.ie We are
Ireland online

Policy Advisory Committee

15 April 2021

Meeting - PAC#27

Policy Advisory Committee - Agenda

1. Membership Matters
2. Minutes from the PAC#26 meeting
3. Matters arising
4. NIS 2 – Role for the PAC ?
5. Update on the handling of online abuse
6. Any Other Business
7. Next Meeting

1. Membership Matters

- Please keep **microphones muted** throughout the call
- Please **“raise a hand”** to ask a question or **add comments** in the chat box
- Request to allow the meeting be **recorded** to assist with minute drafting
  - Recording will deleted once the Minutes are approved by PAC

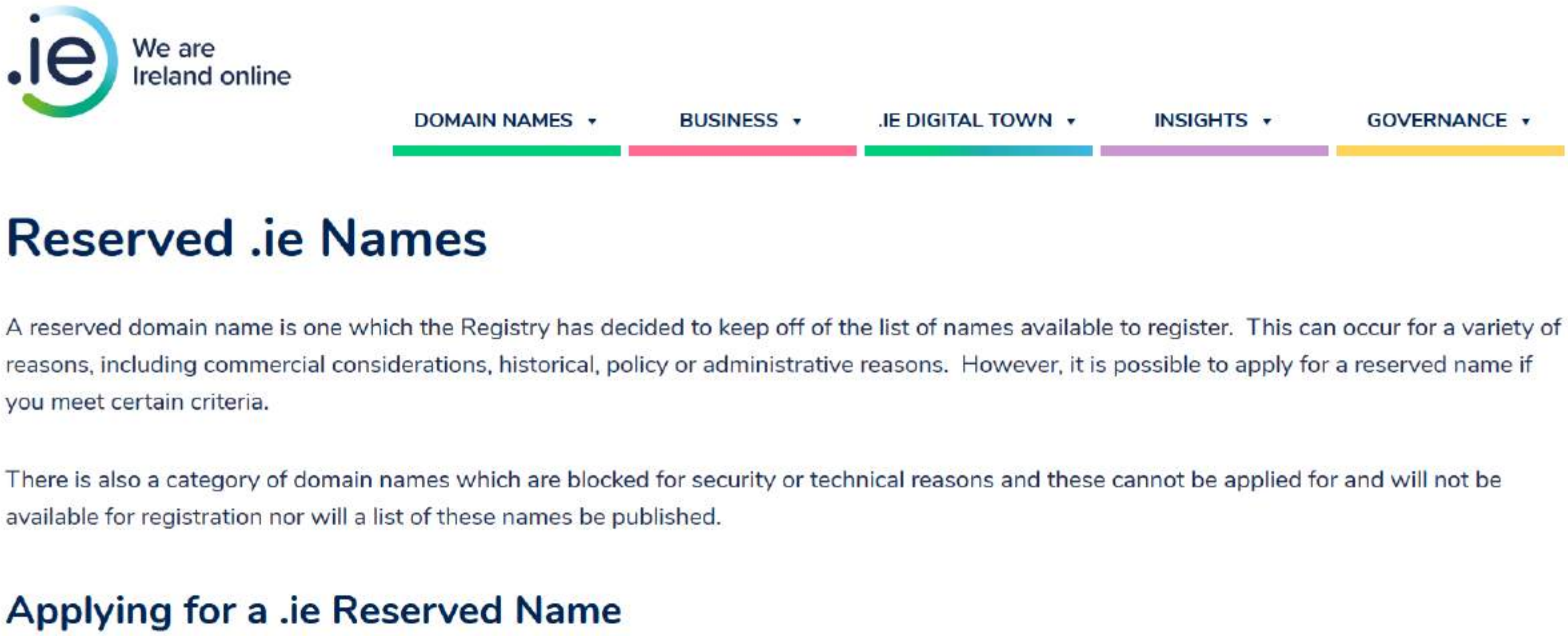
2. Minutes of the PAC #25 Meeting

- Meeting minutes are circulated to the membership within one week of each meeting
- Comments/feedback accepted over a two week period
- If clarifications/edits are requested, and consensus exists, these are reflected in the Minutes
- Meeting minutes, and supporting slides, are published on weare.ie after the comment period has ended
- Published online at https://www.weare.ie/policy-development-process/

3. Matters arising

- Policy change request relating to the handling of reserved/blocked names

  Update:- this went live on the .IE website on 1st March:-



Reserved .ie Names

A reserved domain name is one which the Registry has decided to keep off of the list of names available to register. This can occur for a variety of reasons, including commercial considerations, historical, policy or administrative reasons. However, it is possible to apply for a reserved name if you meet certain criteria.

There is also a category of domain names which are blocked for security or technical reasons and these cannot be applied for and will not be available for registration nor will a list of these names be published.

