РЕПУБЛИКА БЪЛГАРИЯ
Министерство на електронното управление

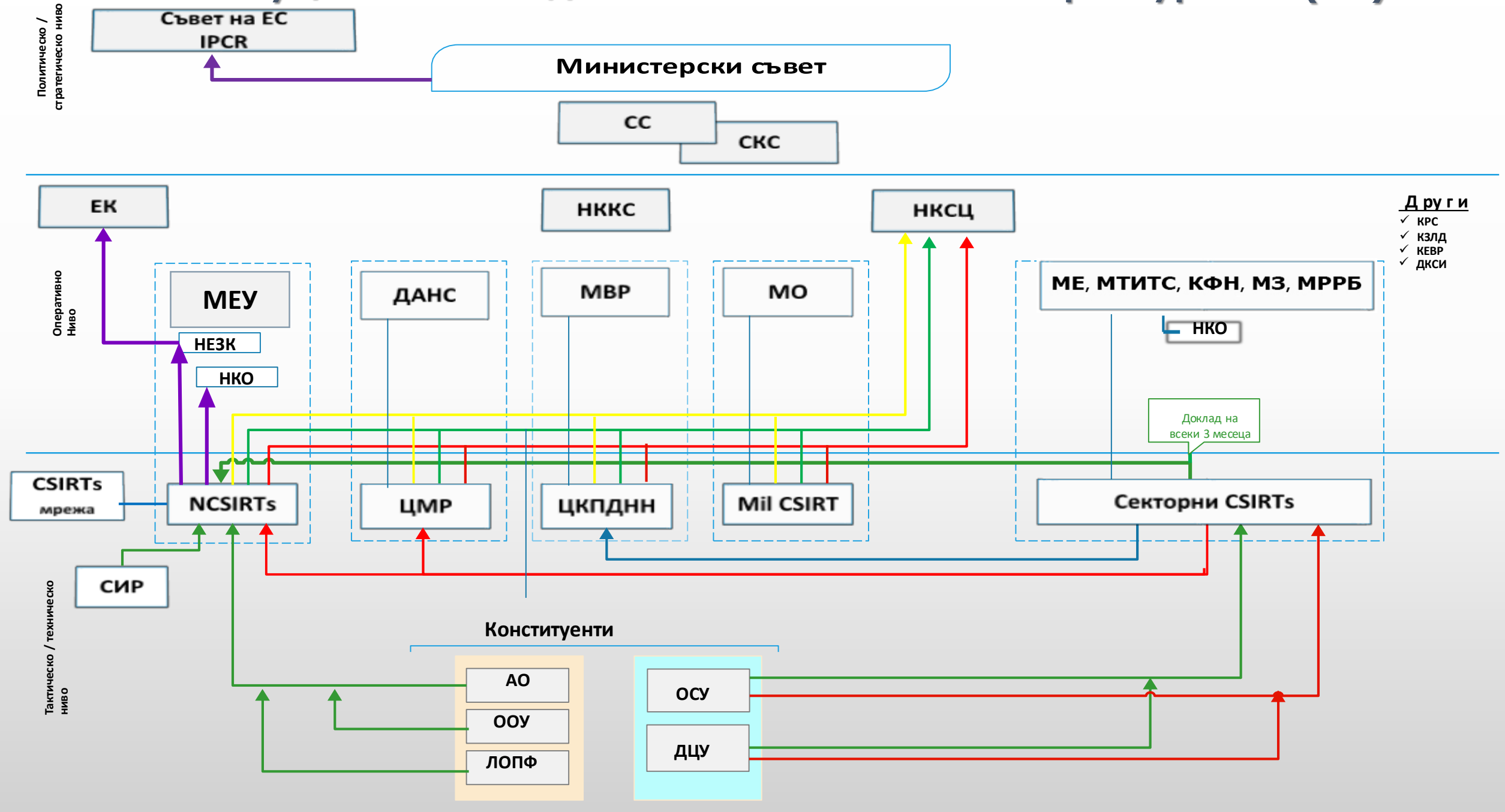

2024
ЗИД на ЗАКОН ЗА КИБЕРСИГУРНОСТ
2022
ДИРЕКТИВА (ЕС) 2022/2555
Регламент (ЕС) 2022/2554
от 14 декември 2022 година
2019
НАРЕДБА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
2018
ЗАКОН ЗА КИБЕРСИГУРНОСТ
2016
ДИРЕКТИВА (ЕС) 2016/1148 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА
от 6 юли 2016 година

