Challenges and solutions of implementing the NIS2 Directive in Lithuania

Audrius Verseckas, Advisor

National Energy Regulatory Council of Lithuania

NATIONAL ENERGY REGULATORY COUNCIL

About me

CISO of National Energy Regulator

Master's degree in Information Systems

30 years in Information technology

Cyber Security Sertificates

Disclaimer

This is one person's perspective

It‘s all about the Council

The information provided is public

Mistakes! Who doesn't make them?

Summary

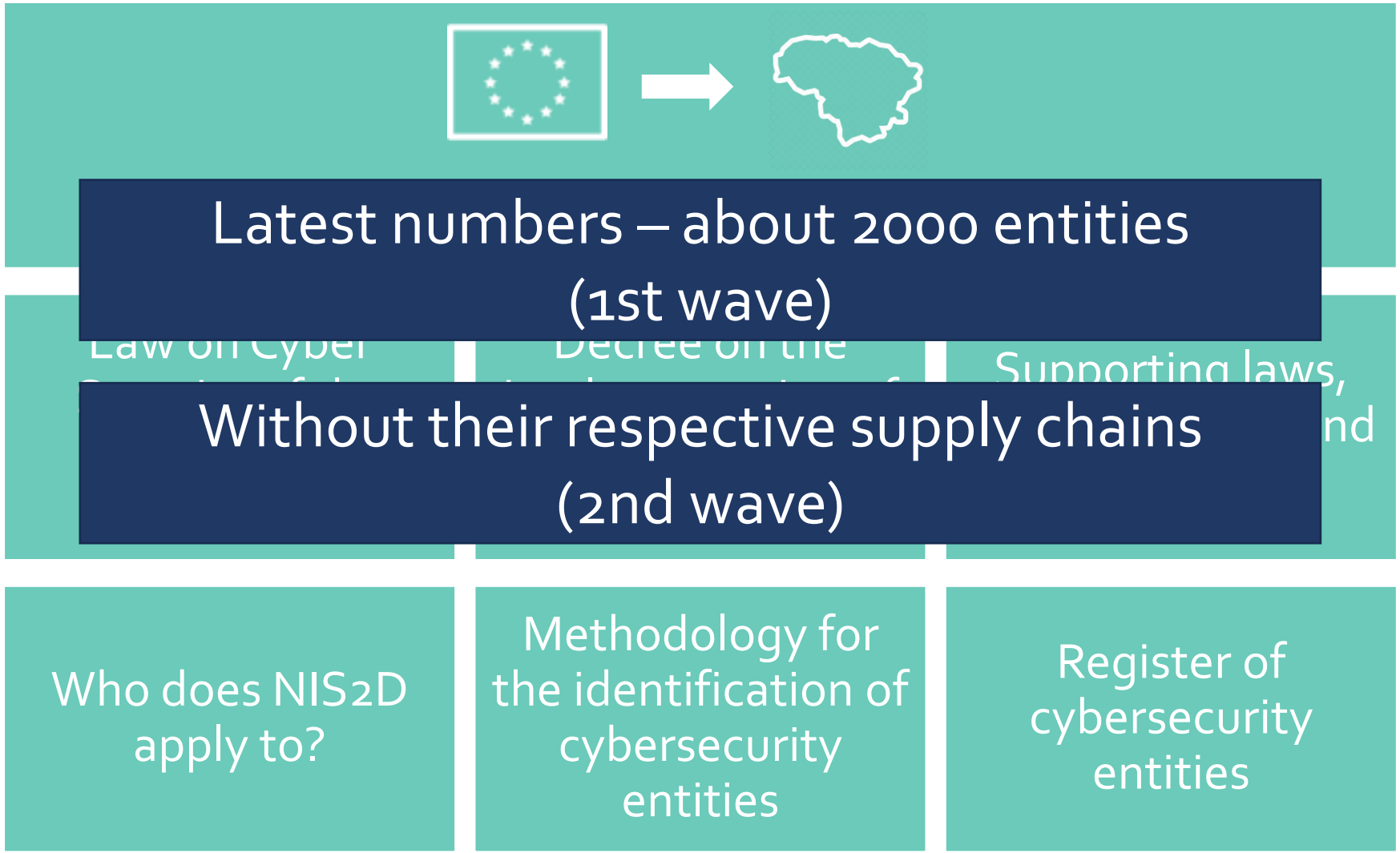
NIS2 Directive in Lithuania

Key concepts of implementation

National cybersecurity authority help

Main challenges for the Council

NIS2 Directive (NIS2D) → NIS2D-LTU



NIS2D-LTU – Key concepts of the Law

(2) the duties of the responsibl

(1) cybersecurity policies;
(7) effectiveness procedure;
(9) cryptography and

(8) cyber hygiene practices
curity

Decree on the implementation of the Cyber Security Law
„Description of cybersecurity requirements“

(3) manag
incidents;
(4) business continuity;
(6) management of vulnerabilities;

(11) the use of multifactor/persistent authentications, secure communications;

(1) cybersecurity risk;
(5) supply chain security;