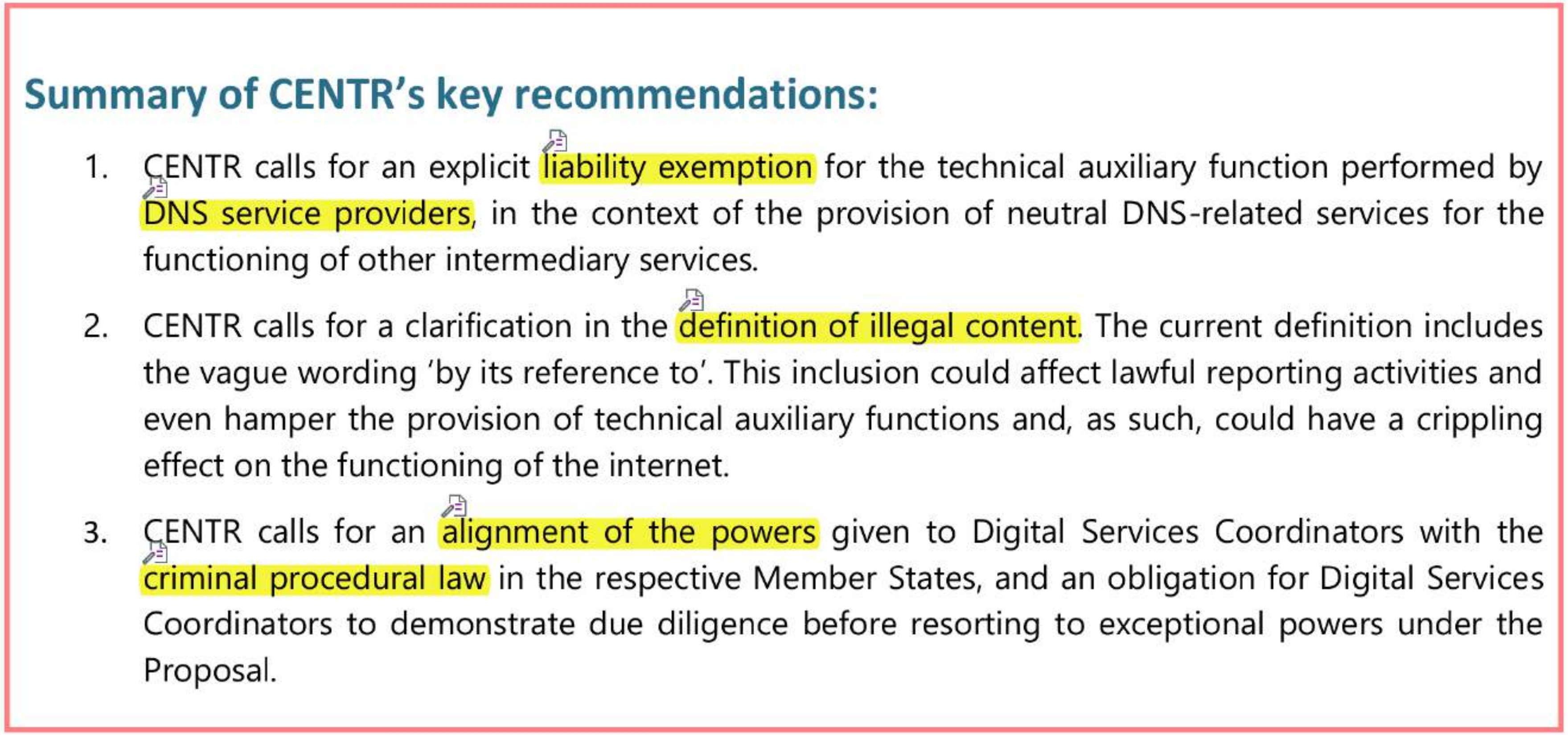
Applying for a .ie Reserved Name

- Next Step:- Policy Conclusion Template – at the next meeting

3. Matters arising

- Digital Services Act

Update:- .IE supported the CENTR submission on the DSA proposals



Summary of CENTR's key recommendations:

1. CENTR calls for an explicit liability exemption for the technical auxiliary function performed by DNS service providers, in the context of the provision of neutral DNS-related services for the functioning of other intermediary services.
2. CENTR calls for a clarification in the definition of illegal content. The current definition includes the vague wording 'by its reference to'. This inclusion could affect lawful reporting activities and even hamper the provision of technical auxiliary functions and, as such, could have a crippling effect on the functioning of the internet.
3. CENTR calls for an alignment of the powers given to Digital Services Coordinators with the criminal procedural law in the respective Member States, and an obligation for Digital Services Coordinators to demonstrate due diligence before resorting to exceptional powers under the Proposal.

.ie We are Ireland online

4. Update on handling of online abuse in the .ie namespace

Recap – the discussions:-

The topic was raised for discussion at the PAC#19 meeting:-

- ➢ In light of increased concerns of online abuse amongst all internet users
- ➢ National / International response focusing on **appropriate, effective, efficient abuse handling:-**
  - ▪ EU legislation (e.g. NIS, ENISA, Cybersecurity Act, CPC Regulation), "Notice & Action" etc.
  - ▪ Dept. of Communications - recent press release regarding social media and takedown legislation
- ➢ to identify the issues involved in developing an appropriate abuse handling strategy
- ➢ PAC split discussions into two work streams – **Technical Abuse** (5.1) and **Criminal Abuse** (5.2)

4. Update on handling of online abuse in the .ie namespace

Recap:- the challenges

- **Stopping abusive activity and removing illegal content**
  - Removal of the content from the Internet is the most *effective* way to avoid content being accessed.
  - Two parties have access to the content (or the device storing it): the **content publisher** and **hosting provider.**

- **What role have ccTLD operators played?**
  - Attempts to "block" abuse at the Registry-level usually result in domain registration **suspension/deletion**
  - Historically, ccTLD operators have taken action as **last resort** (in emergency/Court Order/Law Enforcement)

- **Challenges faced by Registry-level action:-**
  - the abusive content remains **available** (as only the host or content publisher can truly remove it)
  - such measures may have **unintended collateral damage**

4. Update on handling of online abuse in the .ie namespace

4.1. Technical abuse

Recommendation (PAC#24)

.IE and PAC acknowledged:

- **increases** in registration and technical abuse in other EU ccTLDs
  - particularly in light of the current Covid-19 situation, and the rise in e-commerce etc.
- need to ensure the **continued safety** of the .ie namespace for the Irish internet community
- intention to progress this work stream to **support the Registrar community** in its response to abuse

Consensus - PAC confirmed to issue a recommendation to the .IE Board for the Registry to:

- introduce a Netcraft-style, free, informational service for Registrars
- publish guidelines for Registrars outlining suggested actions to be taken

  (with the Registry working with PAC Registrar reps on word-crafting)

4. Update on handling of online abuse in the .ie namespace

Update

- ➢ Helpful guidelines for Registrars were finalized (drafted with PAC Registrar representatives input)
- ➢ These were circulated to the Registrar channel
- ➢ .IE Tech Services team worked with NetCraft to:-
    - review the practical considerations related to the implementation of the service
    - negotiate contractual T&Cs ….and costs to be paid by .IE
- ➢ Netcraft Service launched on 1st March