Закон за киберсигурност

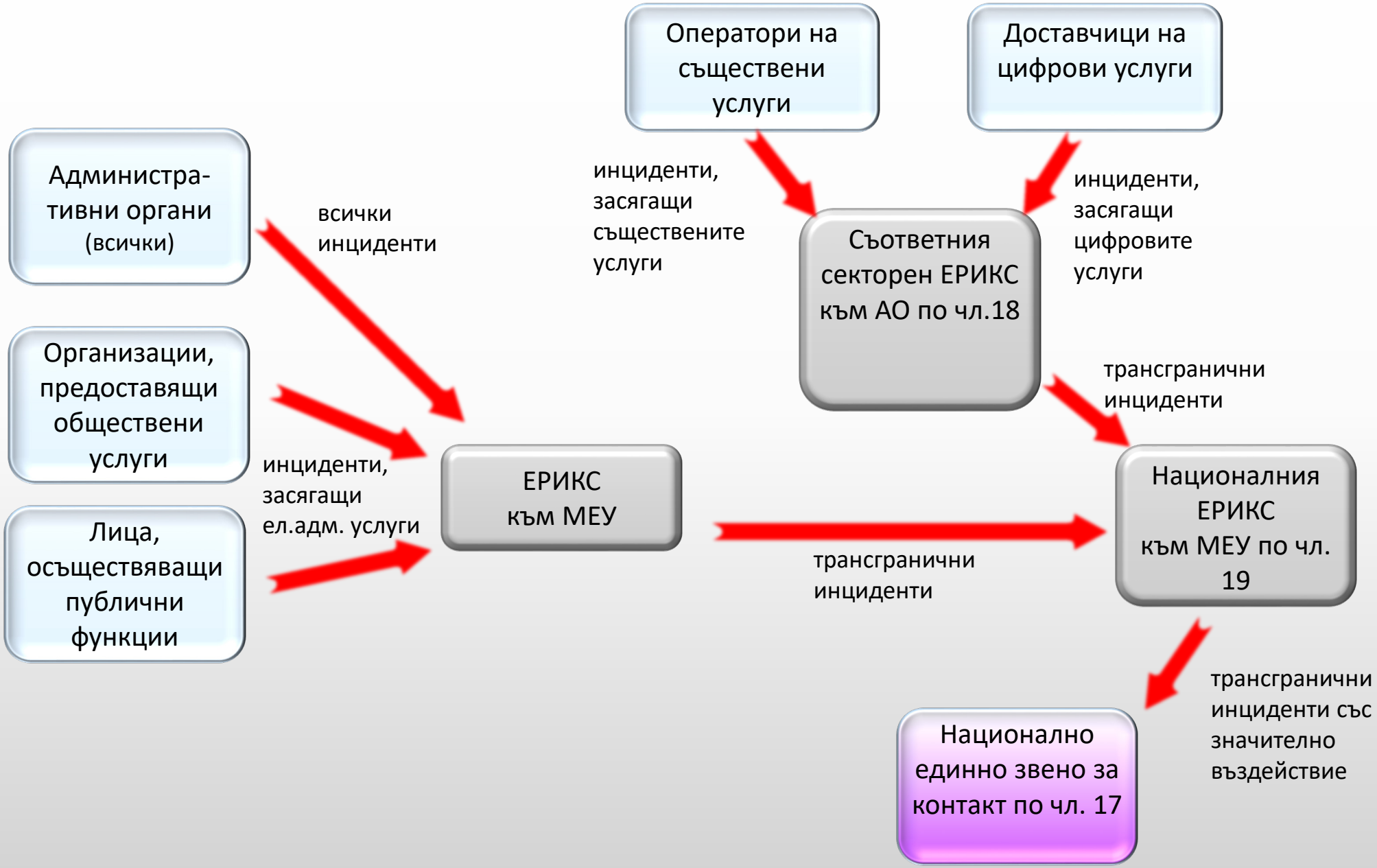
Този закон урежда:

- организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността;
- предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност.о

Институционален модел на системата за киберсигурност (КС)



Изискване за докладване на инциденти



АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ

При какви нарушения се налагат санкции?

- При неуведомяване за инциденти в срок и при предоставянето на недостатъчна информация (за определянето на инцидента като трансграничен);
- При непредоставяне на информация на НКО или неизпълнение на указания от НКО;
- При друго нарушение по Глава Втора (МИС).

От кого се издават наказателните постановления?

- Министъра на електронното управление;
- Ръководителите на административните органи по чл.16, към които се създават Националните компетентни органи;
- Министър на вътрешните работи;
- Председателя на Държавна агенция „Национална сигурност“.

