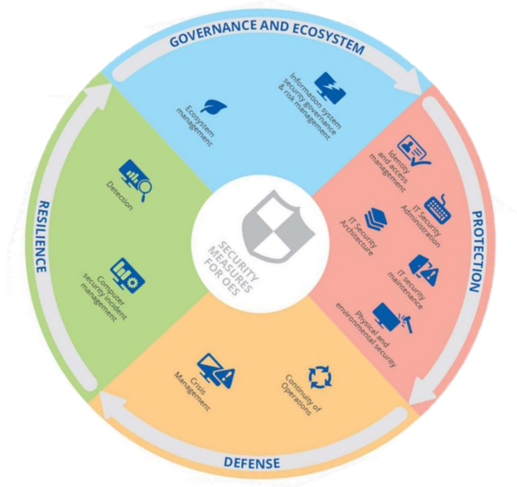

GOVERNANCE AND ECOSYSTEM
Ecosystem management
Information system security governance & risk management
PROTECTION
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
DEFENSE
Crisis Management
Continuity of Operations
RESILIENCE
Detection
Computer security incident management
SECURITY MEASURES FOR OES

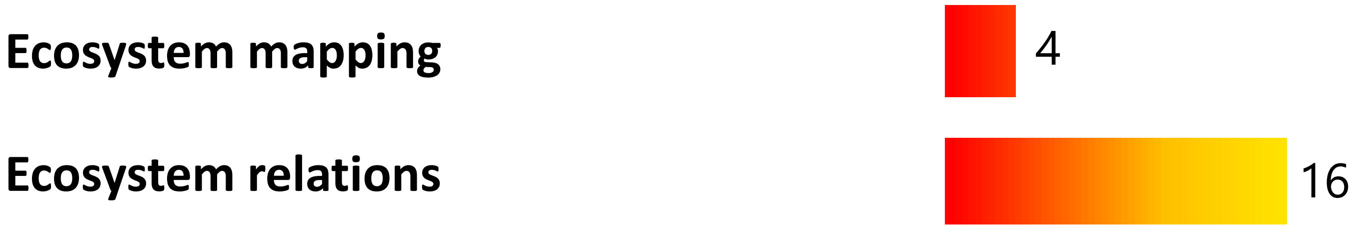


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

GOVERNANCE AND ECOSYSTEM

Ecosystem management

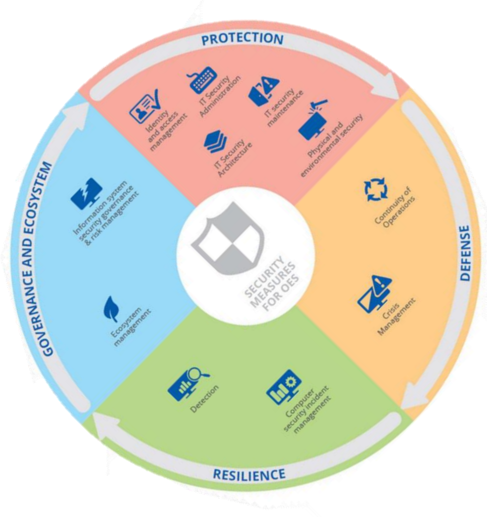

GOVERNANCE AND ECOSYSTEM
Ecosystem management
Information system security governance & risk management
PROTECTION
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Computer security incident management
Detection
SECURITY MEASURES FOR OES