.ie We are Ireland online

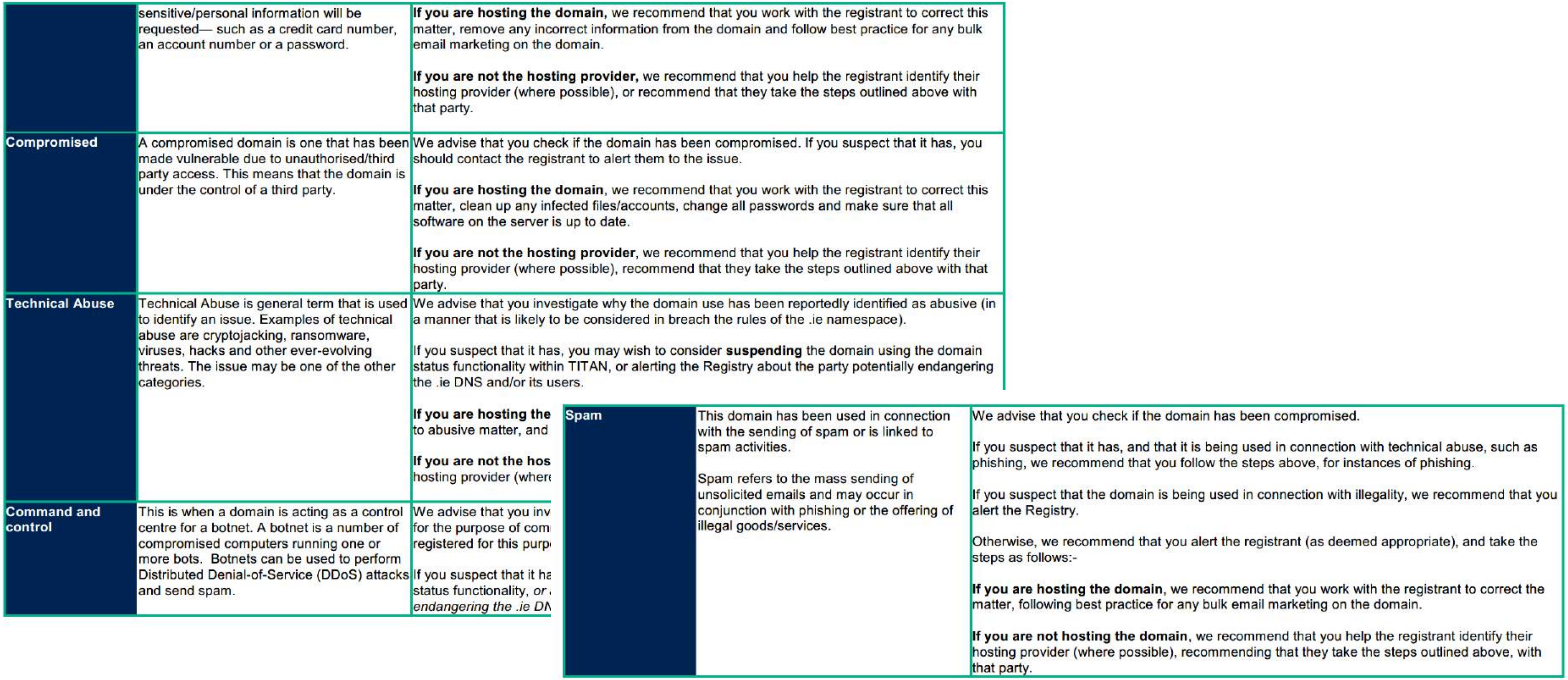
Guidelines for Registrars on handling reported .ie domain technical abuse

The guidelines below have been drafted to assist Registrars in handling reports of technical abuse relating to .ie domains under their management which they receive via the Netcraft reporting service, or otherwise.

The guidelines are not designed to be prescriptive. Registrars may have existing protocols in place, and may take any alternative/additional steps, and provide any advice that they deem appropriate in order to support the registrant in addressing and resolving the reported abusive issue.

If you suspect that a domain is being used in a way which breaches the rules of the .ie namespace, or presents a risk / danger to the .ie DNS or its users, you may use the domain status functionality within the Registry's TITAN systems to temporarily remove the .ie domain in question from the zone whilst you investigate the matter. These domain status features are subject to certain fair use rules, which are detailed here.

Abuse Category	Description	Recommended Action Steps
Malware	Malware refers to software that is used/distributed with malicious intent. It is used by cyber attackers to gain access or cause damage to a computer or network, and/or to gather sensitive/personal information.	We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue. **If you are hosting the domain**, we recommend that you work with the registrant to clean up any infected files/accounts, change all passwords and make sure that all software on the server is up to date. **If you are not the hosting provider**, we recommend that you help the registrant identify their hosting provider (where possible), and recommend they take the above steps with that party.
Phishing	Phishing is a method of collecting personal information using deceptive e-mails and websites. Phishing messages usually appear to come from well-known organisations. The messages will typically ask a user to click on a link which brings them to a fake site that appears to be legitimate where important	We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue. If you suspect that the domain is being used in connection with illegality, we recommend that you alert the registry. Otherwise, we recommend that you alert the registrant (as deemed appropriate), and take the steps outlined below:



	sensitive/personal information will be requested— such as a credit card number, an account number or a password.	**If you are hosting the domain,** we recommend that you work with the registrant to correct this matter, remove any incorrect information from the domain and follow best practice for any bulk email marketing on the domain. **If you are not the hosting provider,** we recommend that you help the registrant identify their hosting provider (where possible), or recommend that they take the steps outlined above with that party.
Compromised	A compromised domain is one that has been made vulnerable due to unauthorised/third party access. This means that the domain is under the control of a third party.	We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue. **If you are hosting the domain**, we recommend that you work with the registrant to correct this matter, clean up any infected files/accounts, change all passwords and make sure that all software on the server is up to date. **If you are not the hosting provider**, we recommend that you help the registrant identify their hosting provider (where possible), recommend that they take the steps outlined above with that party.
Technical Abuse	Technical Abuse is general term that is used to identify an issue. Examples of technical abuse are cryptojacking, ransomware, viruses, hacks and other ever-evolving threats. The issue may be one of the other categories.	We advise that you investigate why the domain use has been reportedly identified as abusive (in a manner that is likely to be considered in breach the rules of the .ie namespace). If you suspect that it has, you may wish to consider **suspending** the domain using the domain status functionality within TITAN, or alerting the Registry about the party potentially endangering the .ie DNS and/or its users. **If you are hosting the** to abusive matter, and **If you are not the hos** hosting provider (where
Command and control	This is when a domain is acting as a control centre for a botnet. A botnet is a number of compromised computers running one or more bots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks and send spam.	We advise that you inv for the purpose of com registered for this purp If you suspect that it ha status functionality, *or endangering the .ie DN*

Spam	This domain has been used in connection with the sending of spam or is linked to spam activities. Spam refers to the mass sending of unsolicited emails and may occur in conjunction with phishing or the offering of illegal goods/services.	We advise that you check if the domain has been compromised. If you suspect that it has, and that it is being used in connection with technical abuse, such as phishing, we recommend that you follow the steps above, for instances of phishing. If you suspect that the domain is being used in connection with illegality, we recommend that you alert the Registry. Otherwise, we recommend that you alert the registrant (as deemed appropriate), and take the steps as follows:- **If you are hosting the domain**, we recommend that you work with the registrant to correct the matter, following best practice for any bulk email marketing on the domain. **If you are not hosting the domain**, we recommend that you help the registrant identify their hosting provider (where possible), recommending that they take the steps outlined above, with that party.