NIS2


Cyber Security
Username
Remember me
Forgot password
LOGIN
Face ID
Data Protection
Data Information

Три основни стълба на МИС 2

Отговорност на ДЧ

Национални компетентни органи

Национални стратегии

Процедури за CVD

Рамки за управление на кризи

Управление на риска

- Отговорност на висшето ръководство за неспазване на изискванията
- От съществените и важните субекти се изисква да предприемат мерки за сигурност
- От субектите се изисква да уведомяват за инциденти в рамките на определен срок

ОТГОВОРНОСТИ НА СУБЕКТИТЕ

СЪТРУДНИЧЕСТВО И ОБМЕН НА ИНФОРМАЦИЯ

Cooperation Group

CSIRTs Network

CyCLONe

CVD and European Vulnerability registry

Peer-reviews

Двугодишен доклад на ENISA за киберсигурността

Съществени и важни субекти

Субектите могат да бъдат определени като "съществени" или "важни" в зависимост от фактори като размер, сектор и критичност.

Класификационна схема

Въвеждане на **горна граница на размера** с концепцията за:

- **Големи субекти:**
  - най-малко **250 служителя**
  - или **50 млн. евро оборот**
- **Средни субекти:**
  - най-малко **50 служителя**
  - или **10 млн. евро** оборотr

→ **По подразбиране в „Обхват“**

Държавите членки могат да идентифицират ‘малки по големина субекти’

- С **висок рисков профил**
- Или когато са **единствен доставчик на услуги**.

ПРИЛОЖЕНИЕ I - СЕКТОРИ С ВИСОКА СТЕПЕН НА КРИТИЧНОСТ

Съществени и важни субекти

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: public transport: ***only*** if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
BANKING	Credit institutions **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
HEALTH	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: entities holding a distribution authorization for medicinal products: ***only*** if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
WASTE WATER	(***only*** if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Of regional governments: risk based. (Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

ПРИЛОЖЕНИЕ II -ДРУГИ КРИТИЧНИ СЕКТОРИ

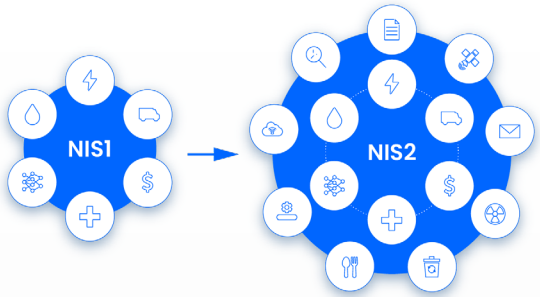
SECTOR	SUB-SECTOR	LARGE ENTITIES (>=250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES
POSTAL AND COURIER SERVICES		IMPORTANT	IMPORTANT	NOT IN SCOPE
WASTE MANAGEMENT	(***only*** if principal economic activity)	IMPORTANT	IMPORTANT	NOT IN SCOPE
CHEMICALS	Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
FOOD	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
MANUFACTURING	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)	IMPORTANT	IMPORTANT	NOT IN SCOPE
DIGITAL PROVIDERS	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
RESEARCH	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES	All sizes, but only subject to Article 3(3) and Article 28			

Забележки:

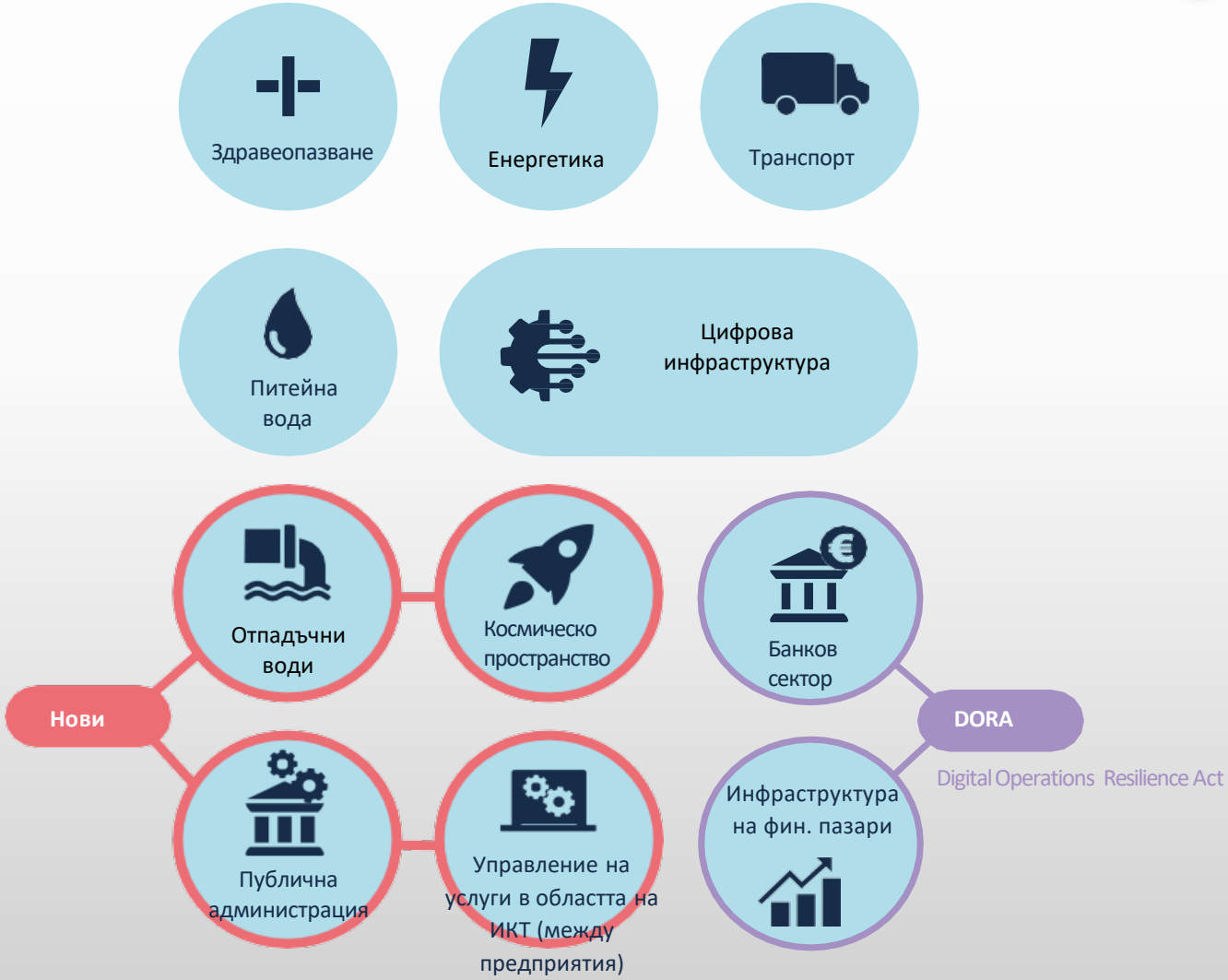
Субекти, определени като критични субекти съгласно Директива (ЕС) 2022/2557 (Директива за СЕР), се считат за съществени субекти съгласно NIS2. Lex Specialis може да се прилага, когато секторните разпоредби са поне еквивалентни.

Съществуват някои изключения от горното ръководство, моля, направете справка в текста на Директивата за пълен и изчерпателен списък на всички изключения.

МИС 2 Обхват



Приложение 1 - Сектори с висока степен на критичност



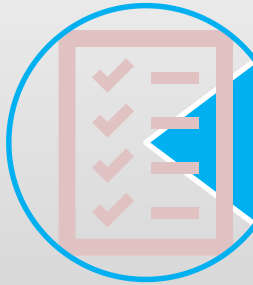
Приложение 2 - Други критични сектори

Задължения за докладване (чл. 23)

Съществените и важни субекти уведомяват CSIRT за значителни инциденти.

- **<24h ранно предупреждение.**
- **<72h първоначална оценка на инцидента.**
- **<1 месец окончателен доклад с подробно описание.**

CSIRT трябва да предоставят отговор на основния и важен субект (<24 часа) и да **предоставят насоки за мерки за смекчаване.** Когато е уместно, те ще препращат информацията до единното звено за контакт на други ДЧ



Комисията може да приема актове за изпълнение, в които допълнително се уточняват видът на информацията, форматът и процедурата