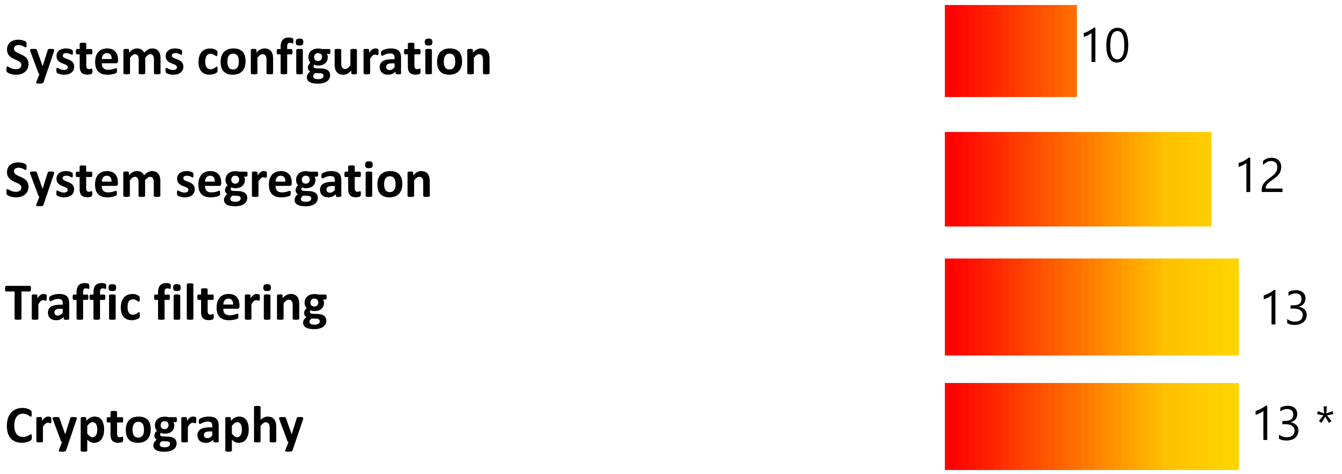


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

PROTECTION

IT Security Architecture

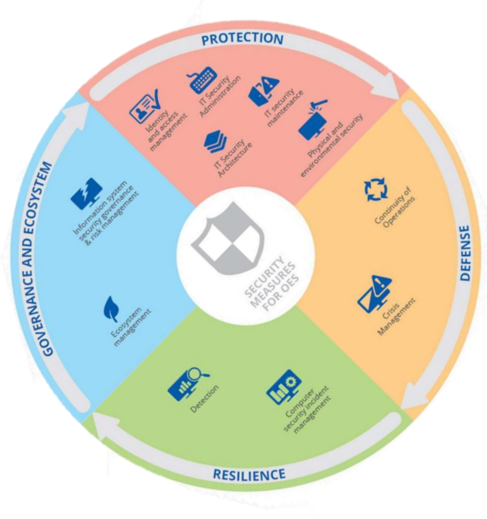

PROTECTION
DEFENSE
RESILIENCE
GOVERNANCE AND ECOSYSTEM
Identity and access management
IT Security Administration
IT security maintenance
IT Security Architecture
Physical and environmental security
Continuity of Operations
Crisis Management
Computer security incident management
Detection
Ecosystem management
Information system security governance & risk management
SECURITY MEASURES FOR OES



The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

PROTECTION

IT Security Administration

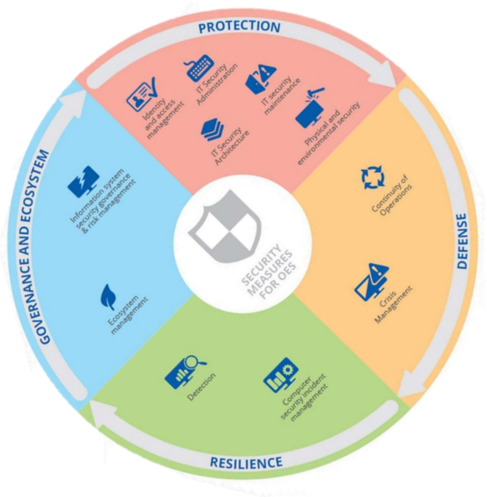

PROTECTION
Identity and access management
IT Security Administration
IT security maintenance
IT Security Architecture
Physical and environmental security
DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Detection
Computer security incident management
GOVERNANCE AND ECOSYSTEM
Information system security governance & risk management
Ecosystem management
SECURITY MEASURES FOR OES