4. Update on handling of online abuse in the .ie namespace

Early feedback on Netcraft service….redacted

4. Update on handling of online abuse in the .ie namespace

Early feedback on Netcraft service….redacted

4. Update on handling of online abuse in the .ie namespace

4.2. Criminal Abuse

- Discussions have focused on potential introduction of a cooperative arrangement with the Garda National Cyber Crime Bureau (GNCCB)

- GNCCB contacted .IE prior to PAC discussion requesting the introduction of such an arrangement

- .IE raised suggestion for PAC input:
    - Some members commented that they felt .IE should be prepared to act responsibly and have a protocol in place to address serious, criminal abuse, if/when it arises.
    - Other members questioned whether there was a genuine need for such an arrangement

- Representatives from GNCCB and Economic Crime Bureau (GNECB) presented at PAC#23 on:
    - what problems they are having with tackling online abuse (particularly with .ie names)
    - which crimes they wish to tackle via a cooperative arrangement
    - what frictions they’re experiencing with “normal” channels for suspension/takedown

4. Update on handling of abuse in the .ie namespace

The GNCCB/GNECB representatives also noted that **reactive policing** efforts operate relatively effectively:

- no notable abuse concerns within the .ie namespace
- no notable friction with existing takedown and suspension procedures
- ISPs typically act responsively and responsibly in response to requests from the GNCCB and GNECB

They commented on a shift to **proactive, preventative** policing:

- to combat the tech-savvy nature of criminals (adapting promptly to site takedowns)
- to protect legitimate internet users from becoming victims of serious, life-altering crime

Regarding a potential **Cooperative Arrangement:**

- They acknowledged the important value of a potential arrangement
- Noted that it should be a structured process with appropriate **safeguards** that meet the needs of all stakeholders, and operate in a manner which is mutually beneficial
- Would potentially be used where hosts had failed to address the issue

4. Update on the handling of online abuse in the .ie namespace

Recommendation (PAC#24)

PAC agreed that there was **consensus**:-

- to re-visit the draft protocol arrangement,
- to revise this to ensure the safeguards identified are included
- to circulate this revised edition to the representative from the GNCCB for discussion purposes, and
- to revert to the PAC with the GNCCB feedback in due course

Updates and **Next Steps:**

- PAC proposed edits were applied to the draft protocol arrangement
- Circulated to the wider Registrar channel, with a request for feedback & experiences
- Further updates will be provided at the next PAC meeting

5. NIS2 – Role for the PAC ?

Overview:

NIS 2018:-

- The main objective of the NIS Directive is to ensure that there is a common high level security of network and information systems (NIS) across Member States

Roinn Cumarsáide, Gníomhaithe
ar son na hAeráide & Comhshaoil
Department of Communications,
Climate Action & Environment

NATIONAL CYBER SECURITY CENTRE
NCSC

NIS 2:-

- Impact on domain name channel partners ?

- Impact on Ireland Inc ?

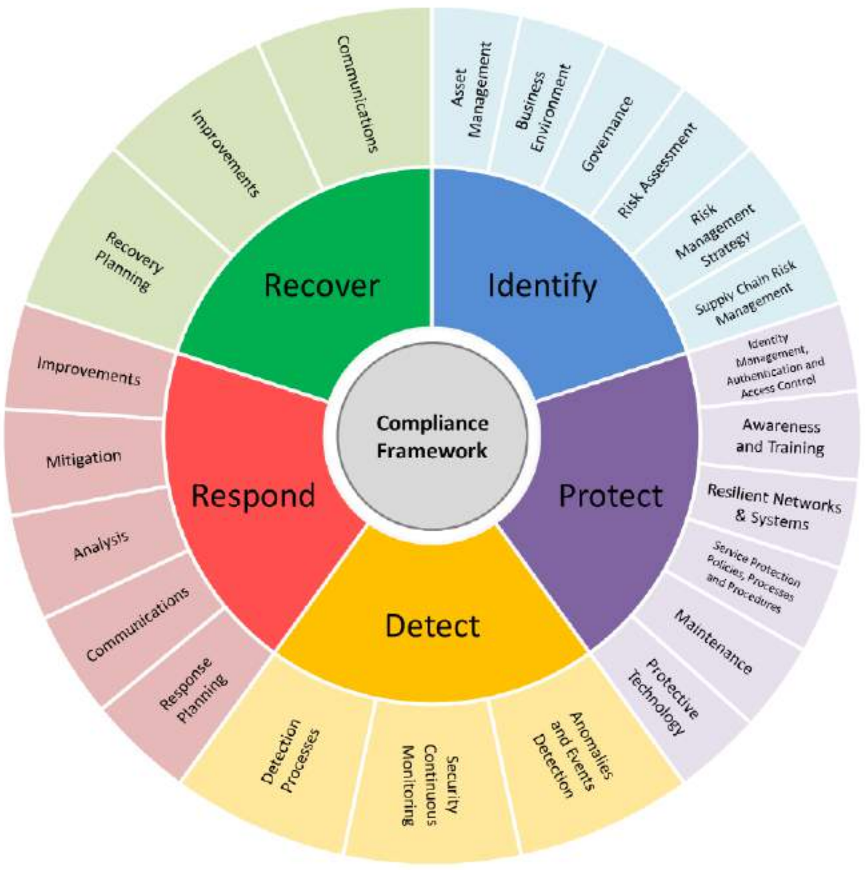
5. NIS2 – Role for the PAC ?

NIS 2018:-

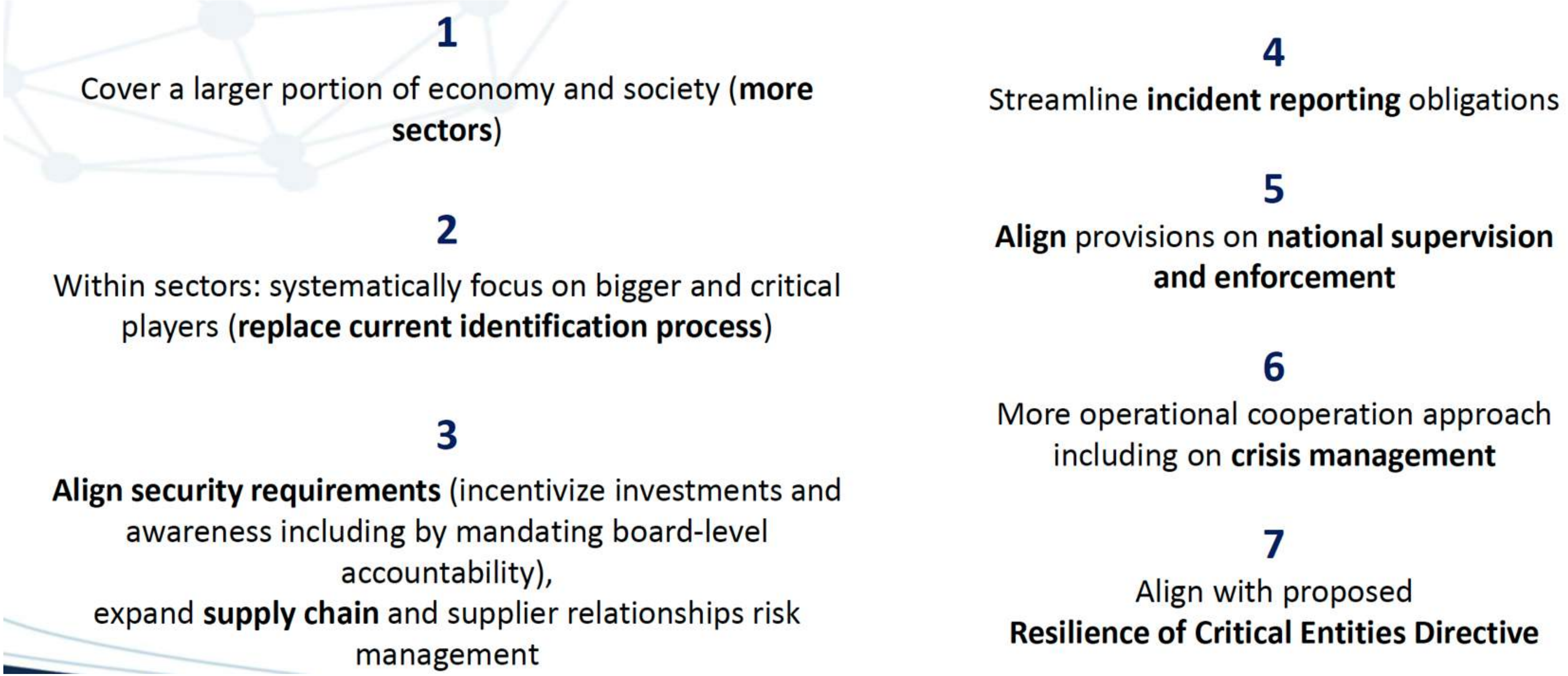
Regulation 17(1) provides that Operators of Essential Services shall –

