ENCRYPT 4.0

Kofinanziert von der Europäischen Union

CRAM EXCEL TOOL

Leitfaden

Die Cyber Risk Audit Matrix (CRAM) ist ein Analysetool, das die produzierenden Unternehmen dabei unterstützt, Risiken zu identifizieren, zu analysieren, zu priorisieren und rechtzeitig Schutzmaßnahmen zu ergreifen.

Dieser kurze Leitfaden soll Sie bei der Anwendung des CRAM-Excel-Tools unterstützen. Bitte lesen Sie vorher das CRAM-Handbuch!

Das CRAM enthält:

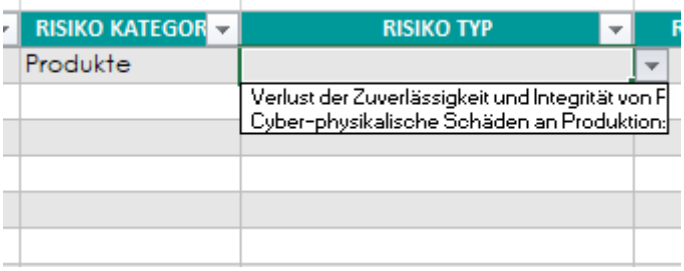
- **Risiko Nummer:** Automatisch festgelegt – zur Identifikation des Risikos.

- **Risiko Kategorie**

Wählen Sie im Tool die Risikokategorie aus, die Beschreibung der Kategorien finden Sie im CRAM-Handbuch.

- **Risiko Typ**

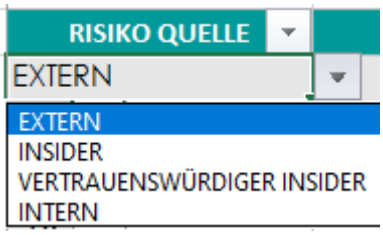
Entsprechend der ausgewählten Kategorie schlägt Ihnen das CRAM-Tool die jeweilige Risikoart vor.



Bei einigen Risikoarten gibt es ein Dropdown-Menü, in dem Sie einige weitere Risiken finden, die nicht sichtbar sind.

- **Risiko Quelle:**

Wählen Sie die Risiko Quelle: External, Insider, Trusted Insider, Internal.



Risk Source	Description
EXTERNAL	Angriffe von externen Kräften haben ihren Ursprung im digitalen Umfeld.
INSIDER	Eine Bedrohung, die von einem Mitarbeiter verursacht wird, der den autorisierten Zugang wissentlich oder unwissentlich nutzt, um die Sicherheit des Unternehmens zu beeinträchtigen.
TRUSTED INSIDER	Jede Person, der Zugang zu den Systemen und physischen Räumlichkeiten eines Unternehmens gewährt wurde. Dazu gehören ehemalige Mitarbeiter, Lieferanten, Kunden, Geschäftspartner, Besucher oder sonstige Dritte.
INTERNAL	Interne Quelle (Hardware, Netzwerk, Software, Organisation).

- **Risiko Beschreibung**

Offenen Sie das Feld für die Beschreibung des Risikos. Dies wird dazu beitragen, das Risiko und die nächsten Schritte des Prozesses besser zu definieren.

* Wenn der Risikotyp "Datenintegritätsprobleme" ist, geben Sie bitte den Datentyp in der "Risikobeschreibung" an.

DATENINTEGRITÄT
High-level digitale Daten
Low-level digitale Daten
Finanz Daten
Physische Daten
Benutzerdaten

- **potenzielle Kosten im Zusammenhang mit den Folgen des Risikos**

Öffnen sie das Feld, um alle potenziellen Kosten zu identifizieren, die mit den Folgen des eintretenden Risikos verbunden sind. B.: Geldwert im Zusammenhang mit Diebstahl geschützter Informationen oder Finanzbetrug; Kosten im Zusammenhang mit schwerwiegenden Nutzungs- oder Produktivitätsverlusten umfassen Viren und Malware, Denial-of-Service-Angriffe auf Webserver, Missbrauch von Zugriffsrechten und Gerätevandalismus oder direkter Diebstahl…

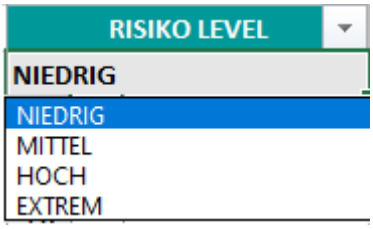
- **möglicherweise betroffene Organisationsabteilungen**

Öffnen Sie das Feld, um die möglicherweise betroffene(n) Abteilung(en) der Organisation zu identifizieren.

