ENCRYPT 4.0

Съфинансирано от Европейския съюз

Матрица за одит на кибер риска (CRAM)

EXCEL ИНСТРУМЕНТ

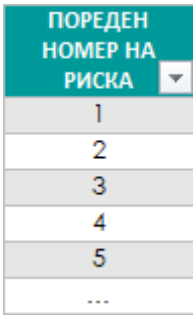
Подробни инструкции

Матрицата за одит на кибер риска (Cyber Risk Audit Matrix (CRAM)) е аналитичен инструмент, който има за цел да помогне на производствените компании да идентифицират, анализират, приоритизират рискове, както и своевременно да изготвят защитни процедури.

Този кратък наръчник има за цел да ви помогне в прилагането на инструмента CRAM в excel. Моля, преди това прочетете наръчника за използване на Матрицата за одит на кибер риска (CRAM)!

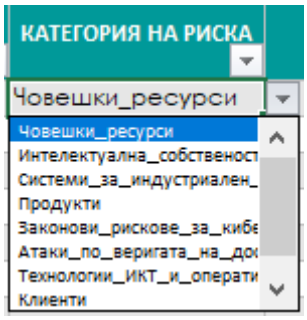
Матрицата за одит на кибер риска (CRAM) включва следните раздели:

- Автоматично фиксиран **номер на риска**, единствено с цел спомагане идентификацията на риска**.**



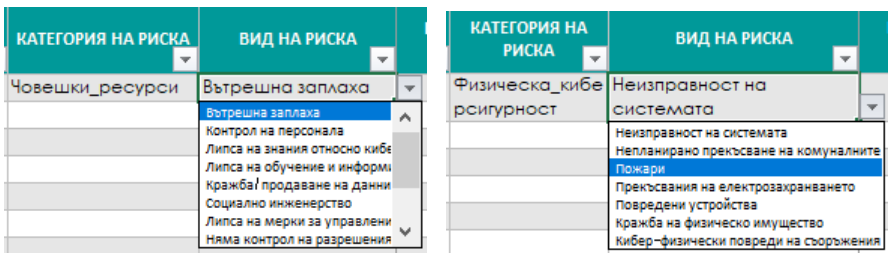
- **Категория на риска**

Изберете в инструмента категорията на риска; описанията на категориите са дадени в наръчника за използване на Матрицата за одит на кибер риска (CRAM).



- **Вид риск**

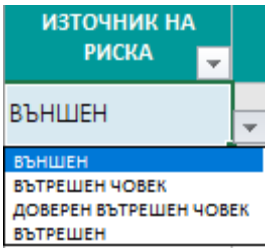
Според избраната категория инструментът CRAM ще ви предложи съответния вид риск.



За някои видове рискове има падащо меню, където ще намерите допълнителни рискове, които не са видими.

- **Източник на риска**

Изберете източник на риска: външен, вътрешен източник, доверен вътрешен източник, вътрешен.



Източник на риска	Описание
ВЪНШЕН	Атаки от външни страни, произтичащи от дигиталната среда.
ВЪТРЕШЕН ИЗТОЧНИК	Заплаха, причинена от служител, използващ умишлено или не упълномощен достъп, за да наруши сигурността на компанията.
ДОВЕРЕН ВЪТРЕШЕН ИЗТОЧНИК	Лице, получило достъп до системите и физическите помещения на бизнеса. Това включва бивши служители, доставчици, бизнес партньори, посетители и други трети страни.
ВЪНШЕН	Вътрешен източник (хардуерен, мрежов, софтуерен, организационен).

- **Описание на риска**

Отворено поле за описание на риска. Това ще спомогне по-доброто дефиниране на риска и следващите стъпки в процеса.

* Ако видът на риска е „проблеми с целостта на данните“, моля, посочете вида на данните в „Описание на риска“.