- take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which it uses in its operations, and
- take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used by it for the provision of the essential services in respect of which it is designated as an operator of essential services with a view to ensuring the continuity of the provision by it of those services.

Appendix A: Framework Infographic



5. NIS2 – Role for the PAC ?
NIS2 vision - main objectives



1

Cover a larger portion of economy and society (**more sectors**)

2

Within sectors: systematically focus on bigger and critical players (**replace current identification process**)

3

Align security requirements (incentivize investments and awareness including by mandating board-level accountability),
expand **supply chain** and supplier relationships risk management

4

Streamline **incident reporting** obligations

5

Align provisions on **national supervision and enforcement**

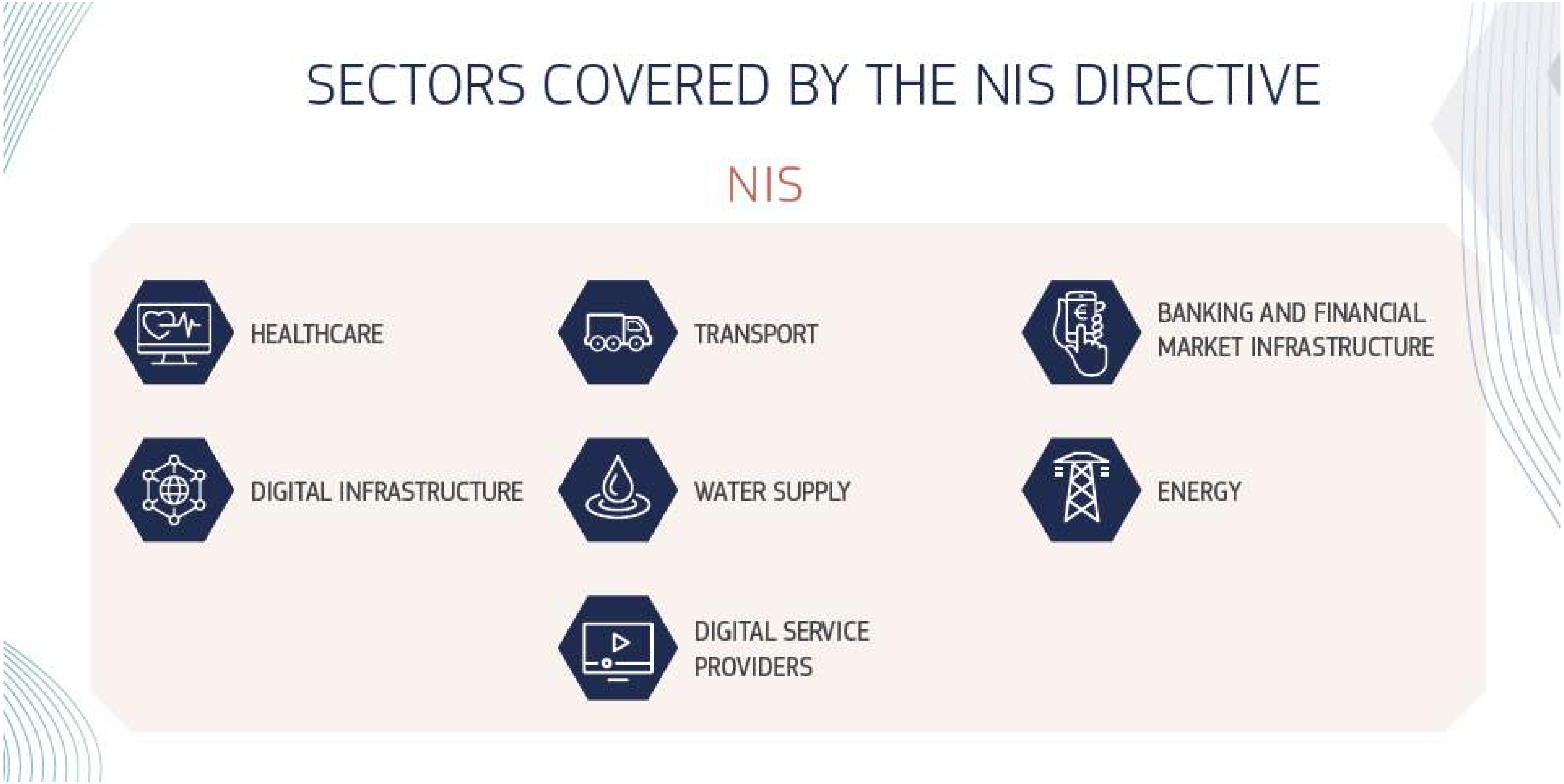
6

More operational cooperation approach including on **crisis management**

7

Align with proposed
Resilience of Critical Entities Directive

5. NIS2 – Role for the PAC ?

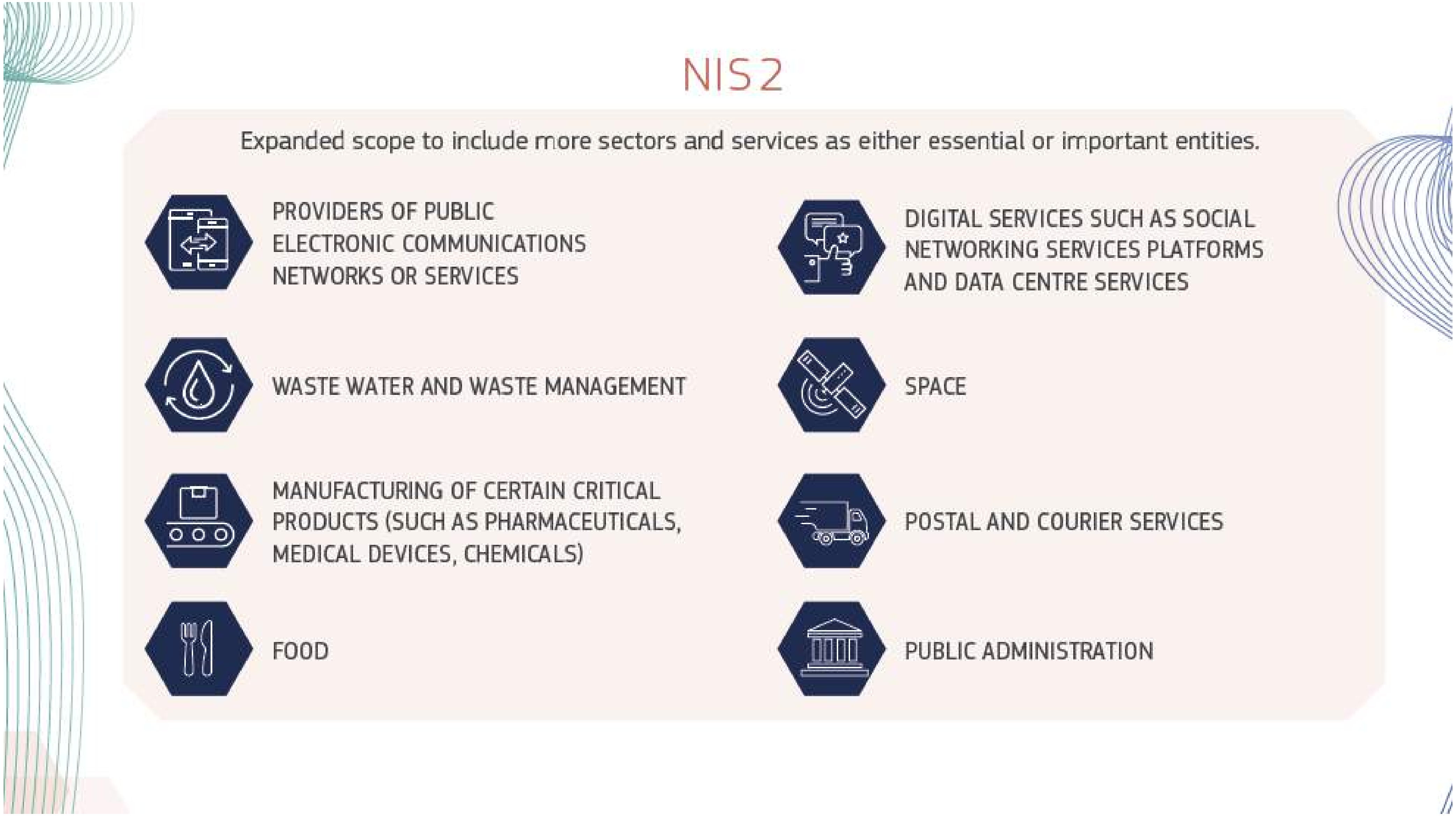


SECTORS COVERED BY THE NIS DIRECTIVE

NIS

- HEALTHCARE
- TRANSPORT
- BANKING AND FINANCIAL MARKET INFRASTRUCTURE
- DIGITAL INFRASTRUCTURE
- WATER SUPPLY
- ENERGY
- DIGITAL SERVICE PROVIDERS

