



Challenges and solutions of implementing the NIS2 Directive in Lithuania

Audrius Verseckas, Advisor
National Energy Regulatory Council of Lithuania

About me



CISO of National
Energy Regulator



Master's degree in
Information Systems



30 years in Information
technology



Cyber Security
Certificates

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



Latest numbers – about 2000 entities
(1st wave)

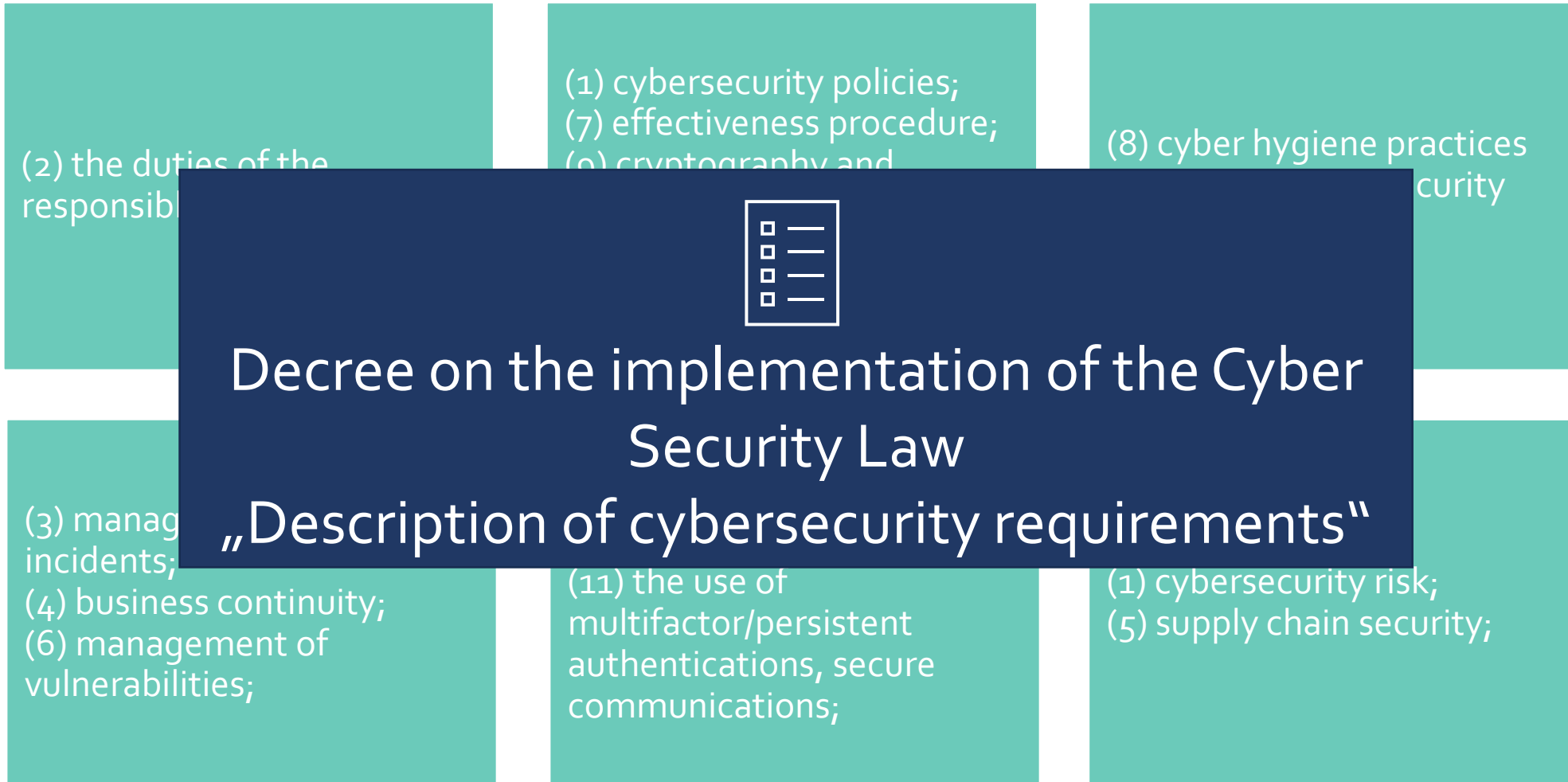
Without their respective supply chains
(2nd wave)

Who does NIS2D
apply to?

