CRAM - INSTRUMENT EXCEL

Pas cu pas

Cyber Risk Audit Matrix (CRAM) este un instrument analitic care va sprijini companiile producătoare să identifice, să analizeze, să prioritizeze riscurile și să stabilească prompt măsuri de protecție.

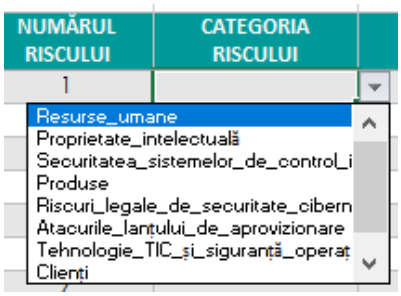
Acest scurt ghid își propune să vă sprijine în aplicarea instrumentului CRAM în format excel. Vă rugăm să citiți manualul CRAM înainte!

CRAM cuprinde:

- **numărul de risc** care este stabilit automat, pentru a facilita identificarea riscului.
-

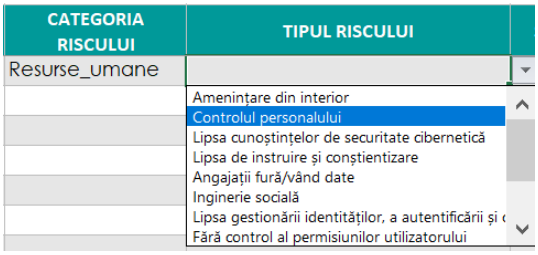
- **categoria de risc**

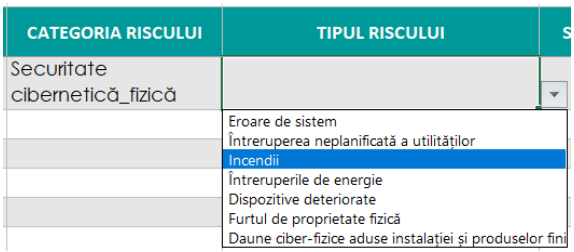
Selectați în instrument categoria de risc, descrierea categoriilor fiind prezentată în Manualul CRAM.



- **tipul de risc**

În funcție de categoria selectată, instrumentul CRAM vă va sugera tipul respectiv de risc.

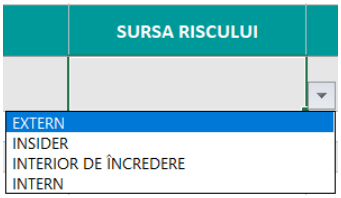




În unele categorii de risc, există un meniu derulant în care puteți găsi mai multe riscuri care nu sunt vizibile.

- **sursa de risc**

Selectați sursa riscului: extern, interior, interior de încredere, intern.



Sursa de risc	Descriere
EXTERN	Atacurile din partea forțelor externe au avut originea în mediul digital.
INTERIOR	O amenințare cauzată de un angajat care va folosi accesul autorizat, cu bună știință sau fără să vrea, pentru a dăuna securității companiei.
INTERIOR DE ÎNCREDERE	Este oricine căruia i s-a oferit acces la sistemele și spațiile fizice ale unei companii. Acestea includ foști angajați, vânzători, clienți, parteneri de afaceri, vizitatori sau alte terțe părți.
INTERN	Sursă internă (hardware, rețea, software, organizațional).

- **descrierea riscului**

Câmp deschis pentru descrierea riscului. Acest lucru va ajuta la o mai bună definire a riscului și a următorilor pași ai procesului.

* Dacă tipul de risc este „Probleme de integritate a datelor”, vă rugăm să includeți tipul de date în „Descrierea riscului”

PROBLEME DE INTEGRITATE A DATELOR
date digitale de nivel înalt
date digitale de nivel scăzut
date financiare
date fizice
datele utilizatorului

- **costuri potențiale asociate cu consecințele riscului**

Câmp deschis pentru a identifica toate costurile potențiale asociate cu consecințele riscului care se va întâmpla. De exemplu: valoarea monetară legată de furtul de informații deținute sau de fraudă financiară; costurile legate de pierderea severă a utilizării sau a productivității includ viruși și programe malware, atacuri de refuzare a serviciului web server, abuz de privilegii de acces și vandalism sau furt total de echipamente…

- **departamentul de organizare care ar putea fi afectat**

Deschideți câmpul pentru a identifica departamentele organizației care ar putea fi afectate.