5. NIS2 – Role for the PAC ?



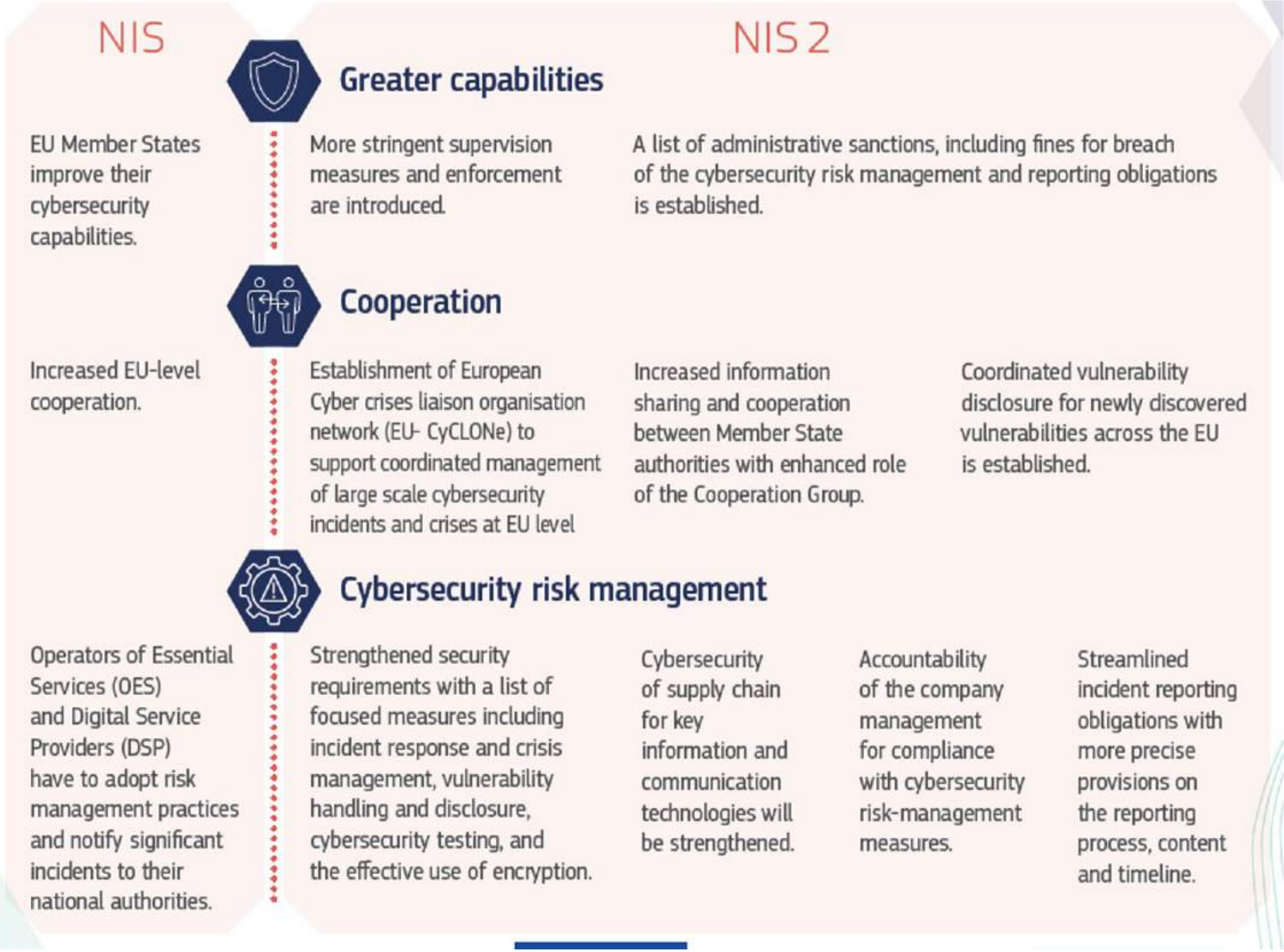
NIS2

Expanded scope to include more sectors and services as either essential or important entities.

- PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES
- DIGITAL SERVICES SUCH AS SOCIAL NETWORKING SERVICES PLATFORMS AND DATA CENTRE SERVICES
- WASTE WATER AND WASTE MANAGEMENT
- SPACE
- MANUFACTURING OF CERTAIN CRITICAL PRODUCTS (SUCH AS PHARMACEUTICALS, MEDICAL DEVICES, CHEMICALS)
- POSTAL AND COURIER SERVICES
- FOOD
- PUBLIC ADMINISTRATION

We are
Ireland online

5. NIS2 – Role for the PAC ?



NIS

NIS 2

Greater capabilities

EU Member States improve their cybersecurity capabilities.

More stringent supervision measures and enforcement are introduced.