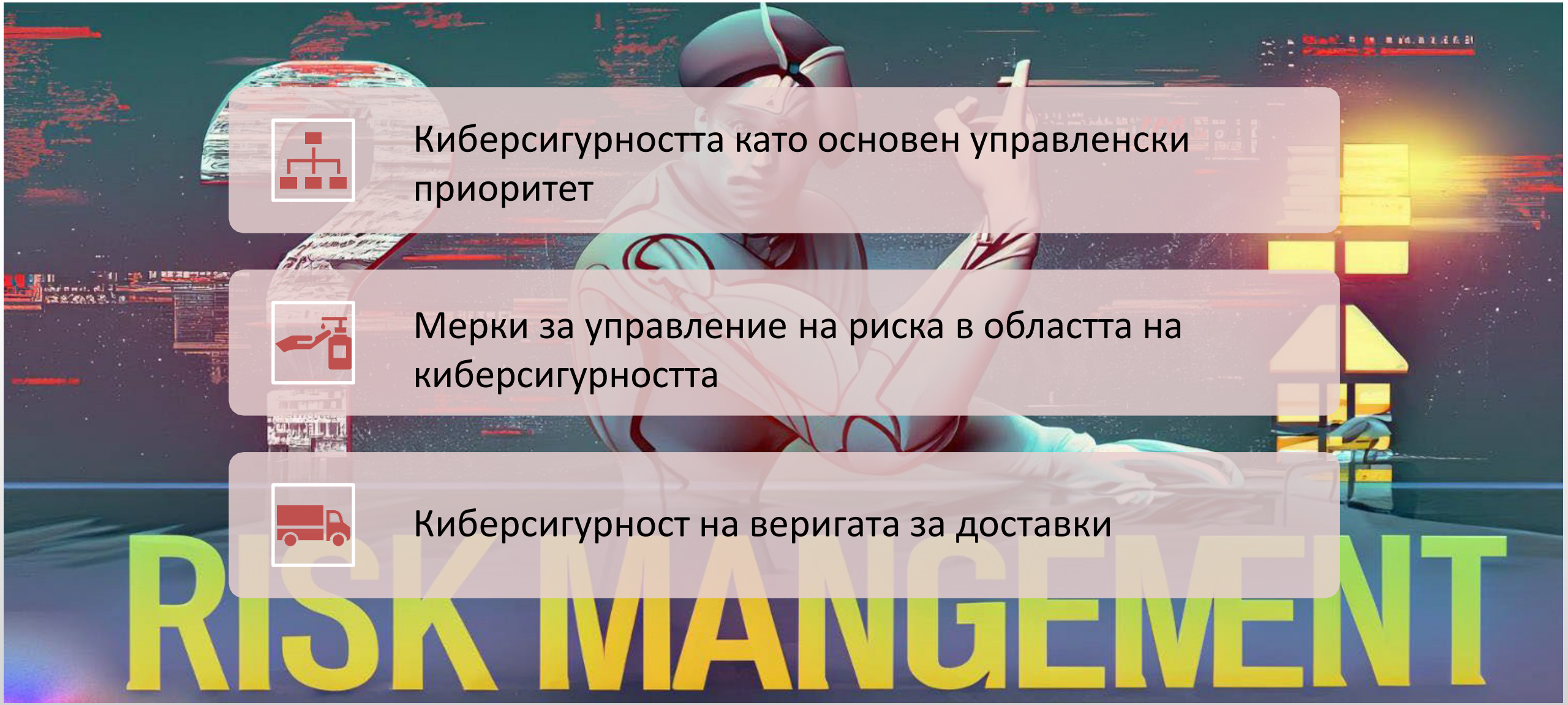
Значителен инцидент

Даден инцидент се счита за **значителен**, ако:

а) е причинил или е в състояние да причини сериозно оперативно смущение в услугите или финансова загуба за засегнатия субект;

б) е засегнал или е в състояние да засегне други физически или юридически лица, причинявайки значителни материални или нематериални вреди.

Управление и мерки за сигурност



- Киберсигурността като основен управленски приоритет
- Мерки за управление на риска в областта на киберсигурността
- Киберсигурност на веригата за доставки