Methodology for
the identification of
cybersecurity
entities

Register of
cybersecurity
entities

NIS2D-LTU – Key concepts of the Law



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

LEVEL **ROLE** **COMPETENCY**

Expert | Chief Information Security Officer | Architecture Design

CompTIA CASP+

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness.

Competencies: IS and Business Strategy Alignment; Architecture Design; Testing; Information Security Strategy Development; Information and Knowledge Management; Information Security Management;

ISACA CISM

Data breaches, ransomware attacks and other constantly evolving security threats are top-of-mind for today's IT professionals. With a Certified Information Security Manager® (CISM®) certification, you'll learn how to assess risks, implement effective governance and proactively respond to incidents.

Competencies: Architecture Design; Technology Trend Monitoring; Problem Management; Information Security Strategy Development; Personnel Development; Information Security Management; Information Systems Governance;

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)



NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

prie Krašto apsaugos ministerijos

Gedimino pr. 40, Vilnius, tel. 1843, www.nksc.lt, el. p. info@nksc.lt

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

Kibernetinio saugumo reikalavimų aprašo skirsnio pavadinimas	TIS) kibernetinio saugumo politikos dokumento (-ų) skyriaus (-ių) pavadinimas	Kibernetinio saugumo reikalavimų aprašo 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



SERTIFIKATAS

ŠIUO SERTIFIKATU PAŽYMIMA, KAD

Audrius Verseckas

Dalyvavo mokymuose „Kibernetinė sauga vadovams“ ir sėkmingai išlaikė testą.

Nacionalinio kibernetinio saugumo centro prie
Krašto apsaugos ministerijos direktorius
Liudas Ališauskas



Kurso trukmė – 1 akad. val.

rugsėjo 17, 2024
Data

5w009mUDVC
Serijos numeris

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"

SEPTIEMKARTAS

ŠIUOSE NATIONAL CYBER SECURITY EXERCISES

Val

NATIONAL CYBER SECURITY CENTER



NKSC virtual cyber training ground

A controlled, closed, interactive environment where cybersecurity professionals can strengthen their professional skills, detect and prevent cyberattacks without harming the infrastructure they manage.

Don't miss the opportunity to gain experience and improve your cybersecurity knowledge. Get in touch to learn more about how you can participate in our on-demand training program.

Join the exercises



NIS2D-LTU – New cyber defense architecture

THREE LINES OF DEFENSE

1

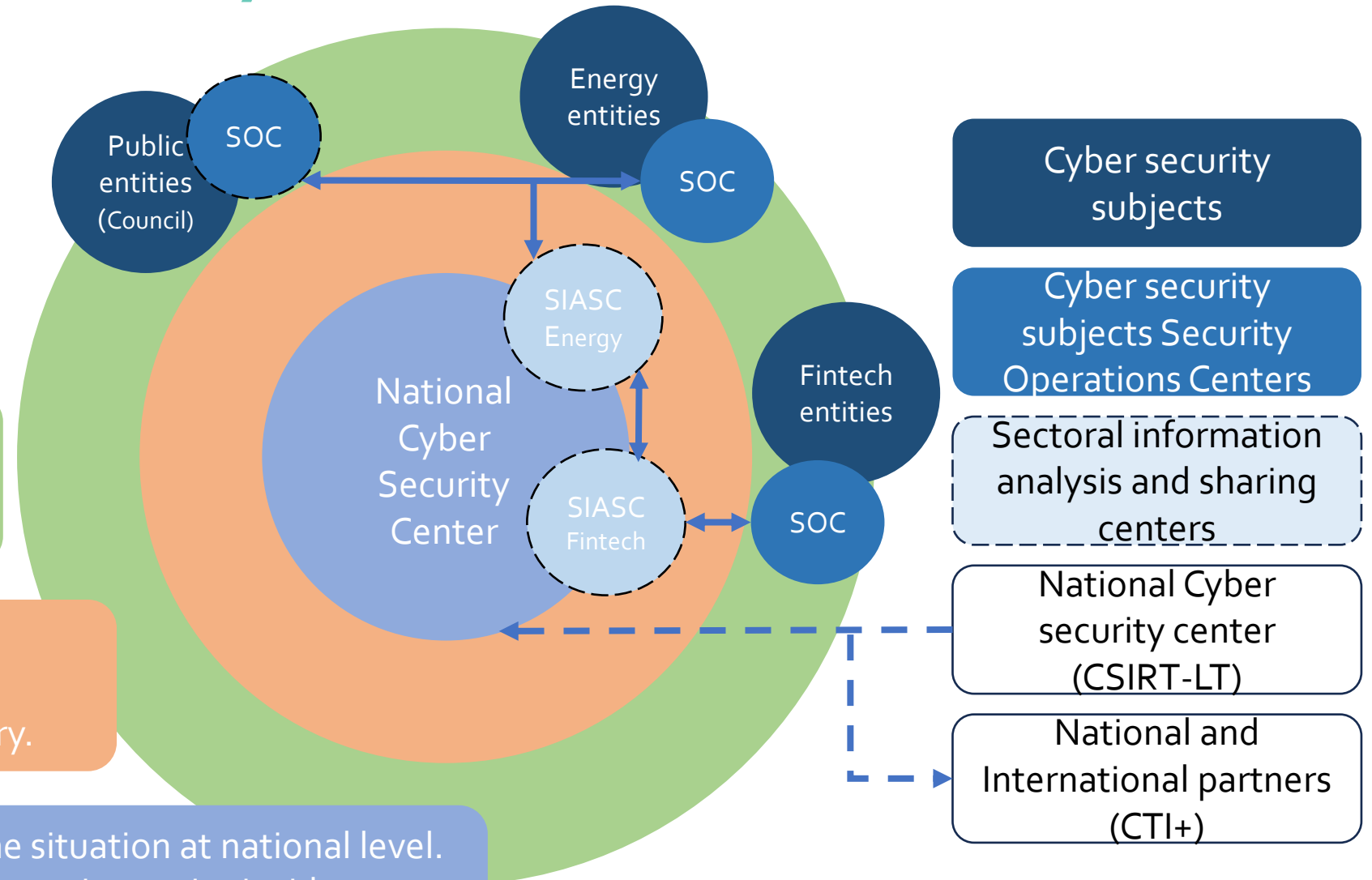
Continuous monitoring.
Incident response.
Vulnerability management.