NIS2D-LTU – Duties

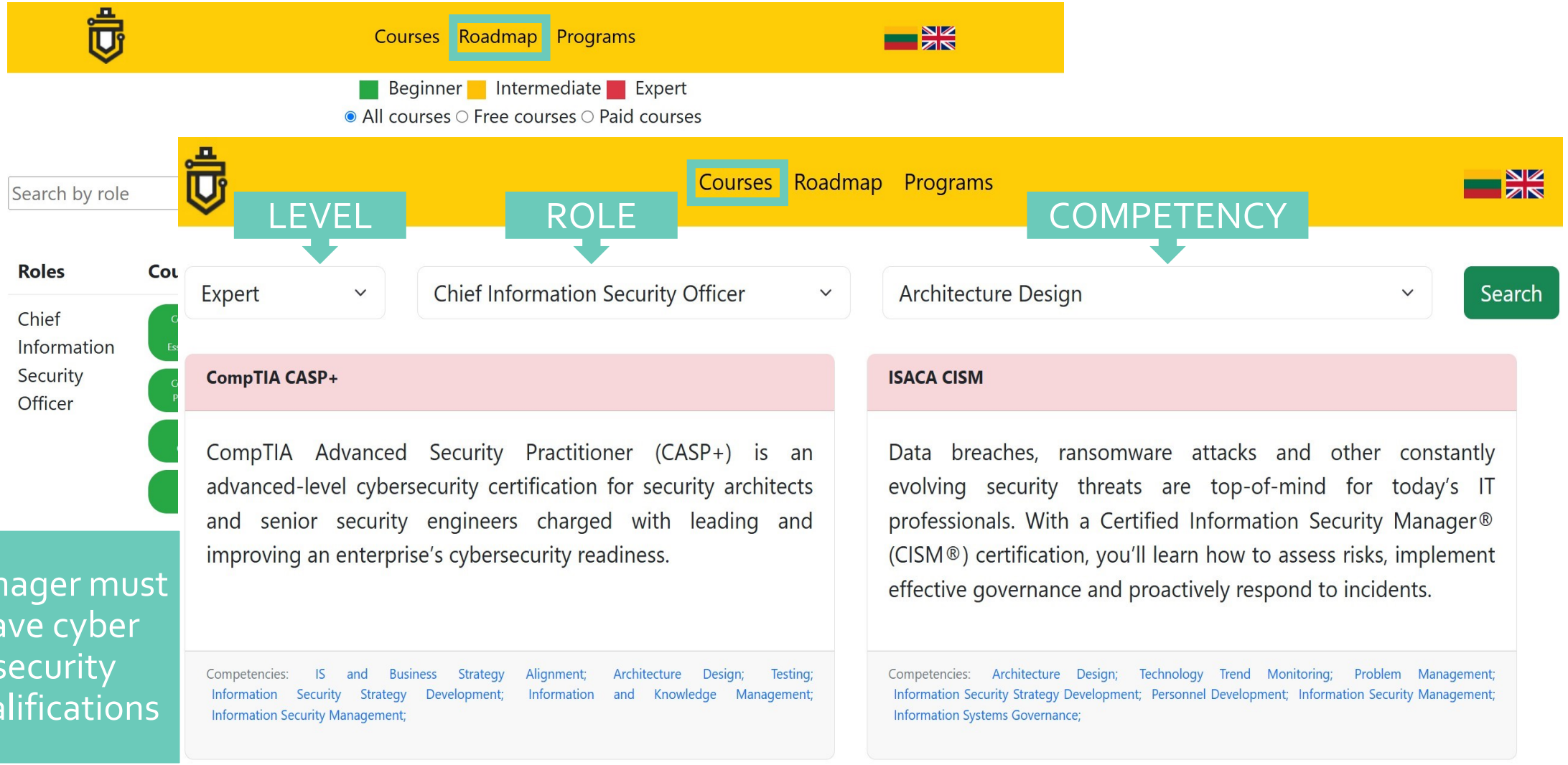
(2) the duties of the head of the entity

- Must appoint a cybersecurity Manager
- CS Manager must not perform IT functions
- CS Manager must have cyber security qualifications
- The head must complete a cyber hygiene course

(2) the duties of the cybersecurity Manager

- Implementation and maintenance of
  - Organizational measures
  - Technical measures
  - Operational measures

NCSC help – Interactive competency platform



Manager must have cyber security qualifications

NIS2D-LTU – Key concepts of the Law

(2) the duties of the responsible persons;

(1) cybersecurity policies;
(7) effectiveness procedure;
(9) cryptography and encryption policy;
(10) policies for NAC;

(8) cyber hygiene practices and regular cybersecurity training;

(3) management of cyber incidents;
(4) business continuity;
(6) management of vulnerabilities;

(6) the security of the lifecycle of NIS;
(11) the use of multifactor/persistent authentications, secure communications;