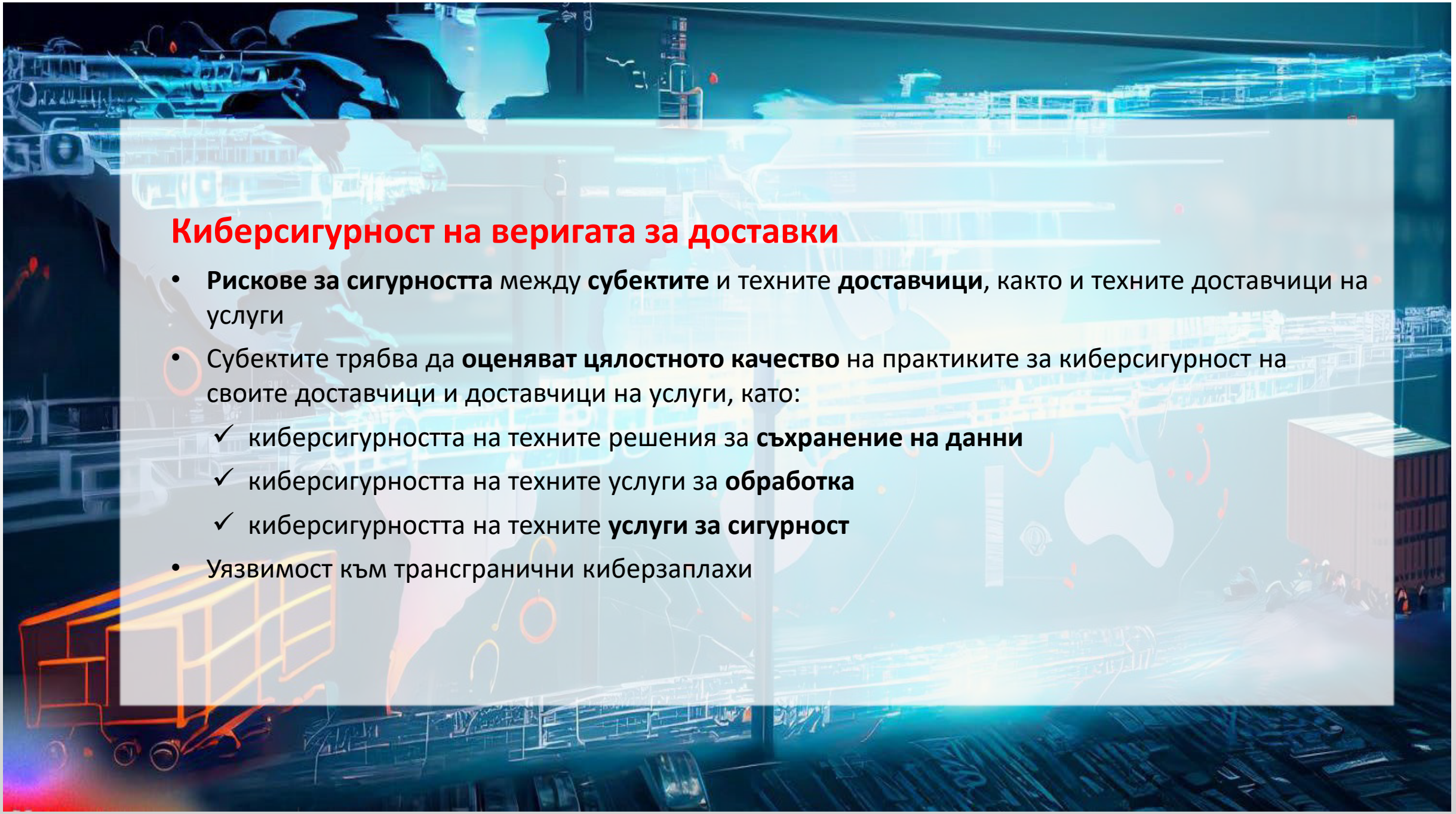
Управителните органи на субектите трябва да :

- да одобрят мерките за киберсигурност;
- да преминават обучение по киберсигурност;
- предлагат подобно обучение на служителите.

Мерки за управление на риска за киберсигурността

Такива мерки се основават на подход, основан на всички рискове, който има за цел да защити мрежата и информационните системи и физическата среда на тези системи от инциденти, и трябва да включват най-малко следното:

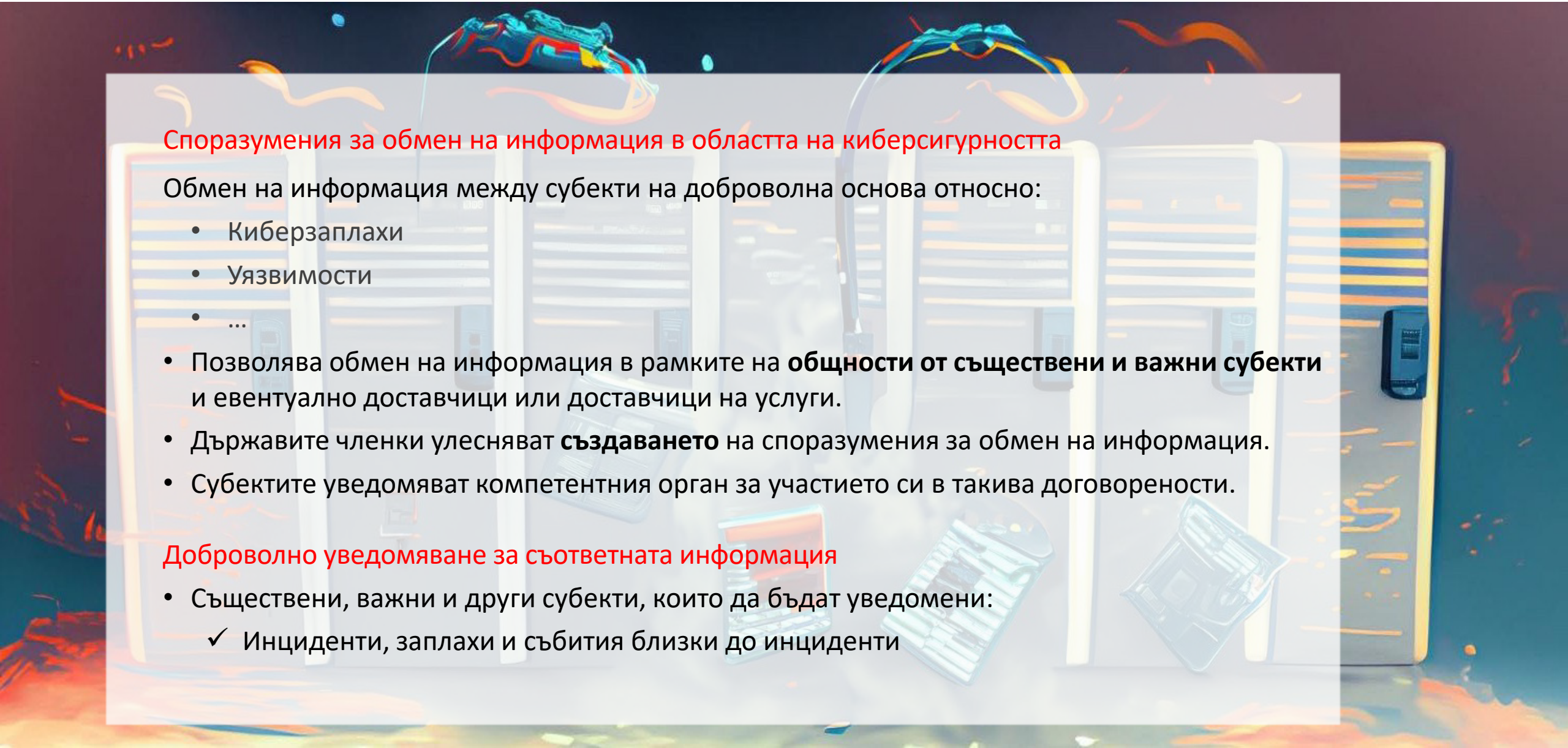
Анализ на риска и сигурност на информационните системи	Политики и процедури за оценка на ефективността на мерките за управление на риска в областта на киберсигурността
Управление на инциденти	Основна компютърна хигиена и обучения
Мерки за непрекъсваемост на дейността (резервни копия, възстановяване след бедствие, управление на кризи)	Политики за подходящо използване на криптографията и криптирането
Сигурност на веригата за доставки	Сигурност на човешките ресурси, политики за контрол на достъпа и управление на активите
Сигурност при придобиването, разработването и поддръжката на системи, включително обработка и разкриване на уязвимости	Използване на многофакторна, защитена гласова/видео/текстова комуникация и защитена спешна комуникация



Киберсигурност на веригата за доставки

- **Рискове за сигурността** между **субектите** и техните **доставчици**, както и техните доставчици на услуги
- Субектите трябва да **оценяват цялостното качество** на практиките за киберсигурност на своите доставчици и доставчици на услуги, като:
  - ✓ киберсигурността на техните решения за **съхранение на данни**
  - ✓ киберсигурността на техните услуги за **обработка**
  - ✓ киберсигурността на техните **услуги за сигурност**
- Уязвимост към трансгранични киберзаплахи

Споделяне на информация



Споразумения за обмен на информация в областта на киберсигурността

Обмен на информация между субекти на доброволна основа относно:

- Киберзаплахи
- Уязвимости
- …

- Позволява обмен на информация в рамките на **общности от съществени и важни субекти** и евентуално доставчици или доставчици на услуги.
- Държавите членки улесняват **създаването** на споразумения за обмен на информация.
- Субектите уведомяват компетентния орган за участието си в такива договорености.

