Deloitte.

Регламент за оперативната устойчивост на цифровите технологии (DORA)

10 юли 2024 г.|Делойт България

MAKING AN IMPACT THAT MATTERS since 1845

Контекст и ключови изводи свързани с Регламента

Еволюция|Хармонизация|По-стриктни изисквания| Нови субекти| Мултидисциплинарност|Оркестрация

Какво е оперативна устойчивост?

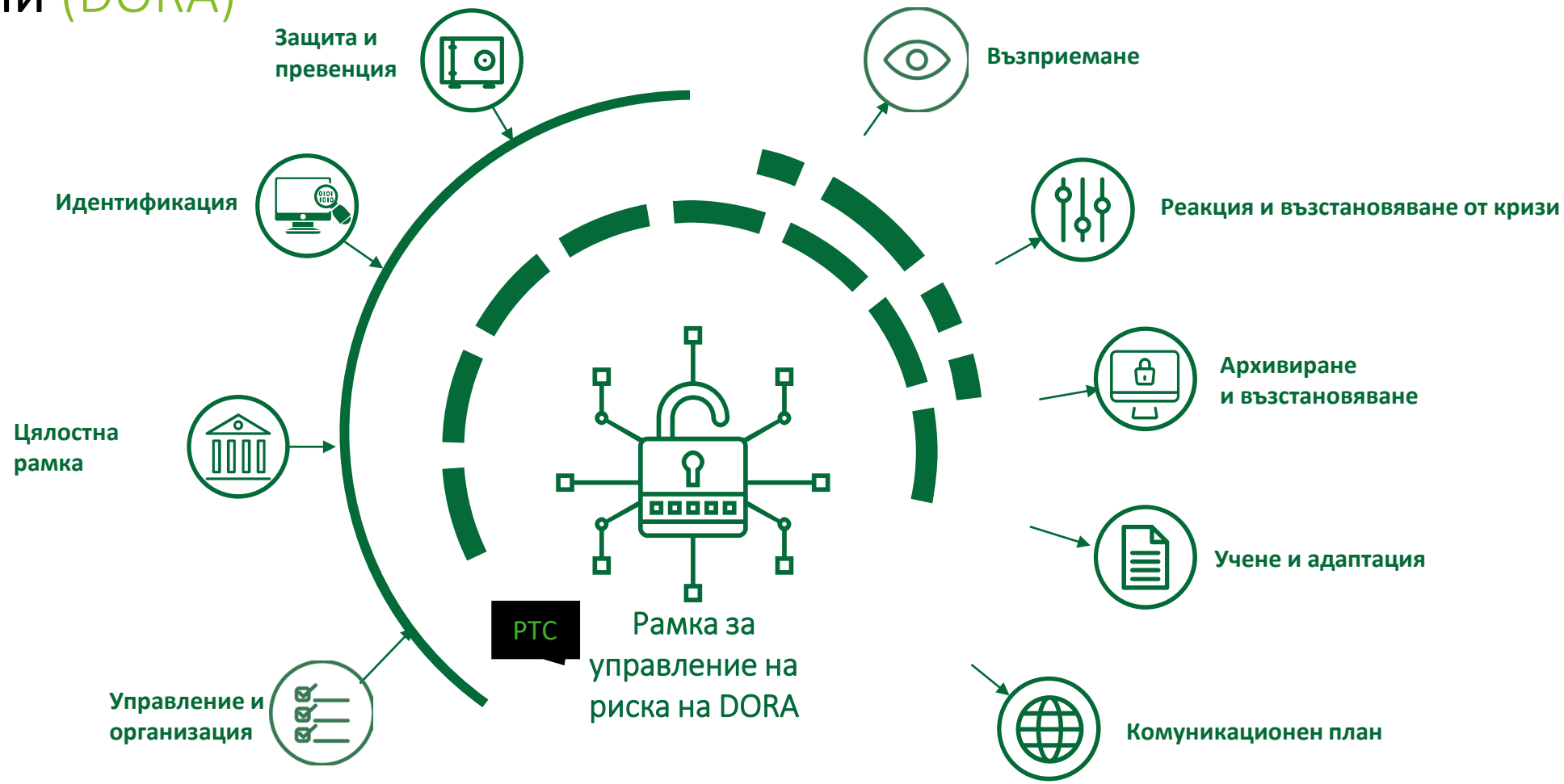
Способността на дадена финансова институция да поддържа своите важни и критични бизнес функции и инфомрационните системи, които ги подпомагат, налични и функциониращи, както при нормални работни условия, така и в случаи на сериозни смущения.

Основни заключения

- Революция (НЕ)
- Амбиции
- Трети страни доставчици на услуги в областта на ИКТ
- В съответствие ли съм?
- Колко трудна е задачата?