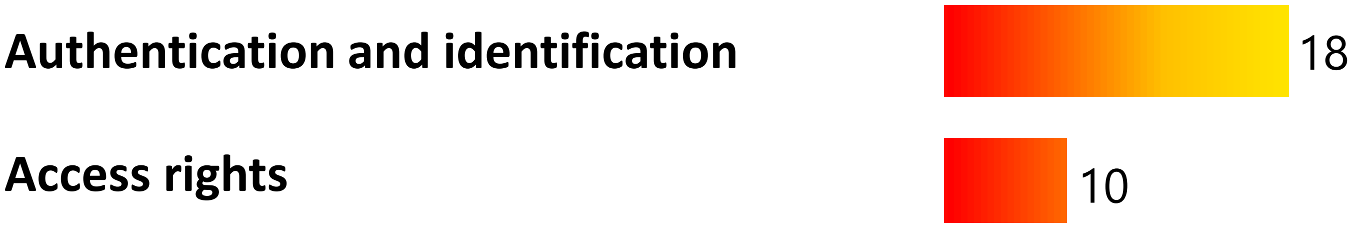
Administration accounts	🟥	10
Administration information systems	🟥	10

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

PROTECTION

Identity and access management

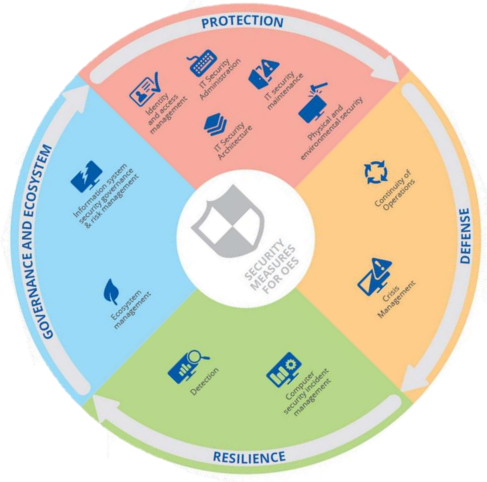

PROTECTION
Identity and access management
IT Security Administration
IT security maintenance
IT Security Architecture
Physical and environmental security
DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Detection
Computer security incident management
GOVERNANCE AND ECOSYSTEM
Information system security governance & risk management
Ecosystem management
SECURITY MEASURES FOR OES

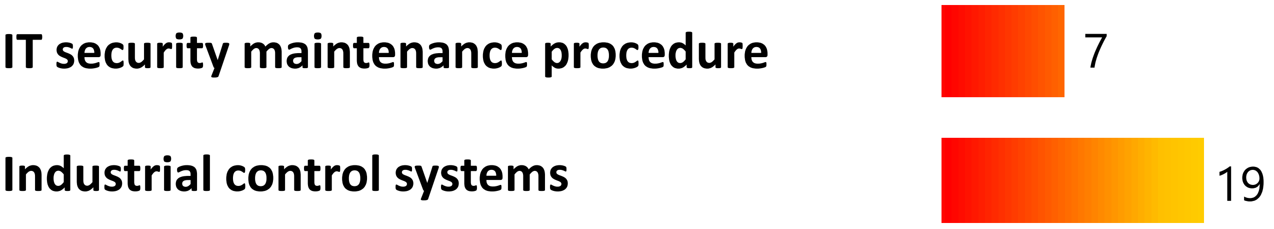


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

PROTECTION

IT Security Maintenance

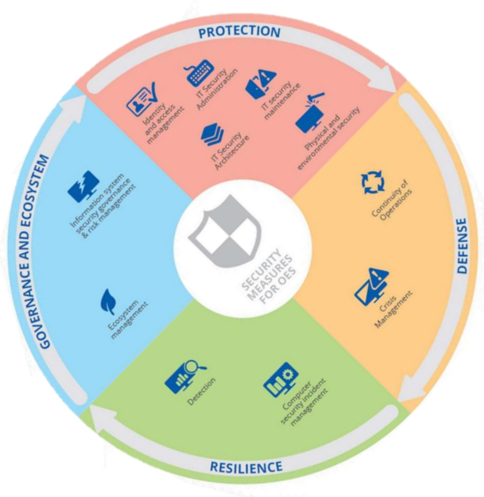

PROTECTION
DEFENSE
RESILIENCE
GOVERNANCE AND ECOSYSTEM
SECURITY MEASURES FOR OES
Identity and access management
IT Security Administration
IT security maintenance
IT Security Architecture
Physical and environmental security
Continuity of Operations
Crisis Management
Computer security incident management
Detection
Ecosystem management
Information system security governance & risk management