Доброволно уведомяване за съответната информация

- Съществени, важни и други субекти, които да бъдат уведомени:
  - ✓ Инциденти, заплахи и събития близки до инциденти

Надзор

Компетентният орган може да:

да извършва одити, инспекции, да изисква информация,... И:

- да издава предупреждения а
- задължителни инструкции
- Да разпорежда на субектите да информират клиентите си за киберзаплахите

Ако прилагането е неефективно:

- Временно да спре сертифицирането или разрешаването на съответните услуги

- Налагане на санкции

Важно!

Санкциите не се дължат на настъпил инцидент!

Изпълнение и санкции

NIS2 предоставя на националните органи минимален списък от правомощия за прилагане на законодателството при неспазване на изискванията, включително:

- Издаване на предупреждения за неспазване на изискванията
- Издаване на задължителни указания
- Нареждане за преустановяване на поведение, което не е в съответствие с изискванията
- Нареждане за привеждане в съответствие на мерките за управление на риска или задълженията за докладване по определен начин и в рамките на определен срок
- Нареждане за информиране на физическо или юридическо лице (лица), на което (които) предоставят услуги или дейности, които са потенциално засегнати от значителна киберзаплаха
- Нареждане за изпълнение на препоръките, дадени в резултат на одит на сигурността, в разумен срок
- Определяне на служител по мониторинга с точно определени задачи за определен период от време, който да следи за спазването на изискванията
- Нареждане да се оповестят публично аспектите на несъответствието
- Налагане на административни глоби
- Сертифицирането на съществени субекти или разрешението, отнасящо се до услугата, може да бъде спряно, ако не е спазен крайният срок за предприемане на действия
- И на лицата, отговорни за изпълнението на управленски задължения на ниво главен изпълнителен директор или законен представител, може да бъде временно забранено да упражняват управленски

Санкции

Административни санкции

В случай на **неспазване на изискванията**:

- **Съществените субекти** са заплашени от глоба в размер до **€ 10 million** или **2% о**т глобалния годишен оборот
- **Важните субекти** са заплашени от глоба в размер до **€ 7 million** or **1,4% о**т глобалния годишен оборот

в зависимост от това коя от двете суми е по-висока.

DORA е Регламент.

Използва директно във всички страни от Европейския съюз.
Той влезе в сила на 16 януари 2023 г. и се прилага от 17 януари 2025 г..

NIS 2 е Директива.

Тя трябва да бъде въведена в националното законодателство чрез акт. Той също така дава свобода за по-точното му определяне на национално равнище. Крайният срок за изпълнение е 17 октомври 2024 г.

Прилики между DORA и NIS2

- **Обхват:** и двете рамки имат за цел да укрепят практиките за киберсигурност и устойчивост в организациите.
- **Действие:** те изискват от организациите да предприемат подходящи мерки за управление на рисковете и за предотвратяване или минимизиране на въздействието на киберинциденти.
- **Тестване:** и двете рамки изискват от организациите да провеждат редовно тестване, за да гарантират оперативната устойчивост и готовност срещу киберзаплахи.
- **Споделяне на информация:** и DORA, и NIS2 насърчават споделянето на информация и разузнавателни данни, свързани с инциденти в областта на киберсигурността.
- **Докладване:** те установяват задължения за докладване на значими инциденти в областта на киберсигурността, които засягат предоставянето на услуги.

Разлики между DORA и NIS2

- **Обхват:** DORA е насочена конкретно към финансовите институции и техните критични ИТ доставчици, докато NIS2 се прилага към по-широк кръг "съществени" и "важни" субекти в различни сектори.
- **Цел:** NIS2 се фокусира върху осигуряването на непрекъсваемост на "съществените" услуги, докато DORA набляга предимно на цифровата оперативна устойчивост във финансовия сектор.
- **Времеви график:** Изискванията на DORA трябва да влязат в сила на 17 януари 2025 г., докато NIS2 се очаква да влезе в сила до 17 октомври 2024 г.; всяка държава - членка на ЕС, обаче трябва да приложи това към своето местно законодателство, така че датите на прилагане могат да варират.
- **Неспазване на изискванията:** Санкциите по DORA за финансовите субекти се определят от компетентните органи, докато ИТ доставчиците се глобяват въз основа на процент от глобалните им приходи. NIS2 налага глоби въз основа на оборота както за "съществени", така и за "важни" субекти.

РЕПУБЛИКА БЪЛГАРИЯ
Министерство на електронното управление

Бисерка Радева – и.д. директор,
дирекция „Мрежова и информационна сигурност“,
Министерство на електронното управление
Тел.: +359 2 949 2301
E-mail: b.radeva@egov.government.bg