2

Cyber threat intelligence.
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.



Council – Why have own SOC?



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

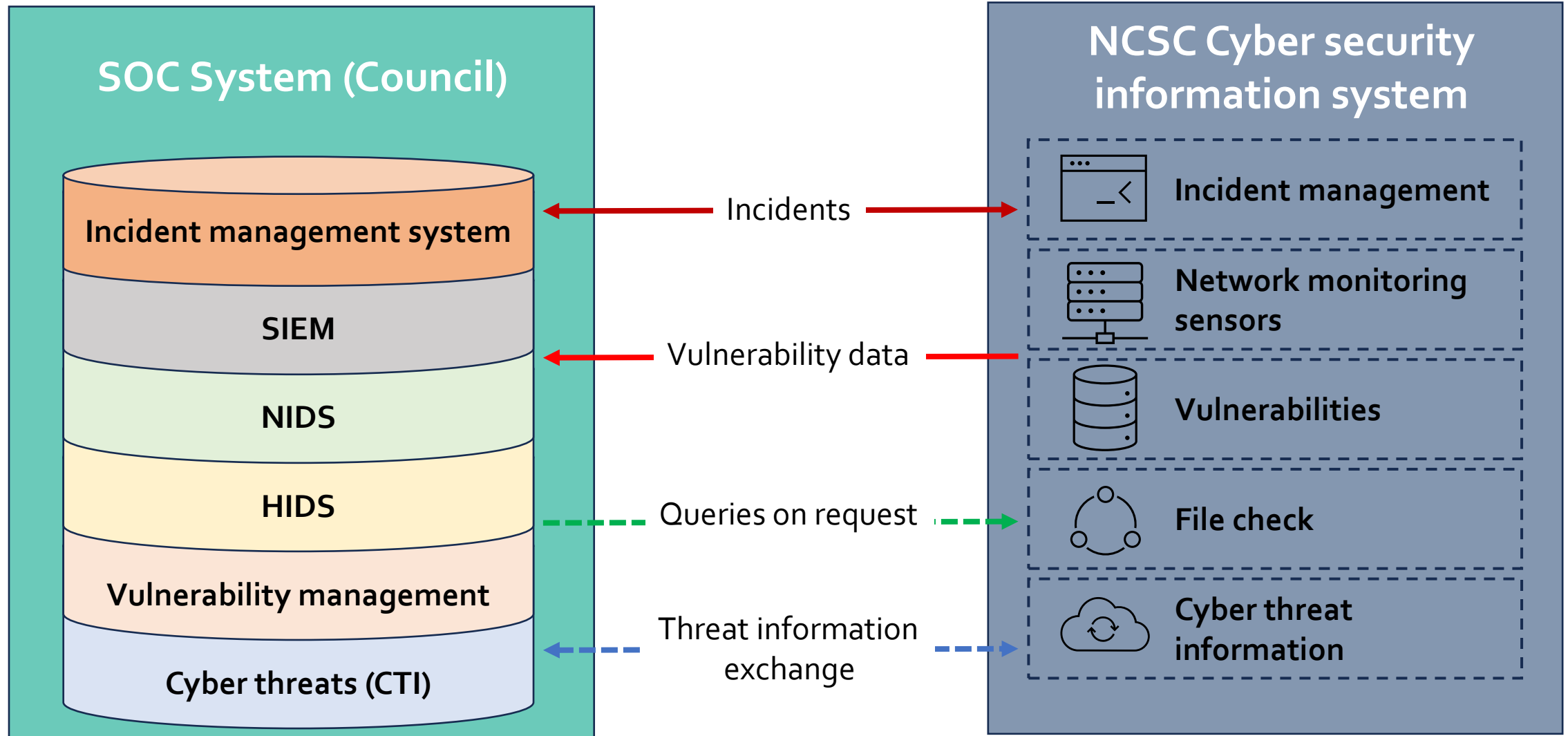


The Network Code on Cybersecurity (NCCS) regulation and the decision that the Council should be the competent authority



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

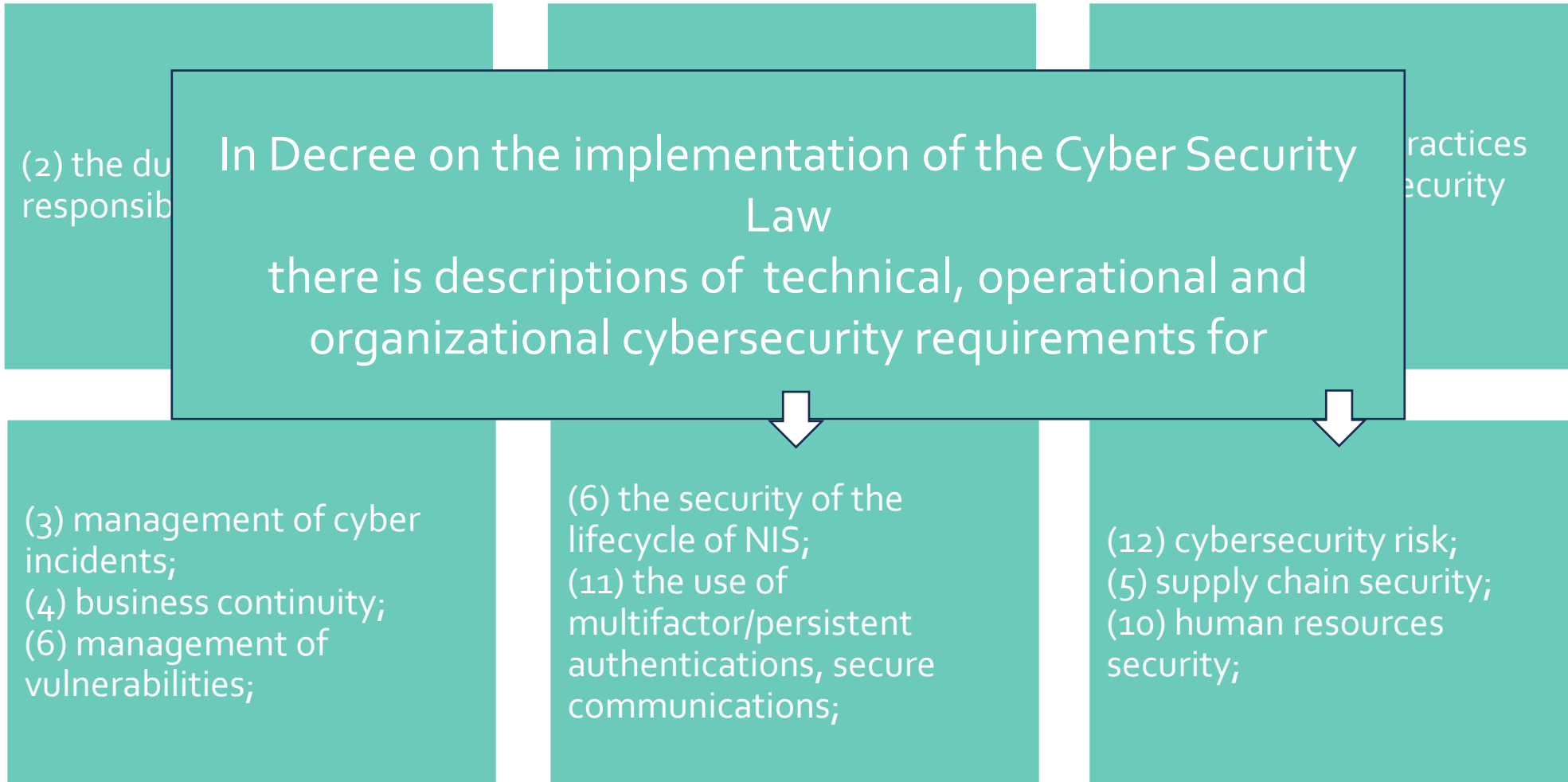
The screenshot displays the NCSC help portal interface. On the left is a dark blue navigation sidebar with a grid icon, a refresh icon, and two buttons labeled 'CY' and 'KS'. The main content area is divided into two sections: 'My organization' and 'Organizations'. The 'My organization' section includes links for 'Statistics', 'My organization', 'My organization's resources', 'My contacts', 'My IP ranges', 'My AS Number', and 'My PGP keys'. The 'Organizations' section includes a link for 'Organization contacts'. The main content area is a grid of tool cards, each with a title, an icon, and an information icon (i). The cards are arranged in two rows. The first row contains: 'MISP' (MISP Threat Sharing icon), 'Communication platform' (Mattermost icon), 'Malicious Code Analysis System (Sandbox) - AX' (Trellix icon), 'Malicious Code Analysis System (Sandbox) - DDAN' (Trend Micro icon), 'Changing your password' (Shield icon), and 'Data sharing system' (Nextcloud icon). The second row contains: 'Virtual cyber training ground' (Shield icon), 'Website security check' (Shield icon), 'Checking DKIM, DMARC, and SPF settings' (Shield icon), and 'Cyber hygiene training' (Shield icon). At the bottom right, there are two yellow circular icons: a lightbulb and a speech bubble. The 'verit' logo is visible in the bottom right corner.