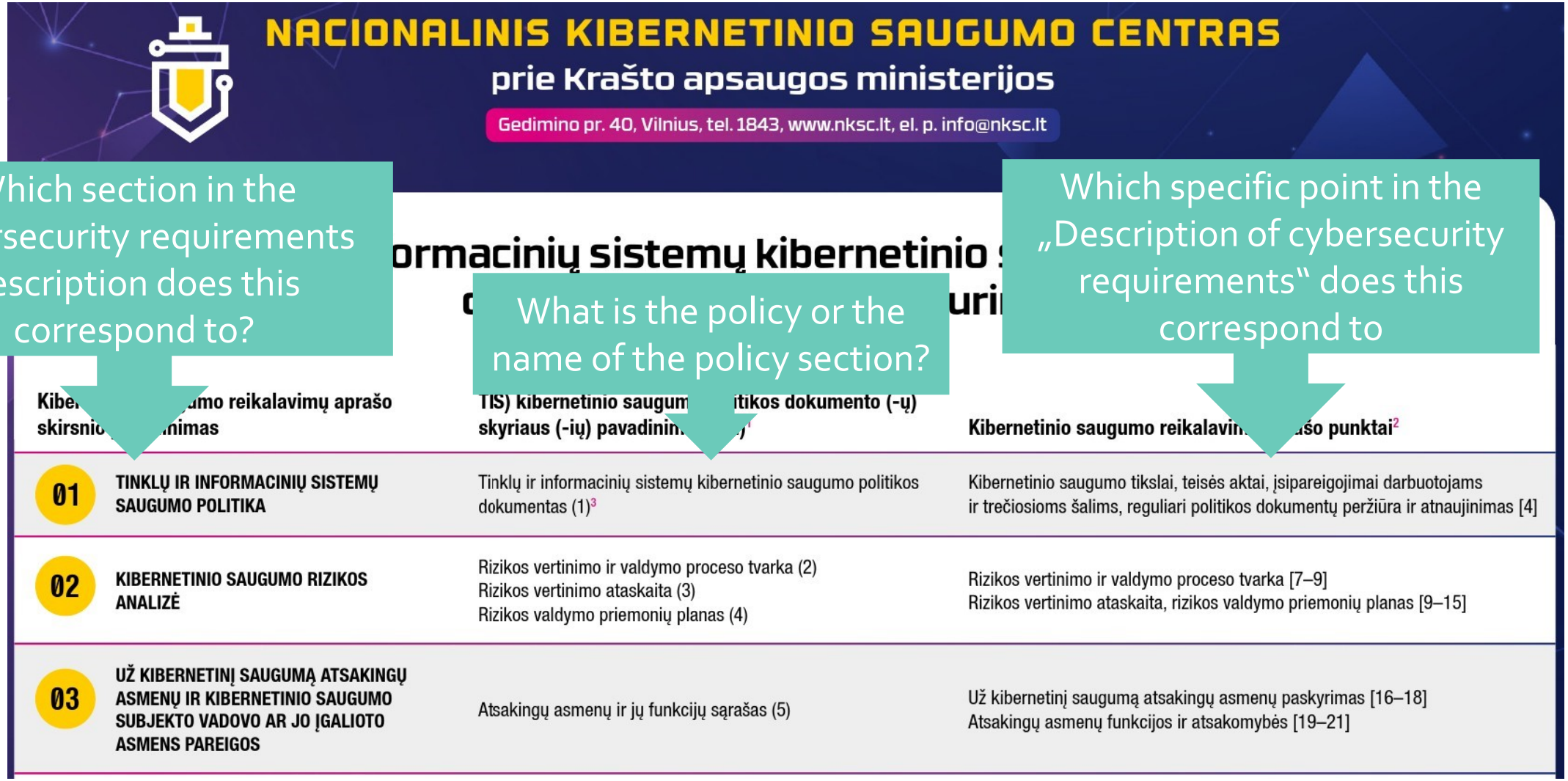
(1) cybersecurity risk;
(5) supply chain security;
(10) human resources security;

NCSC help – Possible content of Policy (-ies)

Which section in the cybersecurity requirements description does this correspond to?

What is the policy or the name of the policy section?

Which specific point in the „Description of cybersecurity requirements" does this correspond to



NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
prie Krašto apsaugos ministerijos
Gedimino pr. 40, Vilnius, tel. 1843, www.nksc.lt, el. p. info@nksc.lt

ormacinių sistemų kibernetinio

Kiber…umo reikalavimų aprašo skirsnio…inimas	TIS) kibernetinio saugum…itikos dokumento (-ų) skyriaus (-ių) pavadinim…[1]	Kibernetinio saugumo reikalavi…šo punktai[2]
01 TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO POLITIKA	Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentas (1)[3]	Kibernetinio saugumo tikslai, teisės aktai, įsipareigojimai darbuotojams ir trečiosioms šalims, reguliari politikos dokumentų peržiūra ir atnaujinimas [4]
02 KIBERNETINIO SAUGUMO RIZIKOS ANALIZĖ	Rizikos vertinimo ir valdymo proceso tvarka (2) Rizikos vertinimo ataskaita (3) Rizikos valdymo priemonių planas (4)	Rizikos vertinimo ir valdymo proceso tvarka [7–9] Rizikos vertinimo ataskaita, rizikos valdymo priemonių planas [9–15]
03 UŽ KIBERNETINĮ SAUGUMĄ ATSAKINGŲ ASMENŲ IR KIBERNETINIO SAUGUMO SUBJEKTO VADOVO AR JO ĮGALIOTO ASMENS PAREIGOS	Atsakingų asmenų ir jų funkcijų sąrašas (5)	Už kibernetinį saugumą atsakingų asmenų paskyrimas [16–18] Atsakingų asmenų funkcijos ir atsakomybės [19–21]

NIS2D-LTU – Key concepts of the Law

(2) the duties of the responsible persons;

(1) cybersecurity policies;
(7) effectiveness procedure;
(9) cryptography and encryption policy;
(10) policies for NAC;

(8) cyber hygiene practices and regular cybersecurity training;

(3) management of cyber incidents;
(4) business continuity;
(6) management of vulnerabilities;

(6) the security of the lifecycle of NIS;
(11) the use of multifactor/persistent authentications, secure communications;

(12) cybersecurity risk;
(5) supply chain security;
(10) human resources security;

NCSC help – Interactive learning platform

NATIONAL CYBER SECURITY CENTER

Log in Help

Cybersecurity for managers

Learn strategies to strengthen basic cybersecurity in your organization, including steps to assess existing security measures and an overview of key cybersecurity legislation. This topic will also encourage you to address key cybersecurity issues and understand the reasons for separating IT and cybersecurity departments.