Регламент за оперативната устойчивост на цифровите технологии (DORA)

УПРАВЛЕНИЕ НА РИСКА В ОБЛАСТТА НА ИКТ



Регламент за оперативната устойчивост на цифровите технологии (DORA)

Инциденти, свързани с ИКТ

Регламент за оперативната устойчивост на цифровите технологии (DORA)

ТЕСТВАНЕ НА ОПЕРАТИВНАТА УСТОЙЧИВОСТ НА ЦИФРОВИТЕ ТЕХНОЛОГИИ

Класическите тестове за проникване (*ограничен обхват) да бъдат заменени с цялостни технически тестове*

Червен екип, Син екип, Лилав екип = TLPT

Задачи и възможности за разузнаване на заплахите

PTC

- (ЗАДЪЛЖИТЕЛНО) Всеобхватна програма за тестване на оперативната устойчивост на цифровите технологии
- (ЗАДЪЛЖИТЕЛНО) Обстойно тестване за проникване, базирано на реални заплахи, най-малко на всеки **3 години**
- (ЗАДЪЛЖИТЕЛНО) Критични функции и услуги, тествани **на живи производствени** системи
- (ЧЛЕН 24) Изисквания към лицата, провеждащи обстойни тестове за проникване

Регламент за оперативната устойчивост на цифровите технологии (DORA)

УПРАВЛЕНИЕ НА РИСКА ОТ ТРЕТИ СТРАНИ В ОБЛАСТТА НА ИКТ

ИКТ риск от трети страни СТРАТЕГИЯ

РТС

Финансовите субекти приемат и редовно преразглеждат стратегия относно риска от трети страни в областта на ИКТ, като вземат предвид стратегията на множество доставчици.

ИКТ риск от трети страни РЕГИСТЪР

РТС

Поддържа и актуализира регистър на информацията във връзка с всички договорни споразумения относно използването на ИКТ услуги, предоставяни от доставчици на услуги от трети страни в областта на ИКТ.

ИКТ риск от трети страни ДОКЛАДВАНЕ

Поддържа и актуализира Регистър на информацията във връзка с всички договорни споразумения относно използването на ИКТ услуги, предоставяни от доставчици на ИКТ услуги, трети страни, и предоставя определена информация на регулаторните органи.

ИКТ риск от трети страни КОНЦЕНТРАЦИЯ

- Идентифициране и оценка на риска от концентрация в областта на ИКТ
- Оценява дали и как потенциално дългите или сложни вериги от подизпълнители могат да повлияят на способността им да наблюдават изцяло договорените функции

Правни аспекти

- **Предварителна оценка на** доставчиците на ИКТ – допълнителни аспекти за доставчици от трети държави
- **Минимално съдържание на** всички договори с трета страна доставчик на ИКТ услуги (напр. ясно и пълно описание на услугите; съхранение на данни, поддръжка, уведомяване за инциденти и планове за действие, права за прекратяване и изходни стратегии и т.н.);
- Допълнителни изисквания за **критични или важни функции**;
- Доставчиците на услуги да спазват адекватни стандарти за **сигурност на данните**;
- Изисквания за **права за достъп**, **проверка и одит;**
- **Задължителни събития за прекратяване, изходни стратегии**;
- **Насоки на ЕЦБ за възлагане на дейности на външни страни** – DORA е с по-широк обхват
- Актуализиране на **политиките и процедурите**

Подготовката за януари 2025

3-етапен подход, започващ с текуща оценка на състоянието и идентифициране на пропуските, определяне на план за действие и пътна карта и изпълнение на плана.

Оценка на текущото състояние

- Определяне на цели
- Идентифициране на заинтересованите страни
- Определяне на критерии за оценка
- Извършване на оценката
- Приоритизиране на пропуските
- Документиране на резултатите

План за действие и пътна карта

- Приоритизиране на дейностите база на сложност и значимост
- Идентифициране на зависимости
- Задаване на срокове и срокове
- Идентифициране на рискове и заплахи за изълнение на пътната карта

Изпълнение

- Алокиране на ресурси
- Възлагане на задачи
- Задаване на срокове
- Проследяване на напредъка
- Разработване на комуникационен план
- Оценка на ефективността

3 Фази на DORA

Фаза 1

Фаза 2

Фаза 3

Предизвикателствата пред финансовите субекти

|Нашата гледна точка|

Авторитетът

Кой предпазва организацията от достигането на задънена улица?

Кой умее да тълкува в пълнота изискванията на Регламента?

Оркестрация

Или как стремежа за координиран и оркестриран подход в управлението на риска породен от използването на цифрови технологии, среща реалността, и тази среща е сеизмична

И още

Критични и важни функции; Бизнес собственик, ИКТ активи и категоризация; Сериозни, но много вероятни кибератаки; Стратегия за оперативна устойчивост на цифровите технологии; Задълбочени тестове за проникване, но в жива среда; И още……..