A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established.

Cooperation

Increased EU-level cooperation.

Establishment of European Cyber crises liaison organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level

Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation Group.

Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established.

Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

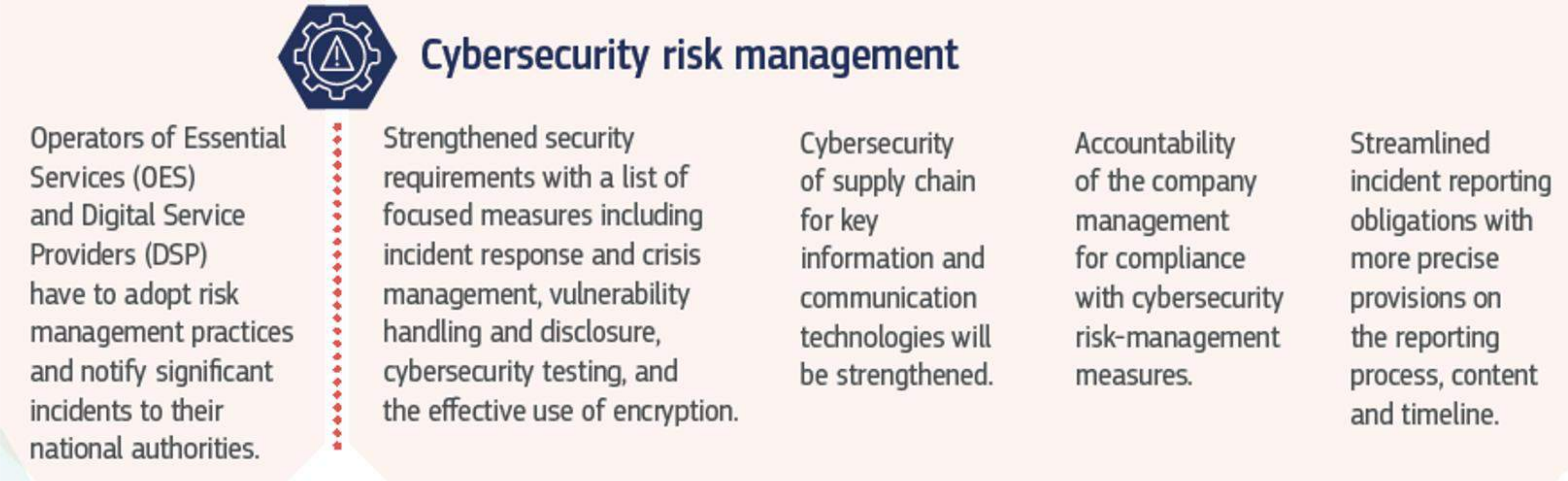
Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

5. NIS2 – Role for the PAC ?



Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

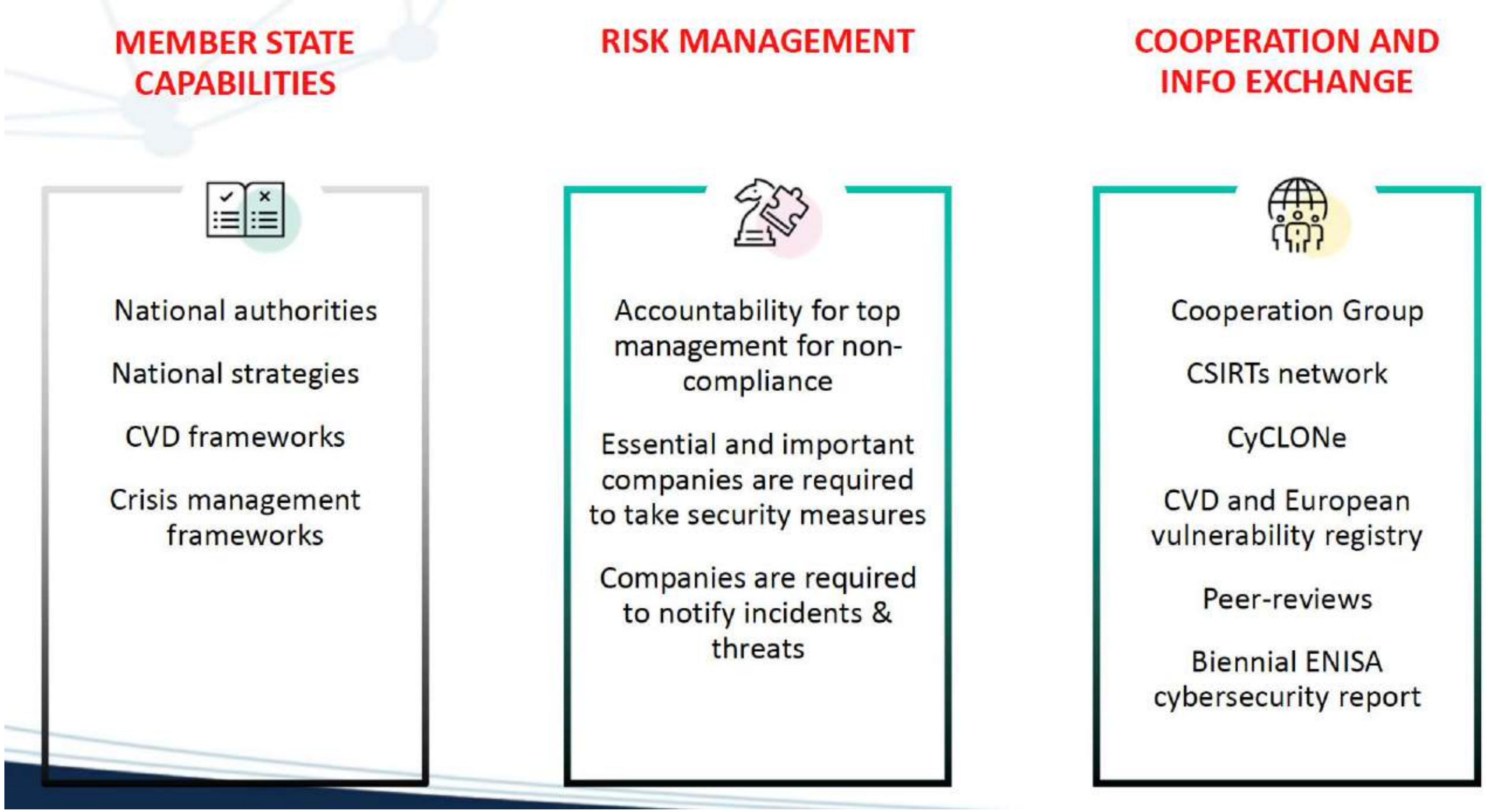
Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