Start this course

The head must complete a cyber hygiene course

NIS2D-LTU – Key concepts of the Law

(2) the duties of the responsible persons;

(1) cybersecurity policies;
(7) effectiveness procedure;
(9) cryptography and encryption policy;
(10) policies for NAC;

(8) cyber hygiene practices and regular cybersecurity training;

(3) management of cyber incidents;
(4) business continuity;
(6) management of vulnerabilities;

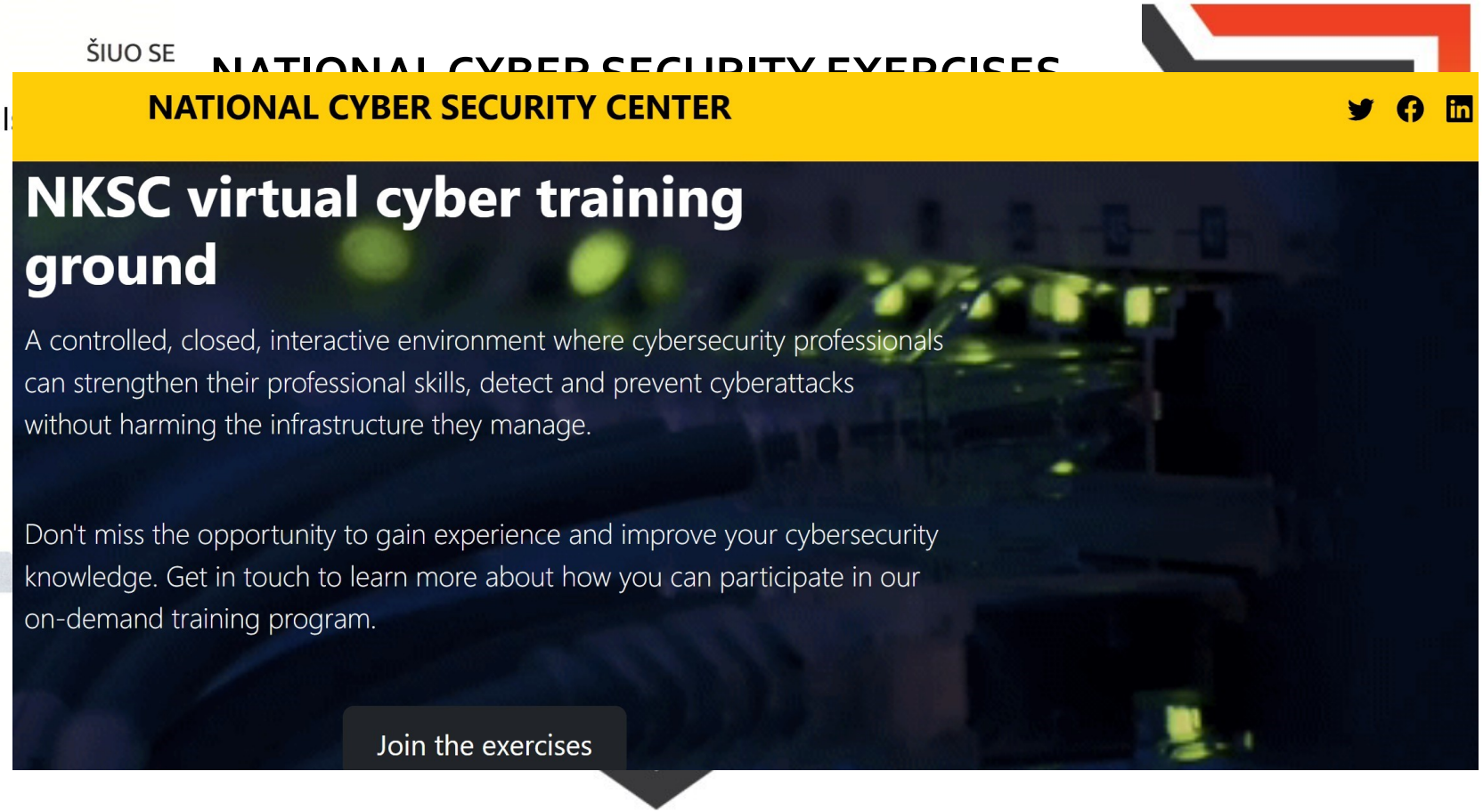
(6) the security of the lifecycle of NIS;
(11) the use of multifactor/persistent authentications, secure communications;

(12) cybersecurity risk;
(5) supply chain security;
(10) human resources security;

NCSC help – Exercises

KIBERNETINIS SKYDAS 2023

NATIONAL CYBER SECURITY EXERCISES
"CYBER SHIELD OPEX"