ПРОБЛЕМИ С ЦЕЛОСТТА НА ДАННИТЕ
цифрови данни на високо ниво
цифрови данни на ниско ниво
финансови данни
физически данни
данни на потребители

- **Потенциални разходи, свързани с последствията от риска**

В това поле можете да посочите и идентифицирате всички потенциални разходи, свързани с последствията от реализиране на риска. Например, стойността, свързана с кражба на фирмена информация или финансова измама, разходи, свързани със сериозна загуба на функционалност или производителност, включително поради вируси и зловреден софтуер, атаки върху уеб сървъра, злоупотреба с привилегии за достъп, както и вандалско поведение спрямо оборудване или директна кражба…

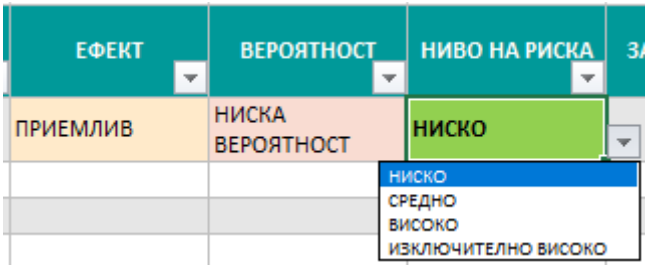
- **Отдел, който може да бъде засегнат**

Отворено поле за посочване на евентуално засегнат/и отдел/и в организацията.

- **Превантивни мерки/ предварително изпълнени действия**

Отворено поле за посочване и описание на превантивни мерки/извършени действия (ако е приложимо).

- **Оценка и изчисляване на елементите на риска** (ефект от риска, вероятност на риска, общо ниво на риска)



Входящи данни относно вероятността (т.е. вероятността да се прояви даден риск) и влиянието (т.е. сериозността при проявление на риска) от идентифицираните рискове. Оценяват се както вероятността, така и влиянието, по скала от Ниско (0), Средно (1), Високо (2) и Изключително високо (3).

НИСКО **0 - Приемлив** ОК е да се продължи	**СРЕДНО** **1 - Среден** Полагане на усилия за смекчаване на	**ВИСОКО** **2- Неприемлив по принцип** Търсене на помощ - следва да се	**ИЗКЛЮЧИТЕЛНО ВИСОКО** **3 - Неприемлив** Събитието трябва да се отложи

ЕФЕКТ			
ПРИЕМЛИВ	**ПОНОСИМ**	**НЕЖЕЛАТЕЛЕН**	**НЕТЪРПИМ**
Малък до никакъв	Чувстват се ефекти, но	Сериозен ефект върху	Може да доведе до
НИСКО 1	СРЕДНО 4	СРЕДНО 6	ВИСОКО 10
НИСКО 2	СРЕДНО 5	ВИСОКО 8	ИЗКЛЮЧИТЕЛНО ВИСОКО 11
СРЕДНО 3	ВИСОКО 7	ВИСОКО 9	ИЗКЛЮЧИТЕЛНО ВИСОКО 12

- **Задействащи фактори**

Отворено поле за описание на задействащите фактори или действия, които карат системата да инициира отговор. Те генерират известие за необичаен инцидент или поведение.

- **Смекчаване/действия за предприемане**

Отворено поле за посочване на смекчаващи действия в посока редуциране на рисковете, квалифицирани като средни и високи. Това означава опит за елиминиране или намаляване на честотата, силата или сериозността на рисковете или минимизиране на потенциалното влияние на дадена заплаха.

В наръчника за използване на Матрицата за одит на кибер риска (CRAM)са идентифицирани два вида контролни действия – превантивни и коригиращи, за всяка от деветте категории рискове.

- **Потенциални разходи за смекчаване**

Отворено поле за посочване на потенциалните разходи за смекчаване.

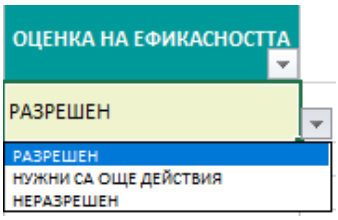
- **Краен срок**

Краен срок за изпълнение на действия.

- **Отговорност**

Отворено поле за ясно посочване на лицето, отговорно за управление на риска, както и на супервайзора, отговорен за мониторинг.

- **Оценка на ефикасността**



Оценката чрез Encrypt 4.0 CRAM е систематичен, постоянен процес. Той е цикличен процес, в рамките на който след идентифициране, анализ, оценка, адресиране и приемане на рисковете трябва да се извърши и мониторинг и преглед на рискове. Ако даден проблем продължава, са необходими допълнителни действия за неговотото разрешаване и за тази цел трябва да се върнете на предишната стъпка от третиране на риска. А ако проблемът остане неразрешен, е необходимо да направите повторна оценка на риска.

- **Доклад**

След попълване на необходимите полета докладът за риска е готов.

Проектът ENCRYPT4.0 (2020-1-RO01-KA202-079983) е финансиран с подкрепата на Европейската комисия. Настоящата публикация отразява само вижданията на автора, а Комисията не носи отговорност за използването на съдържащата се в нея информация.