The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

PROTECTION

Physical and environmental security

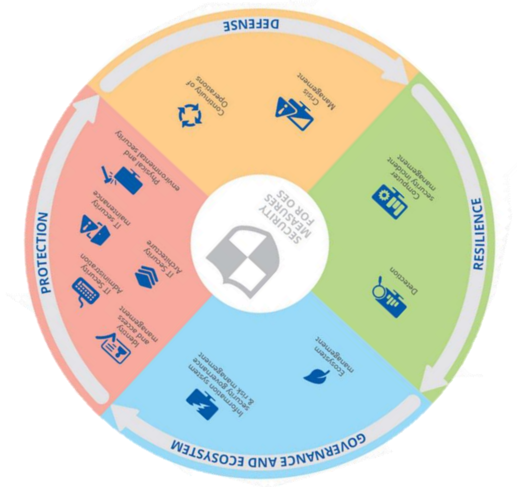

PROTECTION
Identity and access management
IT Security Administration
IT security maintenance
IT Security Architecture
Physical and environmental security
DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Detection
Computer security incident management
GOVERNANCE AND ECOSYSTEM
Information system security governance & risk management
Ecosystem management
SECURITY MEASURES FOR OES

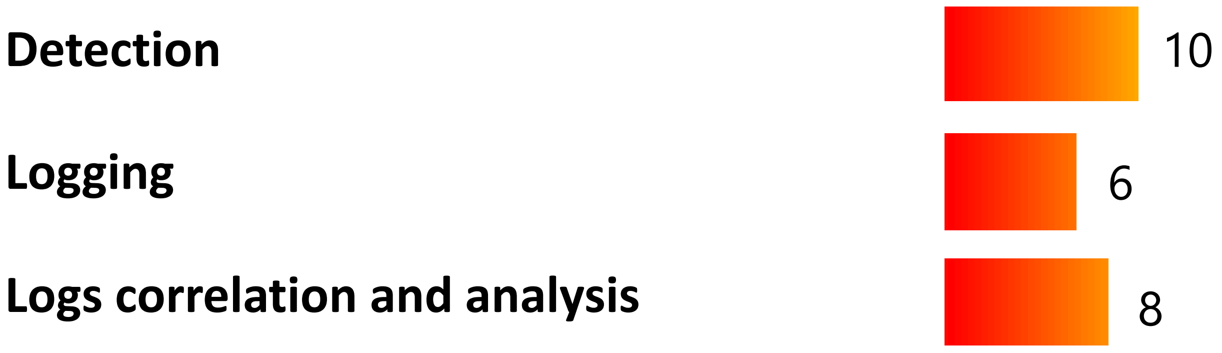
Physical and environmental security 🟥 13

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

DEFENSE

Detention

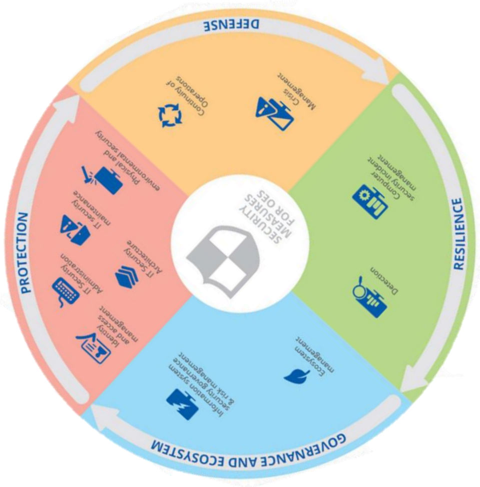

DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Computer security incident management
Detection
GOVERNANCE AND ECOSYSTEM
Ecosystem management
Information system security governance & risk management
PROTECTION
Identity and access management
IT security administration
IT security architecture
IT security maintenance
Physical and environmental security
SECURITY MEASURES FOR OES