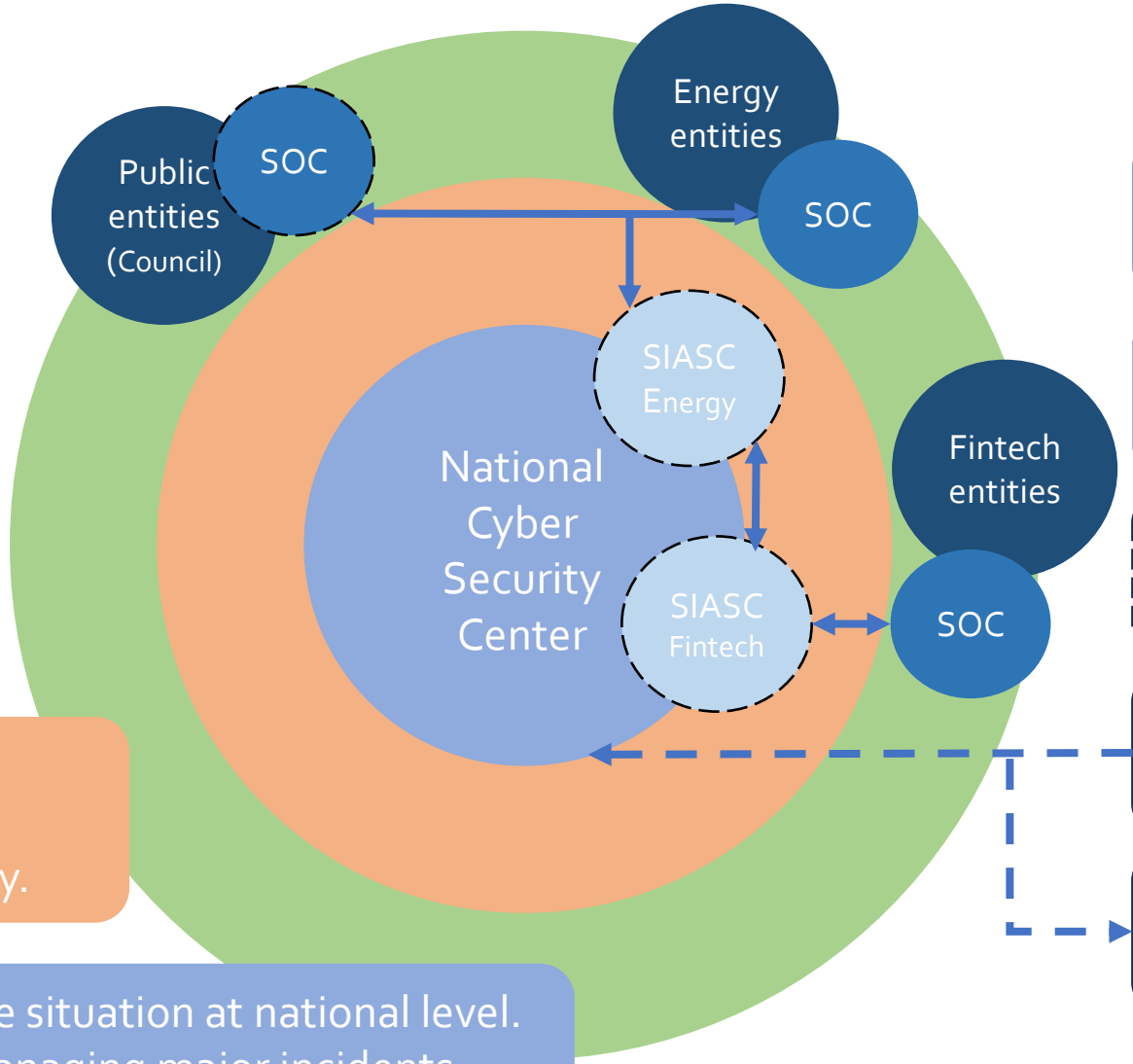
NIS2D-LTU – New cyber defense architecture

THREE LINES OF DEFENSE

1 Continuous monitoring.
Incident response.
Vulnerability management.

2 Cyber threat inteligence.
Assistance across sectors.
Assistance within the country.

3 Monitoring and assessing the situation at national level.
Assistance and support in managing major incidents.
Assistance in developing capacities and competencies.



Cyber security subjects

Cyber security subjects Security Operations Centers

Sectoral information analysis and sharing centers

National Cyber security center (CSIRT-LT)

National and International partners (CTI+)

vert

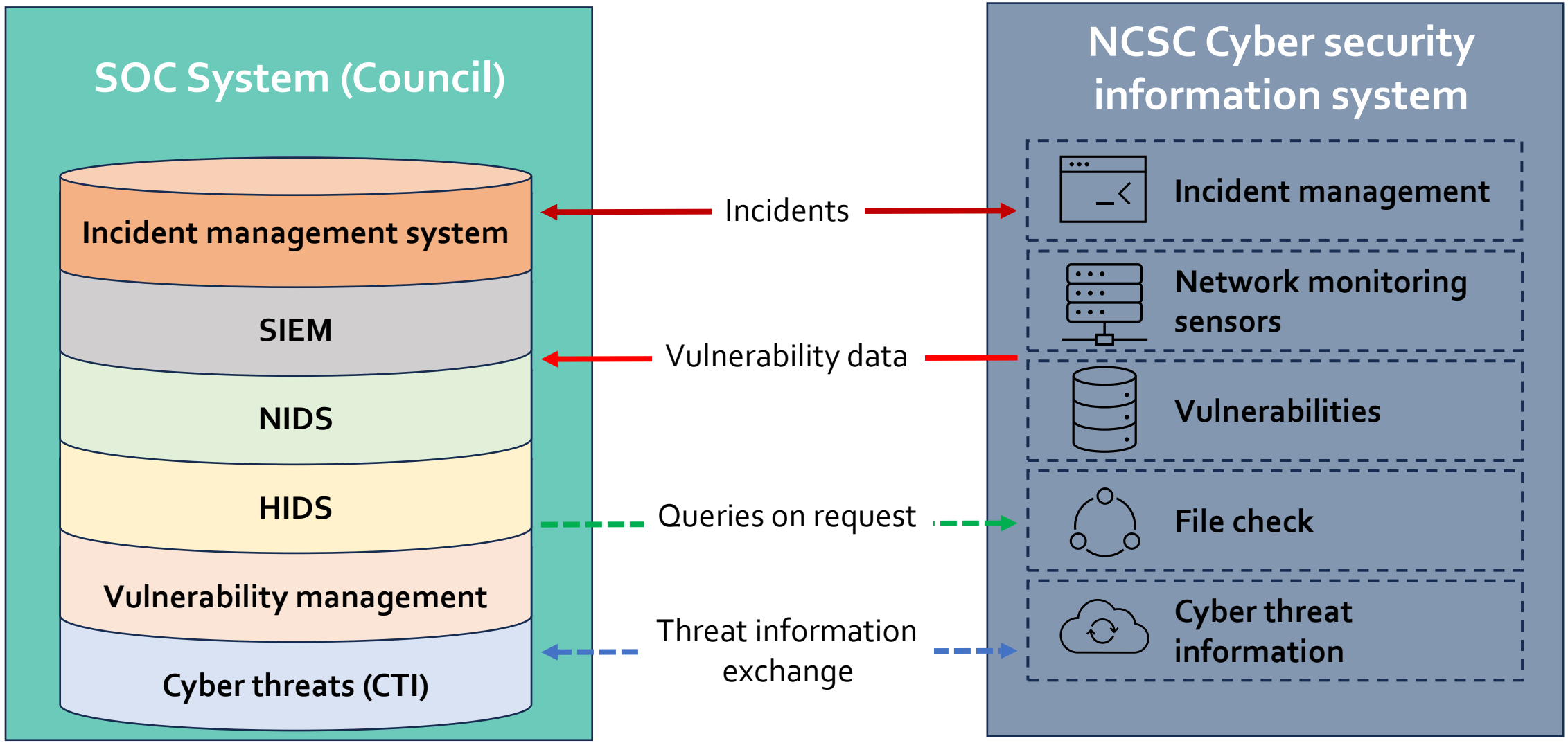
Council – Why have own SOC?

