CRAM EXCEL TOOL

Step-by-step

The Cyber Risk Audit Matrix (CRAM) is an analytic tool that will support the manufacturing companies to identify, analyse, prioritise risks and establish protective measures promptly.

This short guideline aims to support you in the application of the CRAM excel tool. Please read the CRAM Handbook before!

The CRAM includes:

- **risk number** automatically fixed, just to support in the identification of the risk.

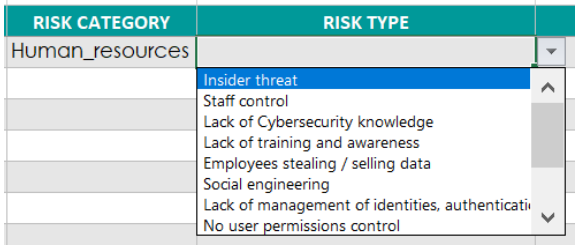
RISK NUMBER
1
2
3
4
5
…

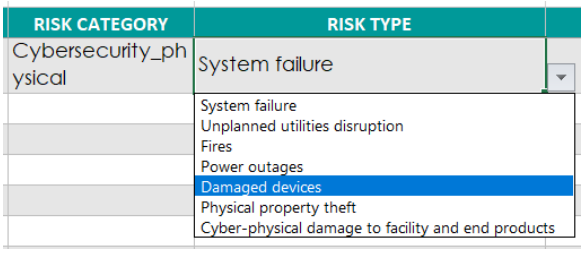
- **risk category**

Select in the tool the risk category, the description of the categories is presented in the CRAM Handbook.

- **risk type**

According to the selected category the CRAM tool will suggest you the respective risk type.

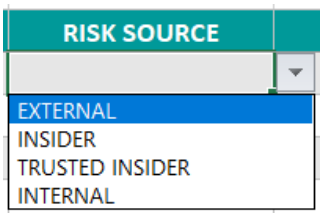




In some risk types, there is a dropdown menu where you can find some more risks that are not visible.

- **risk source**

Select the source of the risk: External, Insider, Trusted Insider, Internal.



Risk Source	Description
EXTERNAL	Attacks from external forces originated in the digital environment.
INSIDER	A threat caused by an employee that will use the authorized access, wittingly or unwittingly, to do harm to the security of the company.
TRUSTED INSIDER	Is anyone who has been given access to a business's systems and physical premises. This includes past employees, vendors, customers, business partners, visitors or other third parties.
INTERNAL	Internal source (hardware, network, software, organisational).

- **risk description**

Open field for the description of the of the risk. This will help to better define the risk and the next steps of the process.

* If Risk Type is "Data Integrity Issues", please include the type of data in the "Risk Description"

DATA INTEGRITY ISSUES
high-level digital data
low-level digital data
financial data
physical data
user data

- **potential costs associated with the consequences of the risk**

Open field to identify all the potential costs associated with the consequences of the risk to happen. E.g.: monetary value related with theft of proprietary information or financial fraud; costs related with severe loss of use or productivity include viruses and malware, Web server denial-of-service attacks, abuse of access privileges, and equipment vandalism or outright theft…

- **organisation department that might be affected**

Open field to identify the organisation department(s) that might be affected.

- **preventive measures/actions previously implemented**

Open field to identify and describe the preventive measures/actions previously implemented (if applicable).

- **Risk elements assessment and calculation** (risk impact, risk likelihood, overall risk level)

IMPACT	LIKELIHOOD	RISK LEVEL
ACCEPTABLE	IMPROBABLE	LOW

LOW
MEDIUM
HIGH
EXTREME

Inputs concerning the probability (i.e. the likelihood that a risk will occur) and the impact (i.e. the severity of the risk should it occur) of the identified risks. They rate both probability and impact using a scale of Low (0), Medium (1), High (2) and Extreme (3).

LOW	MEDIUM	HIGH	EXTREME
0 - Acceptable	1 - Moderate	2- Generally Unacceptable	3 - Intolerable
OK TO PROCEED	TAKE MITIGATION EFFORTS	SEEK SUPPORT - actions to be implemented in 6 months	PLACE EVENT ON HOLD

IMPACT			
ACCEPTABLE	TOLERABLE	UNDESIRABLE	INTOLERABLE
Little to no effect	Effects are felt but with no critical outcome	Serious impact to the course of action and outcome	Could result in disaster
LOW 1	MEDIUM 4	MEDIUM 6	HIGH 10
LOW 2	MEDIUM 5	HIGH 8	EXTREME 11
MEDIUM 3	HIGH 7	HIGH 9	EXTREME 12

- **triggers**

Open field to describe the triggers or actions that causes the system to initiate a response. Triggers produces an alert when an anomalous incident or behaviour occurs.

- **mitigation/actions to be implemented**

Open field for the identification of mitigation actions for the risks qualified as Medium to High. This means trying to eliminate or reduce the frequency, magnitude, or severity of exposure to risks, or minimising the potential impact of a threat.

In the CRAM Handbook there are identified two types of action controls – preventive and corrective in each of the nine risk categories.

- **potential costs of mitigation**

Open field for the identification of the potential costs of mitigation.

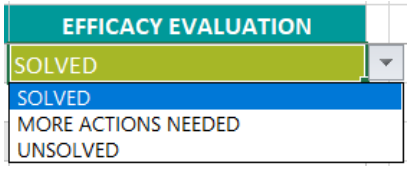
- **deadline**

Deadline for the actions to be implemented.

- **responsibility**

Open field for the clear identification of the person responsible for the risk management and the supervisor responsible for monitoring.

- **effectiveness evaluation**



The Encrypt 4.0 CRAM is a systematic, continuous process. It is a cyclical process that once it has identified, analyzed, assessed, evaluated, addressed, and accepted the risks, it must carry out a risk monitoring and review process. In case the problem persists, you will need to apply further complementary actions to solve the problem, and for this, you will need to go back to the previous step of risk treatment. And if the problem remains unresolved, you will need to re-evaluate the risk.

- **report**

After fulfilling all the necessary fields, you have your risks report completed.

ENCRYPT 4.0
Co-funded by the Erasmus+ Programme of the European Union

ENCRYPT4.0 Project (2020-1-RO01-KA202-079983) has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.