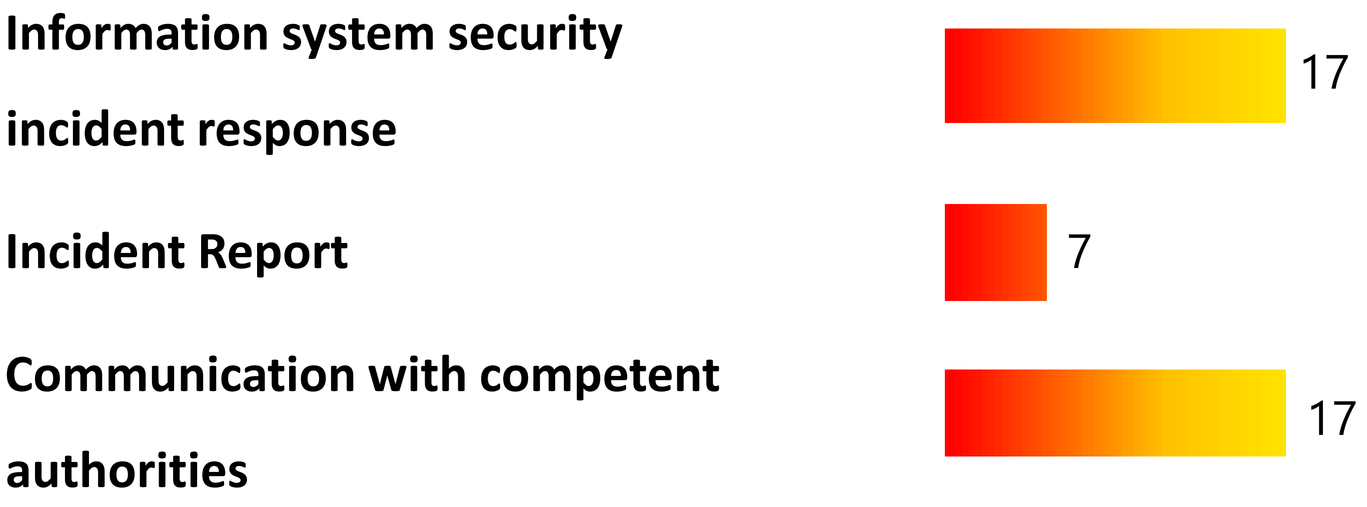


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

DEFENSE

Detention

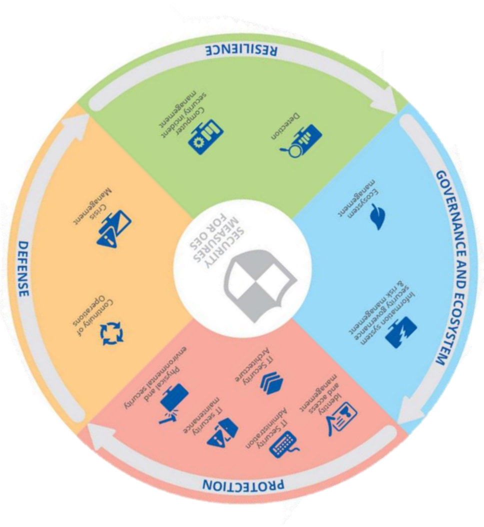

DEFENSE
Continuity of Operations
Crisis Management
RESILIENCE
Computer security incident management
Detection
GOVERNANCE AND ECOSYSTEM
Ecosystem management
Information system security governance & risk management
PROTECTION
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
SECURITY MEASURES FOR OES