Requirement by the Cyber Security Law to have SOC or to buy SOC service.

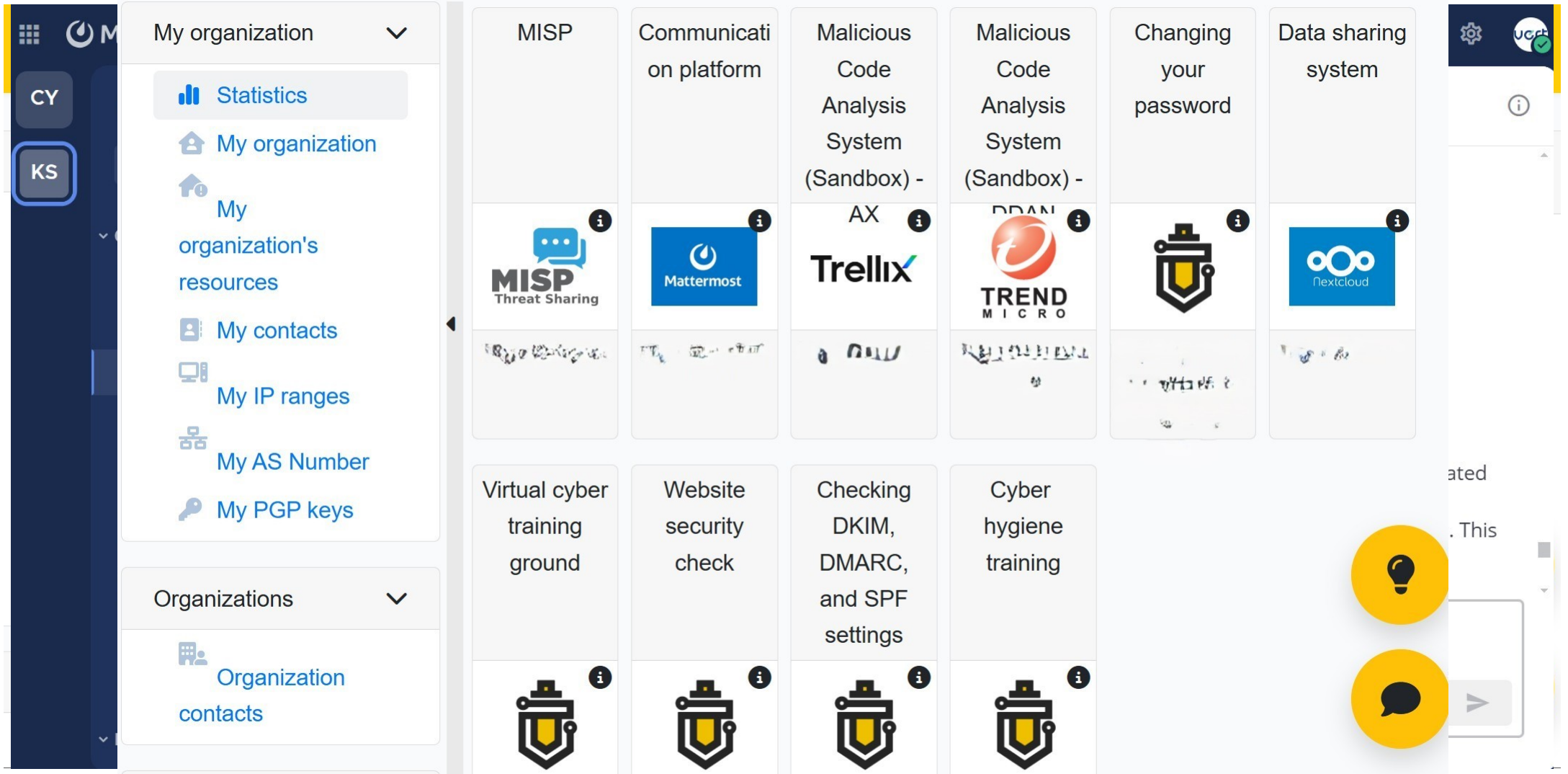
The Network Code on Cybersecurity (NCCS) regulation and the decision that the Council should be the competent authority