- **Vorbeugende Maßnahmen/Aktionen, die zuvor umgesetzt wurden**

Öffnen sie das Feld zur Identifizierung und Beschreibung der zuvor durchgeführten vorbeugenden Maßnahmen/Aktionen (falls zutreffend).

- **Bewertung und Berechnung von Risikoelementen** (Risikoauswirkungen, Risikowahrscheinlichkeit, Gesamtrisikoniveau)



Eingaben bezüglich der Wahrscheinlichkeit (d. h. der Wahrscheinlichkeit, dass ein Risiko eintritt) und der Auswirkung (d. h. der Schwere des Risikos, falls es eintreten sollte) der identifizierten Risiken. Sie bewerten sowohl die Wahrscheinlichkeit als auch die Auswirkung auf einer Skala von Niedrig (0), Mittel (1), Hoch (2) und Extrem (3).

RISIKO LEVEL	NIEDRIG 0 - Akzeptabel OK - Keine Maßnahmen notwendig	MITTEL 1 - Moderat MAßNAHMEN NOTWENDIG	HOCH 2- Generell inakzeptabel UNTERSTÜTZUNG ANFORDERN - Maßnahmen, die innerhalb von 6 Monaten umgesetzt werden sollen	EXTREM 3 - Untragbar UMGEHENDE MAßNAHMEN SETZEN

	AUSWIRKUNG			
	AKZEPTABEL	ERTRÄGLICH	UNERWÜNSCHT	UNTRAGBAR
	Wenig, bis hin zu keiner Auswirkung	Auswirkung spürbar, aber nicht kritisch	Schwerwiegende Auswirkungen auf den Verlauf und das Ergebnis der Aktion	Könnte zu einer Katastrophe führen
WAHRSCHEINLICHKEIT				
UNWAHRSCHEINLICH Risiko tritt wahrscheinlich nicht ein	NIEDRIG 1	MITTEL 4	MITTEL 6	HOCH 10
MÖGLICH Risiko wird wahrscheinlich eintreten	NIEDRIG 2	MITTEL 5	HOCH 8	EXTREM 11
WAHRSCHEINLICH Risiko wird eintreten	MITTEL 3	HOCH 7	HOCH 9	EXTREM 12

- **Auslöser**

Öffnen SIe das FeldFeld, um die Auslöser oder Aktionen zu beschreiben, die das System veranlassen, eine Reaktion auszulösen. Die Auslöser erzeugen eine Warnung, wenn ein anormaler Vorfall oder ein anormales Verhalten auftritt.

- **zu implementierende Maßnahmen**

Öffnen Sie das Feld zur Identifizierung von Minderungsmaßnahmen für die als mittel bis hoch eingestuften Risiken. Dies bedeutet, dass versucht wird, die Häufigkeit, das Ausmaß oder die Schwere von Risiken zu eliminieren oder zu reduzieren oder die potenziellen Auswirkungen einer Bedrohung zu minimieren. Im CRAM-Handbuch werden zwei Arten von Maßnahmenkontrollen identifiziert – präventiv und korrektiv in jeder der neun Risikokategorien.

- **Pentielle Kosten der Maßnahmen**

Öffnen Sie das Feld der Kosten der Maßnahmen.

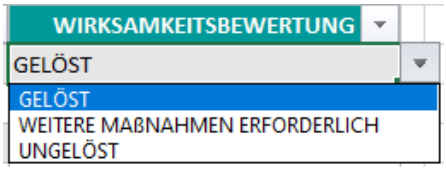
- **Termin**

Frist für die durchzuführenden Maßnahmen.

- **Verantwortung**

Öffnen Sie das Feld zur eindeutigen Identifizierung des Verantwortlichen für das Risikomanagement und des für die Überwachung zuständigen Vorgesetzten.

- **Bewertung der Wirksamkeit**



Das Encrypt 4.0 CRAM ist ein systematischer, kontinuierlicher Prozess. Es handelt sich um einen zyklischen Prozess, der, nachdem er die Risiken identifiziert, analysiert, bewertet, adressiert und akzeptiert hat, einen Risikoüberwachungs- und Überprüfungsprozess durchführen muss. Falls das Problem weiterhin besteht, müssen Sie weitere ergänzende Maßnahmen ergreifen, um das Problem zu lösen, und dazu müssen Sie zum vorherigen Schritt der Risikobehandlung zurückkehren. Und wenn das Problem weiterhin ungelöst bleibt, müssen Sie das Risiko neu bewerten.

- **Bericht**

Nachdem Sie alle erforderlichen Felder ausgefüllt haben, haben Sie Ihren Risikobericht abgeschlossen.

Das Projekt ENCRYPT4.0 (2020-1-RO01-KA202-079983) wurde mit Unterstützung der Europäischen Kommission gefördert. Diese Veröffentlichung gibt nur die Ansichten des Verfassers wieder, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.