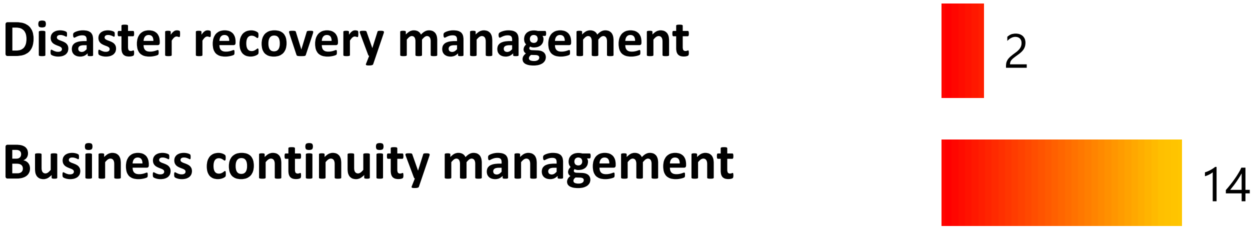


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

RESILIENCE

Continuity of operations


RESILIENCE
GOVERNANCE AND ECOSYSTEM
PROTECTION
DEFENSE
SECURITY MEASURES FOR OES
Computer security incident management
Detection
Ecosystem management
Information system security governance & risk management
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
Continuity of Operations
Crisis Management