- **măsuri/acţiuni preventive implementate anterior**

Câmp deschis pentru a identifica și descrie măsurile/acțiunile preventive implementate anterior (dacă este cazul).

- **Evaluarea și calculul elementelor de risc** (impactul riscului, probabilitatea riscului, nivelul general al riscului)

IMPACT	PROBABILITATE	NIVELUL RISCULUI
ACCEPTABIL	IMPROBABIL	SCĂZUT

SCĂZUT
MEDIU
ÎNALT
EXTREM

Intrări referitoare la probabilitatea (adică probabilitatea ca un risc să apară) și impactul (adică severitatea riscului în cazul în care acesta să apară) riscurilor identificate. Ei evaluează atât probabilitatea, cât și impactul utilizând scala Mic (0), Mediu (1), Mare (2) și Extrem (3).

NIVELUL RISCULUI LEVEL	SCĂZUT 0 - Acceptabil SE POATE CONTINUA	MEDIU 1 - Moderat SUNT NECESARE ACȚIUNI DE ATENUARE	ÎNALT 2- În general inacceptabil CĂUTAȚI SUPORT - acțiuni care urmează să fie implementate în 6 luni	EXTREM 3 - Intolerabil PLASAȚI EVENIMENTUL ÎN AȘTEPTARE

	IMPACT			
	ACCEPTABIL	TOLERABIL	INDEZIRABIL	INTOLERABIL
	Puțin sau fără efect	Efectele sunt resimțite, dar fără rezultate critice	Impact grav asupra cursului acțiunii și rezultatului	Ar putea duce la un dezastru
PROBABILITATE				
IMPROBABIL Este puțin probabil ca riscul să apară	SCĂZUT 1	MEDIU 4	MEDIU 6	ÎNALT 10
POSIBIL Probabil riscul va	SCĂZUT 2	MEDIU 5	ÎNALT 8	EXTREM 11
PROBABIL Riscul va apărea	MEDIU 3	ÎNALT 7	ÎNALT 9	EXTREM 12

- **declanșare**

Deschideți câmpul pentru a descrie declanșatorii sau acțiunile care determină sistemul să inițieze un răspuns. Declanșatoarele produc o alertă atunci când are loc un incident sau un comportament anormal.

- **acțiuni de atenuare/acțiuni care urmează să fie implementate**

Câmp deschis pentru identificarea acțiunilor de atenuare a riscurilor evaluate ca fiind Medii spre Ridicate. Aceasta înseamnă încercarea de a elimina sau de a reduce frecvența, amploarea sau severitatea expunerii la riscuri sau de a minimiza impactul potențial al unei amenințări.

În Manualul CRAM sunt prezentate două tipuri de controale ale acțiunilor – preventive și corective în fiecare dintre cele nouă categorii de risc.

- **costurile potențiale ale atenuării**

Câmp deschis pentru identificarea costurilor potențiale de atenuare.

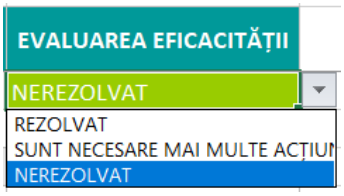
- **termen limita**

Termenul limită pentru acțiunile care urmează să fie implementate.

- **responsabilitate**

Câmp deschis pentru identificarea clară a persoanei responsabile cu gestionarea riscurilor și a supraveghetorului responsabil cu monitorizarea.

- **evaluarea eficacităţii**



CRAM-ul Encrypt 4.0 este un proces sistematic, continuu. Este un proces ciclic care, odată ce a identificat, analizat, evaluat, abordat și acceptat riscurile, trebuie să efectueze un proces de monitorizare și revizuire a riscurilor. În cazul în care problema persistă, va trebui să aplicați acțiuni complementare suplimentare pentru a rezolva problema, iar pentru aceasta, va trebui să reveniți la pasul anterior al tratamentului riscului. Și dacă problema rămâne nerezolvată, va trebui să reevaluați riscul.

- **raport**

După ce ai completat toate câmpurile necesare, ai raportul de riscuri gata completat.

Proiectul ENCRYPT4.0 (2020-1-RO01-KA202-079983) a fost finanțat cu sprijinul Comisiei Europene. Această publicație reflectă doar punctul de vedere al autorilor, iar Comisia nu poate fi trasă la răspundere pentru orice utilizare care ar putea fi făcută informațiilor conținute în aceasta.