Indicators of Compromise (IOCs)

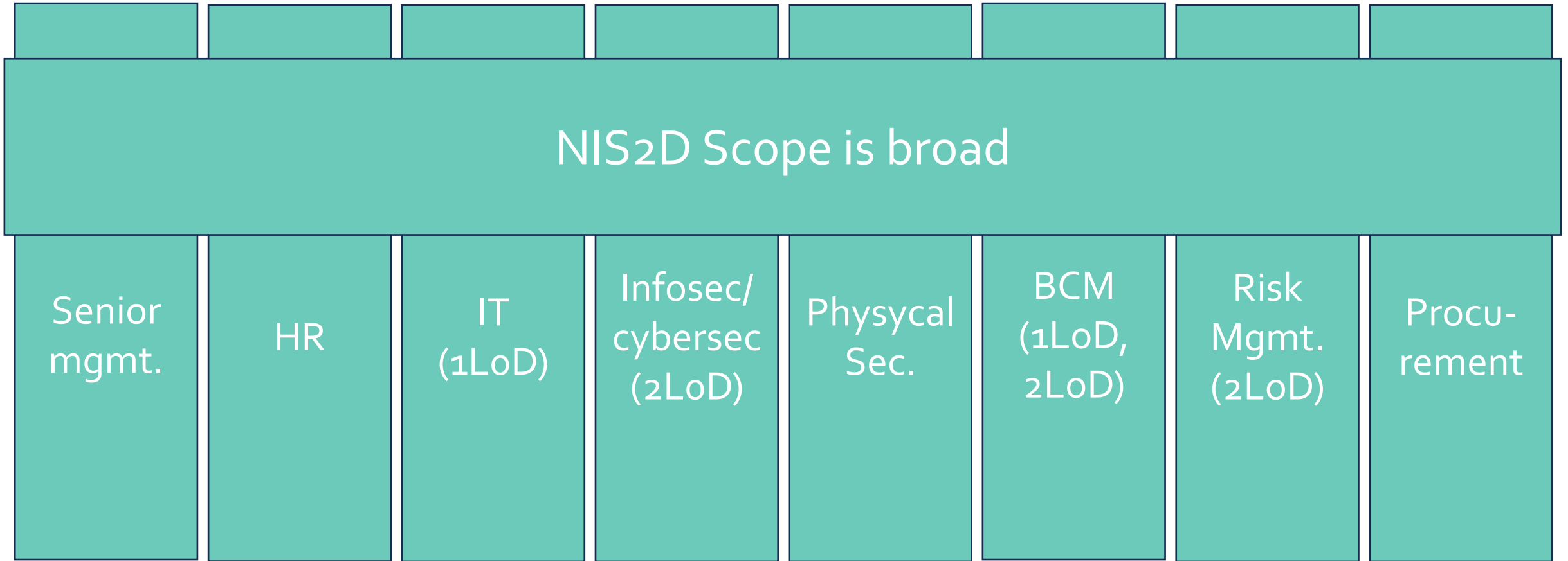
Essential sectors

5

NIS2D-LTU – Key concepts of the Law



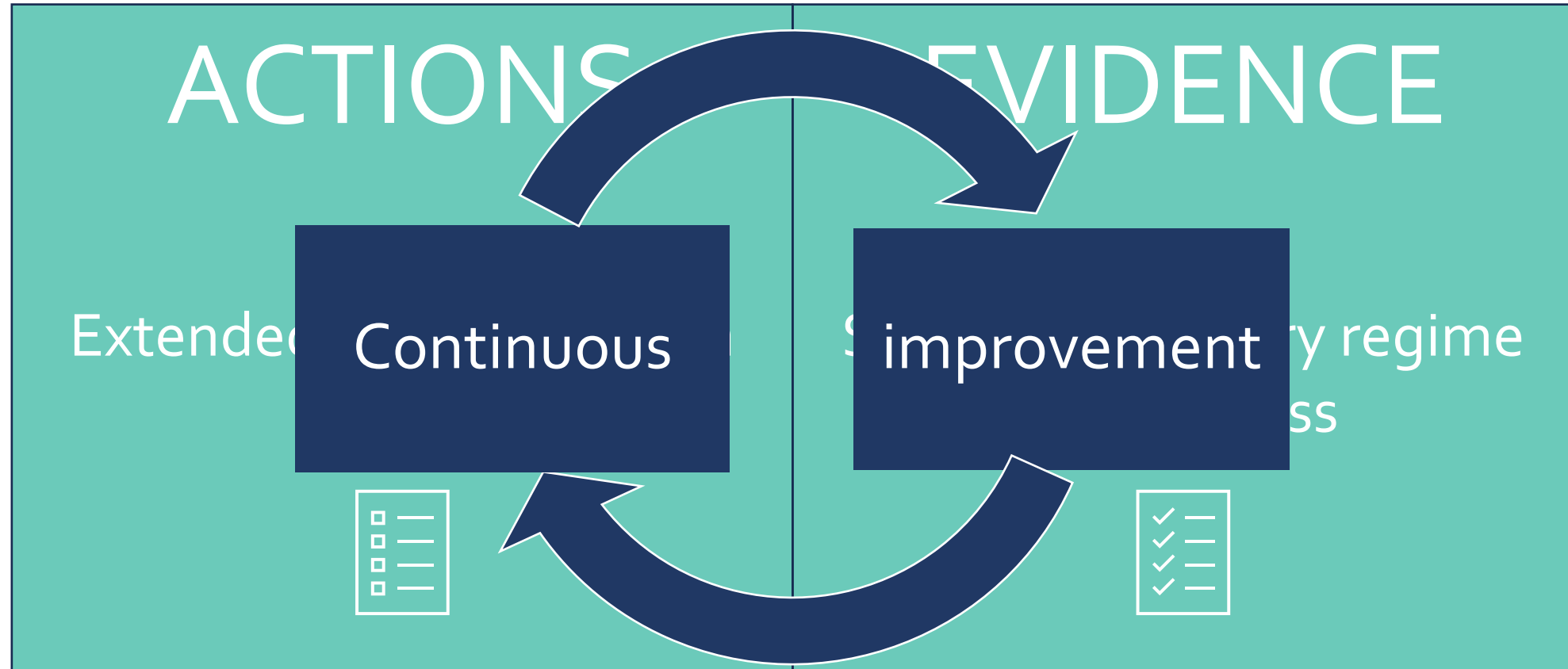
NIS2D-LTU – Implementation in Council



NIS2D-LTU – Implementation in Council



NIS2D-LTU – Implementation in Council



NIS2D-LTU – The essence