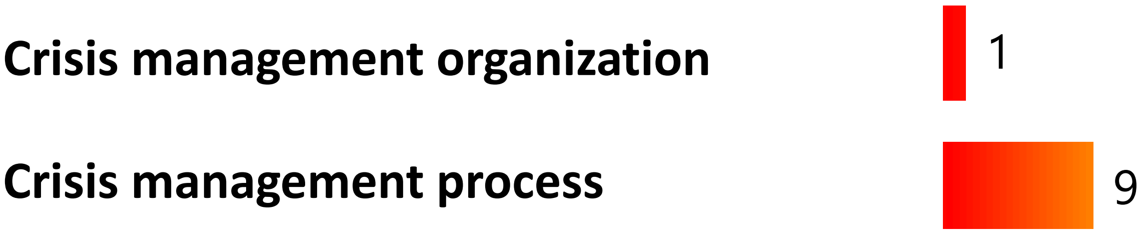


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

RESILIENCE

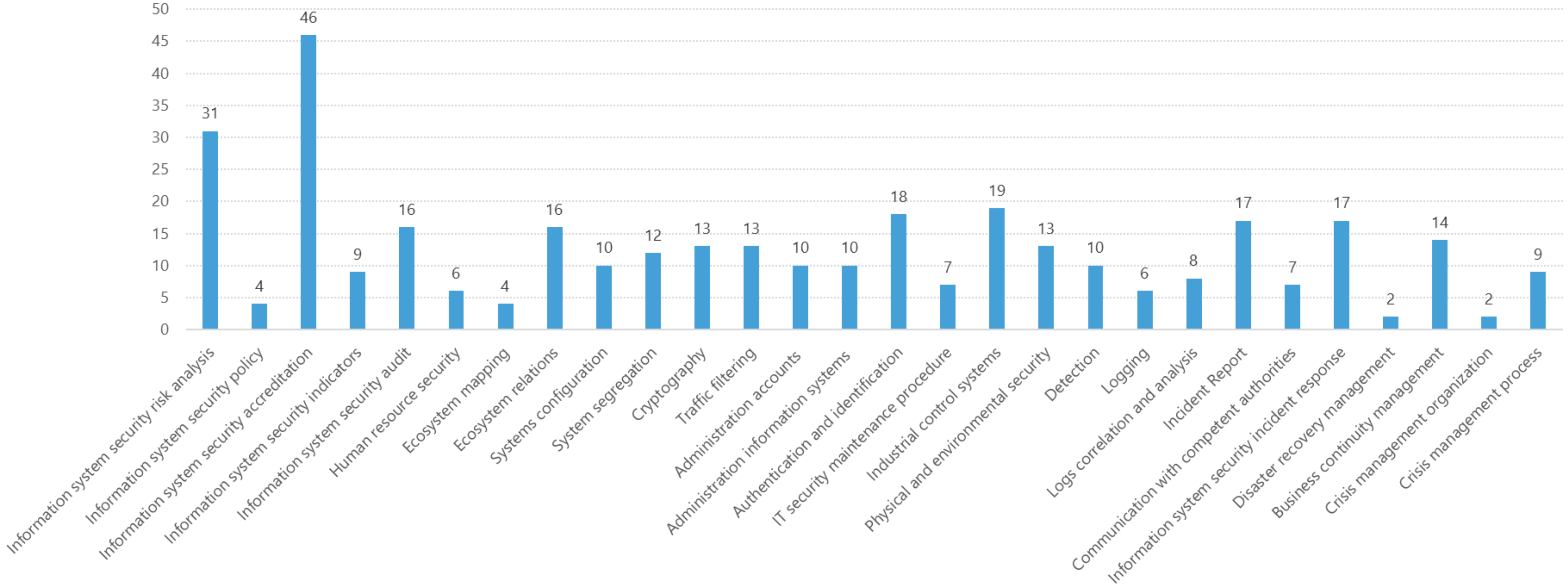
Crisis management

RESILIENCE
GOVERNANCE AND ECOSYSTEM
PROTECTION
DEFENSE
SECURITY MEASURES FOR OES
Computer security incident management
Detection
Ecosystem management
Information system security governance & risk management
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
Continuity of Operations
Crisis Management

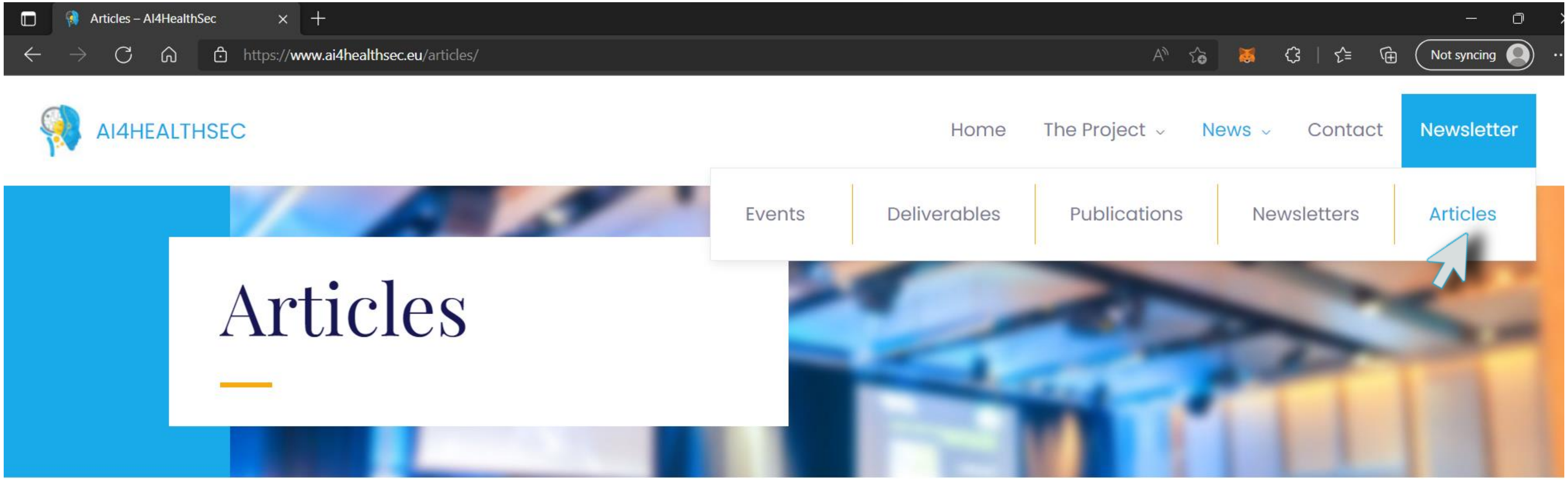


The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

MEASURES vs STANDARDS



The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.



Articles

Articles by the Project Partners

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.

Contact

Via P. Castellino, 111
Napoli – 80131
coord_ai4hsec@icar.cnr.it
Tel. +39 0816139508

Thank you very much!

argyro.chatzopoulou@tuv.at

Follow

https://twitter.com/aifourhealthsec

https://www.linkedin.com/company/ai4healthsec-eu-h2020-project/

https://www.facebook.com/Ai4HealthSec

https://www.ai4healthsec.eu/

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright by the AI4HEALTHSEC Consortium.