NCSC initiative to offer project of ready-made SOC solution with hardware and software, training and procedures

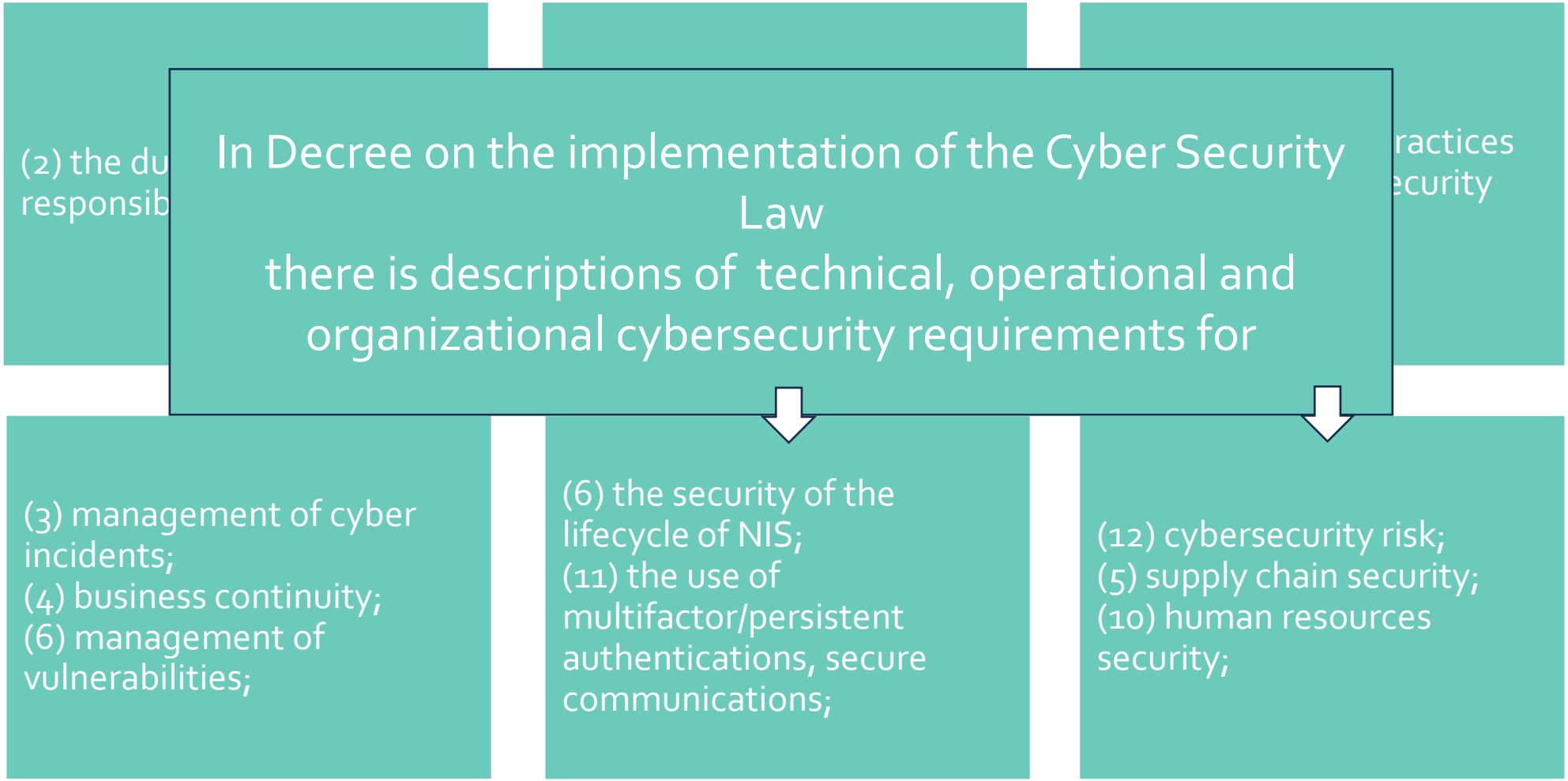
NCSC help – SOC project



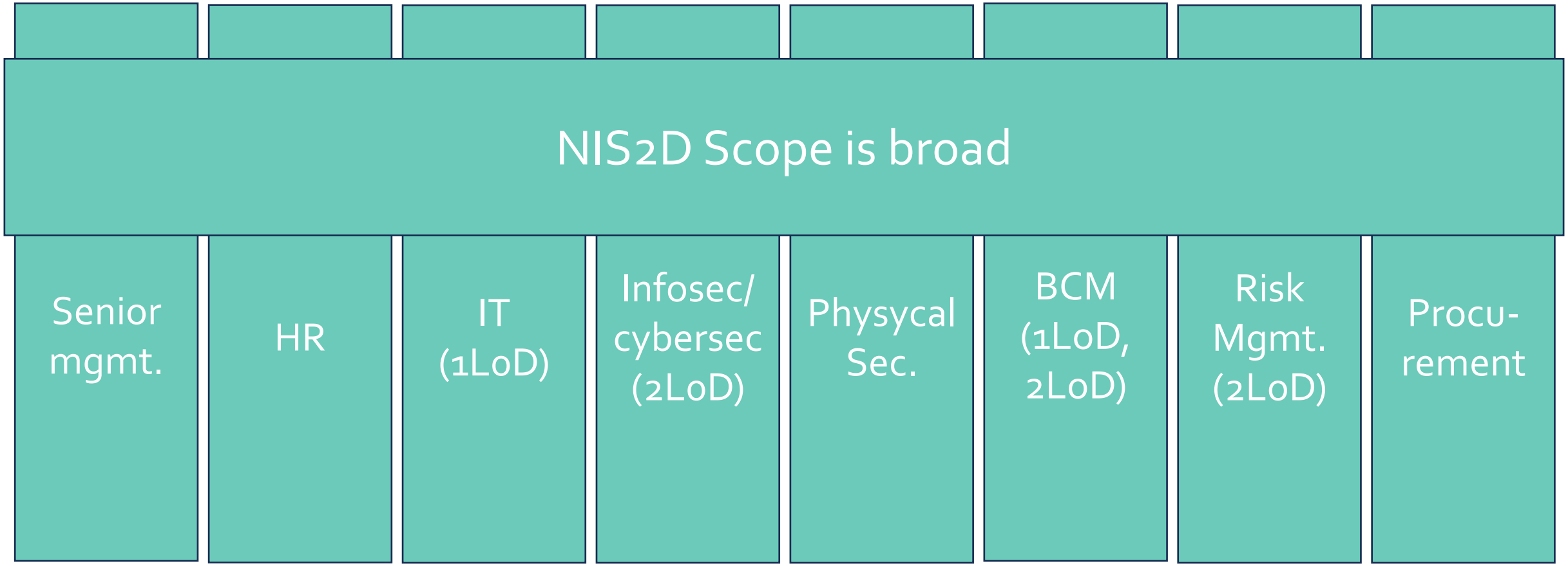
NCSC help – Existing tools



NIS2D-LTU – Key concepts of the Law



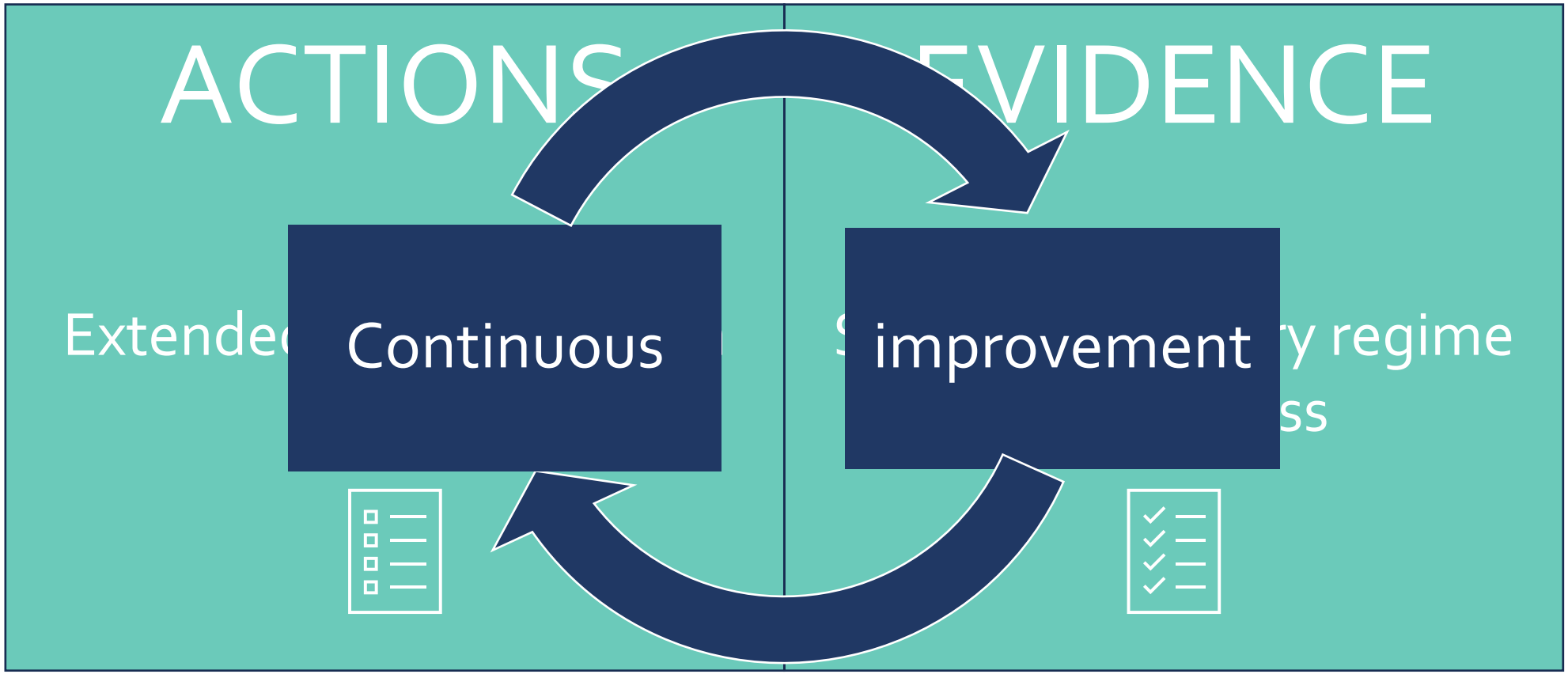
NIS2D-LTU – Implementation in Council



NIS2D-LTU – Implementation in Council

Define the work scope	Normalize toward best practice	Standardize (recognized frameworks)	Project (-s)	Line and audit runbooks	Continuous improve-ments	Integrate management systems	
Project 1:	Framework	Structure	Processes	Documen-tation	Reporting	Managerial actions	
Project 2:	Actions in the line	IT	Risk managers	Procure-ment	HR	Etc.	

NIS2D-LTU – Implementation in Council



NIS2D-LTU – The essence