5. NIS2 – Role for the PAC ?
Three main pillars of the proposal for NIS 2



MEMBER STATE CAPABILITIES

National authorities

National strategies

CVD frameworks

Crisis management frameworks

RISK MANAGEMENT

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify incidents & threats

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

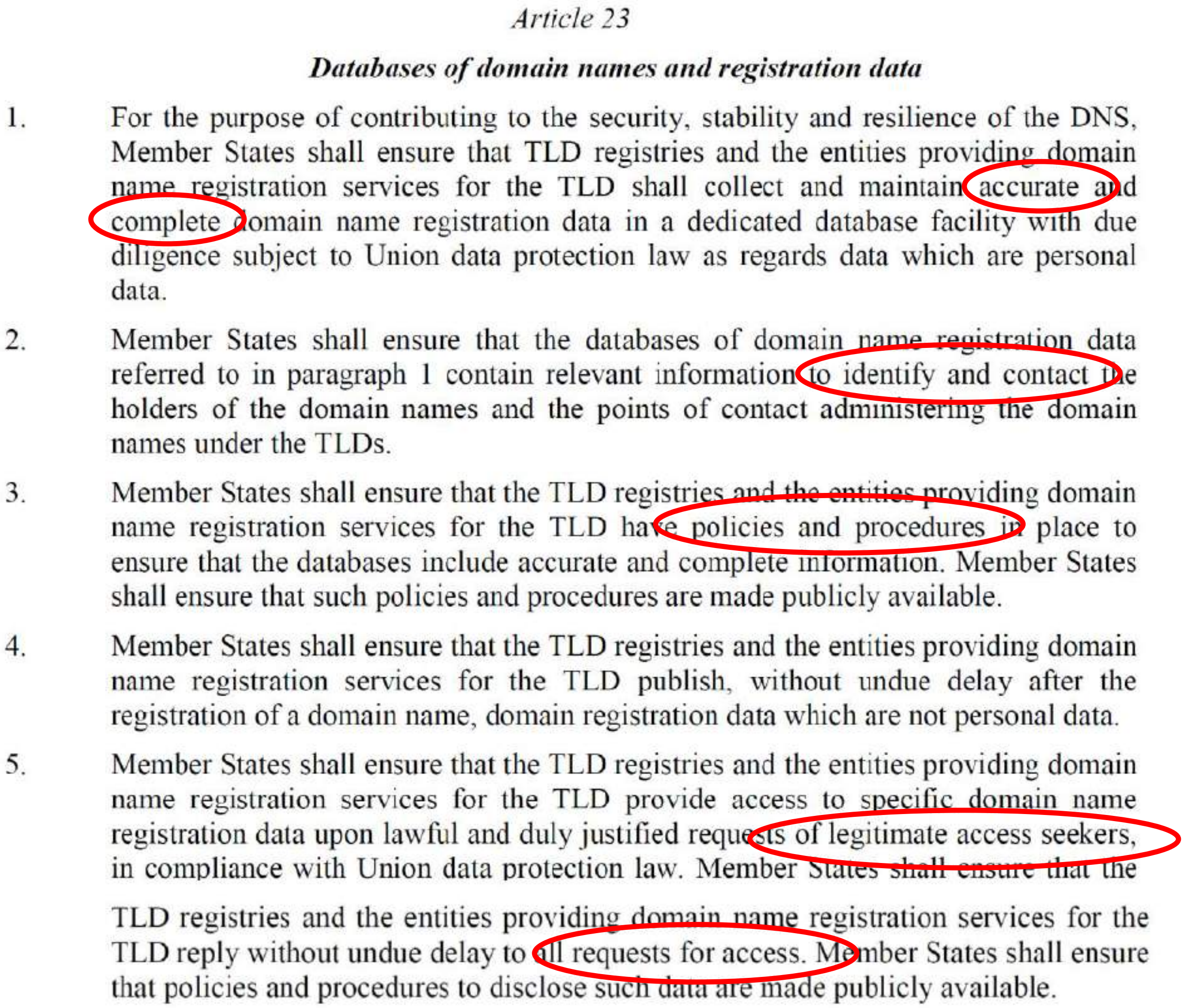
CVD and European vulnerability registry

Peer-reviews

Biennial ENISA cybersecurity report

5. NIS2 – Role for the PAC ?

NIS 2 – implications for data accuracy & completeness



Article 23

Databases of domain names and registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.

5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

- What is accurate?
- What is complete?
- What is maintain?
- Who are legitimate access seekers?

We are
Ireland online

5. NIS2 – Role for the PAC ?

Relevance to .IE / Registrars / Registrants

- DNS
  - “Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend.”
  - “Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.”

5. NIS2 – Role for the PAC ?

- Open discussion…………….

- Role for the PAC ?

6. Any Other Business

6.1 Update on industry related developments/legislative changes

6.2 AOB

7. Next Meeting

Proposed date:

15th July 2021